Documentazione di StorageGRID 11,8

StorageGRID

NetApp
December 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-118/index.html on December 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Documentazione di StorageGRID 11,8 . . . 1
Appliance StorageGRID . . . 2
Note di rilascio . . . 3
Inizia subito con un sistema StorageGRID . . . 4
Scopri di più su StorageGRID . . . 4
Che cos'è StorageGRID? . . . 4
Cloud ibridi con StorageGRID . . . 6
Architettura StorageGRID e topologia di rete . . . 7
Nodi e servizi Grid . . . 11
Come StorageGRID gestisce i dati . . . 22
Esplora StorageGRID . . . 35
Linee guida per il networking . . . 43
Linee guida per il networking: Panoramica . . . 43
Tipi di rete StorageGRID . . . 44
Esempi di topologia di rete . . . 48
Requisiti di rete . . . 55
Requisiti specifici della rete . . . 57
Considerazioni di rete specifiche per l'implementazione . . . 59
Installazione e provisioning di rete . . . 62
Linee guida per la post-installazione . . . 63
Riferimento porta di rete . . . 63
Avvio rapido per StorageGRID . . . 74
Installazione, aggiornamento e correzione rapida StorageGRID . . . 77
Appliance StorageGRID . . . 77
Installare StorageGRID su Red Hat Enterprise Linux . . . 77
Avvio rapido per l'installazione di StorageGRID su Red Hat Enterprise Linux . . . 77
Pianificare e preparare l'installazione su Red Hat . . . 78
Automatizzare l'installazione di StorageGRID su Red Hat Enterprise Linux . . . 102
Implementare nodi grid virtuali (Red Hat) . . . 105
Configurare la griglia e completare l'installazione (Red Hat) . . . 127
Panoramica dell'API REST per l'installazione . . . 140
Dove andare . . . 141
Risolvere i problemi di installazione . . . 141
Esempio di /etc/sysconfig/network-scripts . . . 142
Installare StorageGRID su Ubuntu o Debian . . . 144
Avvio rapido per l'installazione di StorageGRID su Ubuntu o Debian . . . 144
Pianificare e preparare l'installazione su Ubuntu o Debian . . . 145
Automatizzare l'installazione (Ubuntu o Debian) . . . 170
Implementare nodi virtual grid (Ubuntu o Debian) . . . 173
Configurare la griglia e completare l'installazione (Ubuntu o Debian) . . . 195
Panoramica dell'API REST per l'installazione . . . 208
Dove andare . . . 209
Risolvere i problemi di installazione . . . 210

Esempio di /etc/network/interfaces 211
Installare StorageGRID su VMware 212
Guida rapida per l'installazione di StorageGRID su VMware 212
Pianificare e preparare l'installazione su VMware 213
Automatizzare l'installazione (VMware) 223
Implementazione di Virtual Machine Grid Node (VMware) 237
Configurare la griglia e completare l'installazione (VMware) 246
Panoramica dell'API REST per l'installazione 259
Dove andare 260
Risolvere i problemi di installazione 261
Aggiornare il software StorageGRID 262
Aggiornamento del software StorageGRID: Panoramica 262
Novità di StorageGRID 11,8 263
Funzioni e funzionalità rimosse o obsolete 265
Modifiche all'API Grid Management 266
Modifiche all'API di gestione del tenant 267
Pianificare e prepararsi per l'upgrade 267
Aggiornare il software 275
Risolvere i problemi di aggiornamento 283
Applicare la correzione rapida StorageGRID 285
Procedura di hotfix StorageGRID: Panoramica 285
Impatto del sistema quando si applica una correzione rapida 286
Ottenere il materiale necessario per la correzione rapida 287
Scaricare il file hotfix 288
Controllare le condizioni del sistema prima di applicare la correzione rapida 289
Applicare la correzione rapida 289
Configurare e gestire un sistema StorageGRID 294
Amministrare StorageGRID 294
Administer StorageGRID: Panoramica 294
Inizia subito con Grid Manager 294
Controllo dell'accesso a StorageGRID 325
USA la federazione di grid 371
Gestire la sicurezza 408
Gestire i tenant 478
Configurare le connessioni client 497
Gestire reti e connessioni 541
USA AutoSupport 560
Gestire i nodi di storage 576
Gestire i nodi di amministrazione 595
Gestire i nodi di archiviazione 604
Migrare i dati in StorageGRID 626
Gestire gli oggetti con ILM 628
Gestire gli oggetti con ILM 628
ILM e ciclo di vita degli oggetti 629
Creare e assegnare i gradi di storage 651

Utilizzare i pool di storage . . . 653
Utilizza i Cloud Storage Pools . . . 662
Gestire i profili di erasure coding . . . 681
Configurazione delle regioni (opzionale e solo S3) . . . 685
Creare una regola ILM . . . 686
Gestire le policy ILM . . . 703
Utilizzare le policy ILM e le regole ILM . . . 719
USA blocco oggetti S3 . . . 724
Esempio di regole e policy ILM . . . 733
Protezione avanzata del sistema . . . 753
Protezione avanzata del sistema: Panoramica . . . 753
Linee guida per la protezione avanzata degli aggiornamenti software . . . 754
Linee guida per la protezione avanzata delle reti StorageGRID . . . 755
Linee guida per la protezione avanzata dei nodi StorageGRID . . . 756
Linee guida per la protezione avanzata di TLS e SSH . . . 759
Altre linee guida per la protezione avanzata . . . 760
Configurare StorageGRID per FabricPool . . . 761
Configure StorageGRID for FabricPool: Panoramica . . . 761
Informazioni necessarie per collegare StorageGRID come Tier cloud . . . 763
Utilizzare l'installazione guidata di FabricPool . . . 764
Configurare StorageGRID manualmente . . . 778
Configurare Gestore di sistema di ONTAP . . . 788
Configurare il server DNS . . . 790
Best practice StorageGRID per FabricPool . . . 791
Rimuovere i dati FabricPool da StorageGRID . . . 795
Utilizzare tenant e client StorageGRID . . . 797
Utilizzare un account tenant . . . 797
USA un account tenant: Panoramica . . . 797
Come effettuare l'accesso e disconnettersi . . . 798
Comprendere la dashboard di Tenant Manager . . . 803
API di gestione del tenant . . . 806
Utilizzare connessioni di federazione di griglie . . . 811
Gestire gruppi e utenti . . . 825
Gestire le chiavi di accesso S3 . . . 844
Gestire i bucket S3 . . . 850
Gestire i servizi della piattaforma S3 . . . 872
UTILIZZARE L'API REST S3 . . . 912
Versioni e aggiornamenti supportati dall'API REST S3 . . . 912
Riferimento rapido: Richieste API S3 supportate . . . 915
Eseguire il test della configurazione dell'API REST S3 . . . 933
Come StorageGRID implementa l'API REST S3 . . . 935
Supporto per Amazon S3 REST API . . . 950
Operazioni personalizzate di StorageGRID . . . 999
Policy di accesso a bucket e gruppi . . . 1021
Operazioni S3 registrate nei registri di audit . . . 1047

USA API REST di Swift (obsoleto) 1048
USA Swift REST API: Panoramica 1048
Verifica della configurazione delle API REST Swift 1051
Operazioni supportate da Swift REST API 1053
Operazioni API Swift REST di StorageGRID 1065
Operazioni rapide monitorate nei registri di audit 1069
Monitorare e risolvere i problemi di un sistema StorageGRID 1070
Monitorare il sistema StorageGRID 1070
Monitorare un sistema StorageGRID: Panoramica 1070
Visualizzare e gestire la dashboard 1070
Visualizzare la pagina nodi 1073
Informazioni da monitorare regolarmente 1107
Avvisi e allarmi 1137
Riferimenti ai file di log 1229
Configurare le destinazioni dei messaggi di controllo e del registro 1248
Utilizzare il monitoraggio SNMP 1262
Raccogliere dati StorageGRID aggiuntivi 1275
Risolvere i problemi relativi al sistema StorageGRID 1309
Risoluzione dei problemi di un sistema StorageGRID: Panoramica 1309
Risolvere i problemi relativi a oggetti e storage 1316
Risolvere i problemi relativi ai metadati 1354
Risolvere gli errori del certificato 1360
Risolvere i problemi relativi al nodo di amministrazione e all'interfaccia utente 1362
Risolvere i problemi di rete, hardware e piattaforma 1367
Risolvere i problemi di un server syslog esterno 1375
Esaminare i registri di audit 1378
Esaminare i registri di audit: Panoramica 1378
Controllare il flusso e la conservazione dei messaggi 1378
Accedere al file di log di audit 1381
Controllo della rotazione del file di log 1382
Formato del file di log di audit 1382
Formato del messaggio di audit 1395
Messaggi di audit e ciclo di vita degli oggetti 1400
Messaggi di audit 1407
Espandere una griglia 1463
Espandere una griglia: Panoramica 1463
Pianificare l'espansione di StorageGRID 1464
Aggiungere capacità di storage 1464
Aggiungere capacità di metadati 1471
Aggiungi nodi grid per aggiungere funzionalità al tuo sistema 1473
Aggiungere un nuovo sito 1474
Raccogliere il materiale necessario 1475
Scaricare ed estrarre i file di installazione di StorageGRID 1475
Verificare l'hardware e il collegamento in rete 1481
Aggiungere volumi di storage 1482

Aggiungere volumi di storage ai nodi di storage . . . 1482
VMware: Aggiunta di volumi di storage a Storage Node . . . 1485
Linux: Aggiunta di volumi direct-attached o SAN al nodo di storage . . . 1486
Aggiunta di nodi o siti grid . . . 1490
Aggiunta di nodi di griglia al sito esistente o aggiunta di un nuovo sito . . . 1490
Aggiornare le subnet per Grid Network . . . 1490
Implementare nuovi nodi grid . . . 1492
Eseguire l'espansione . . . 1497
Configurare il sistema esteso . . . 1504
Fasi di configurazione dopo l'espansione . . . 1504
Verificare che il nodo di storage sia attivo . . . 1506
Copia database nodo amministratore . . . 1506
Copia le metriche Prometheus . . . 1508
Copia dei registri di audit . . . 1509
Ribilanciare i dati con codifica di cancellazione dopo l'aggiunta di nodi di storage . . . 1511
Risolvere i problemi di espansione . . . 1514
Gestire un sistema StorageGRID . . . 1516
Manutenzione della griglia: Panoramica . . . 1516
Prima di iniziare . . . 1516
Procedure di manutenzione per le appliance . . . 1516
Scarica Recovery Package . . . 1516
Decommissiona i nodi o il sito . . . 1517
Procedura di decommissionamento: Panoramica . . . 1517
Decommissionamento dei nodi . . . 1517
Decommissionamento del sito . . . 1538
Rinominare la griglia, il sito o il nodo . . . 1561
Rinomina griglia, siti e nodi: Panoramica . . . 1561
Aggiungere o aggiornare i nomi visualizzati . . . 1565
Procedure dei nodi . . . 1570
Procedure dei nodi: Panoramica . . . 1570
Procedure di Server Manager . . . 1571
Procedure di riavvio, spegnimento e alimentazione . . . 1580
Procedure di rimappamento delle porte . . . 1592
Procedure di rete . . . 1596
Aggiornare le subnet per Grid Network . . . 1596
Configurare gli indirizzi IP . . . 1598
Aggiungere interfacce al nodo esistente . . . 1616
Configurare i server DNS . . . 1620
Modificare la configurazione DNS per un nodo griglia singolo . . . 1621
Gestire i server NTP . . . 1623
Ripristinare la connettività di rete per i nodi isolati . . . 1624
Procedure host e middleware . . . 1626
Linux: Migrazione del nodo grid al nuovo host . . . 1626
Manutenzione del nodo di archiviazione per il middleware TSM . . . 1629
VMware: Configurare la macchina virtuale per il riavvio automatico . . . 1634

Recovery o sostituzione dei nodi . . . 1635
Procedure di ripristino del nodo Grid: Panoramica . . . 1635
Avvertenze e considerazioni per il ripristino del nodo grid . . . 1635
Condizioni preliminari per il ripristino dei nodi di rete . . . 1636
Ordine di recovery del nodo in caso di guasto di un server che ospita più di un nodo griglia . . . 1636
Indirizzi IP per i nodi ripristinati . . . 1636
Raccogliere i materiali necessari per il ripristino dei nodi grid . . . 1636
Scaricare ed estrarre i file di installazione di StorageGRID . . . 1637
Selezionare la procedura di ripristino del nodo . . . 1643
Ripristino da guasti del nodo di storage . . . 1644
Recovery from Storage Node Failures: Panoramica . . . 1644
Recovery Storage Node Down per più di 15 giorni . . . 1645
Ripristinare il nodo storage dell'appliance . . . 1647
Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto . . . 1669
Ripristino in caso di guasto al disco di sistema . . . 1684
Ripristinare i dati degli oggetti utilizzando Grid Manager . . . 1704
Monitorare i lavori dei dati di riparazione . . . 1707
Ripristino da errori del nodo di amministrazione . . . 1709
Recovery from Admin Node Failures: Workflow . . . 1709
Ripristino da guasti principali del nodo di amministrazione . . . 1709
Ripristino da guasti non primari del nodo di amministrazione . . . 1717
Ripristino da guasti del nodo gateway . . . 1725
Recovery from Gateway Node Failures: Workflow . . . 1725
Sostituire il nodo gateway . . . 1726
Selezionare Avvia ripristino per configurare il nodo gateway . . . 1727
Ripristino da errori del nodo di archiviazione . . . 1728
Recovery from Archive Node Failures: Workflow . . . 1728
Sostituisci nodo archivio . . . 1730
Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di archiviazione . . . 1730
Ripristinare la connessione del nodo di archiviazione al cloud . . . 1732
Sostituire il nodo Linux . . . 1732
Sostituire il nodo Linux . . . 1732
Implementare nuovi host Linux . . . 1732
Ripristinare i nodi della griglia nell'host . . . 1733
Cosa succederà dopo: Se necessario, eseguire ulteriori passaggi di ripristino . . . 1738
Sostituire il nodo VMware . . . 1739
Sostituire il nodo guasto con l'appliance di servizi . . . 1740
Sostituisci nodo guasto con appliance di servizi: Panoramica . . . 1740
Installare l'appliance di servizi (solo modifica della piattaforma) . . . 1741
Preparazione dell'appliance per la reinstallazione (solo sostituzione della piattaforma) . . . 1741
Avviare l'installazione del software sull'appliance di servizi . . . 1742
Monitorare l'installazione delle appliance di servizi . . . 1746
Come il supporto tecnico recupera un sito . . . 1749
Come abilitare StorageGRID nel tuo ambiente . . . 1751
Come gestire StorageGRID utilizzando NetApp Console . . . 1752

Note legali 1753
Copyright 1753
Marchi 1753
Brevetti 1753
Direttiva sulla privacy 1753
Open source 1753

Documentazione di StorageGRID 11,8

Appliance StorageGRID

Passare a. "Documentazione sull'appliance StorageGRID" Per scoprire come installare, configurare e gestire le appliance di storage e servizi StorageGRID.

Note di rilascio

Ottenere informazioni specifiche sulla versione relative a problemi risolti e problemi noti.

Accedere al sito di supporto NetApp per "Visualizzare o scaricare un file PDF" Contenente le note di rilascio di StorageGRID 11,8.

Inizia subito con un sistema StorageGRID

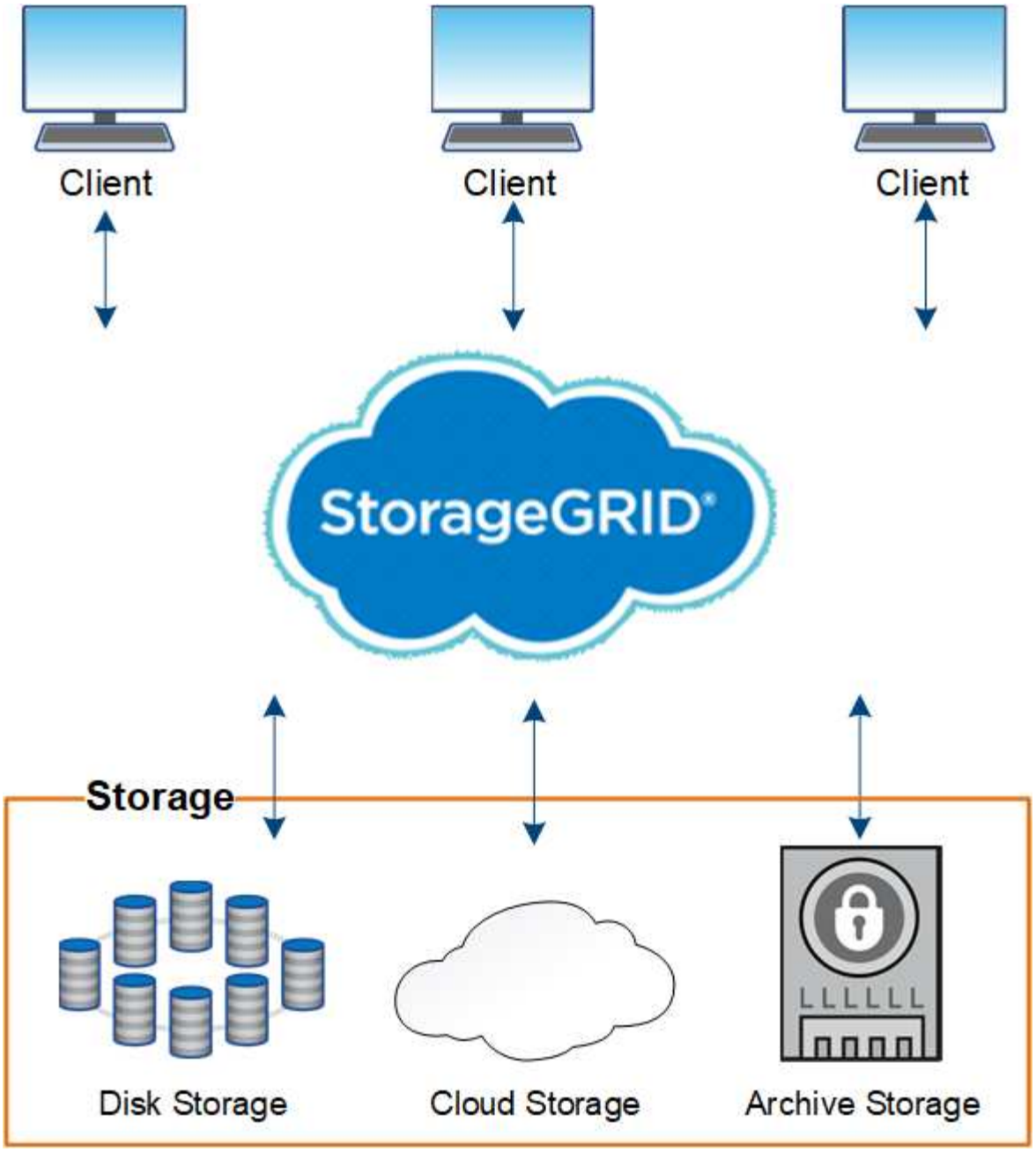
Scopri di più su StorageGRID

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.



Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura. Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità.

Vantaggi di StorageGRID

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

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

- 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 che gestiscono il ciclo di vita dei dati a livello di oggetto, personalizzando la posizione, la durata, le performance, i costi dei dati, e tempo di conservazione.
- 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.
    - Appliance 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 difona 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

Utilizza StorageGRID in una configurazione di cloud ibrido implementando la gestione dei

dati basata su policy per memorizzare gli oggetti nei pool di storage cloud, sfruttare i servizi della piattaforma StorageGRID e tiering dei dati da ONTAP a 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, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud 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.

È supportato anche lo storage di partner di terze parti, incluso lo storage su disco e nastro.

> 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 Simple Notification Service (Amazon SNS).
- 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 FabricPool

È possibile ridurre il costo dello storage ONTAP mediante il tiering dei dati su StorageGRID con FabricPool. FabricPool 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

- "Che cos'è il Cloud Storage Pool?"
- "Gestire i servizi della piattaforma"
- "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.

Vedere "descrizioni dei tipi di nodi della griglia".

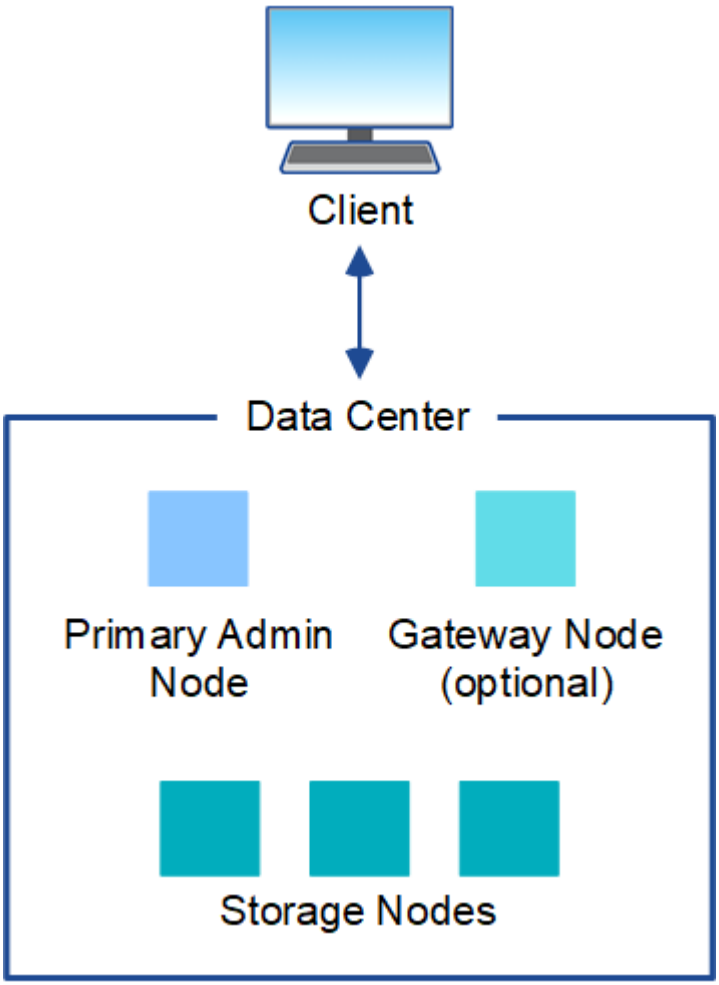
Per ulteriori informazioni sulla topologia della rete StorageGRID, sui requisiti e sulle comunicazioni Grid, consultare "Linee guida per il networking".

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

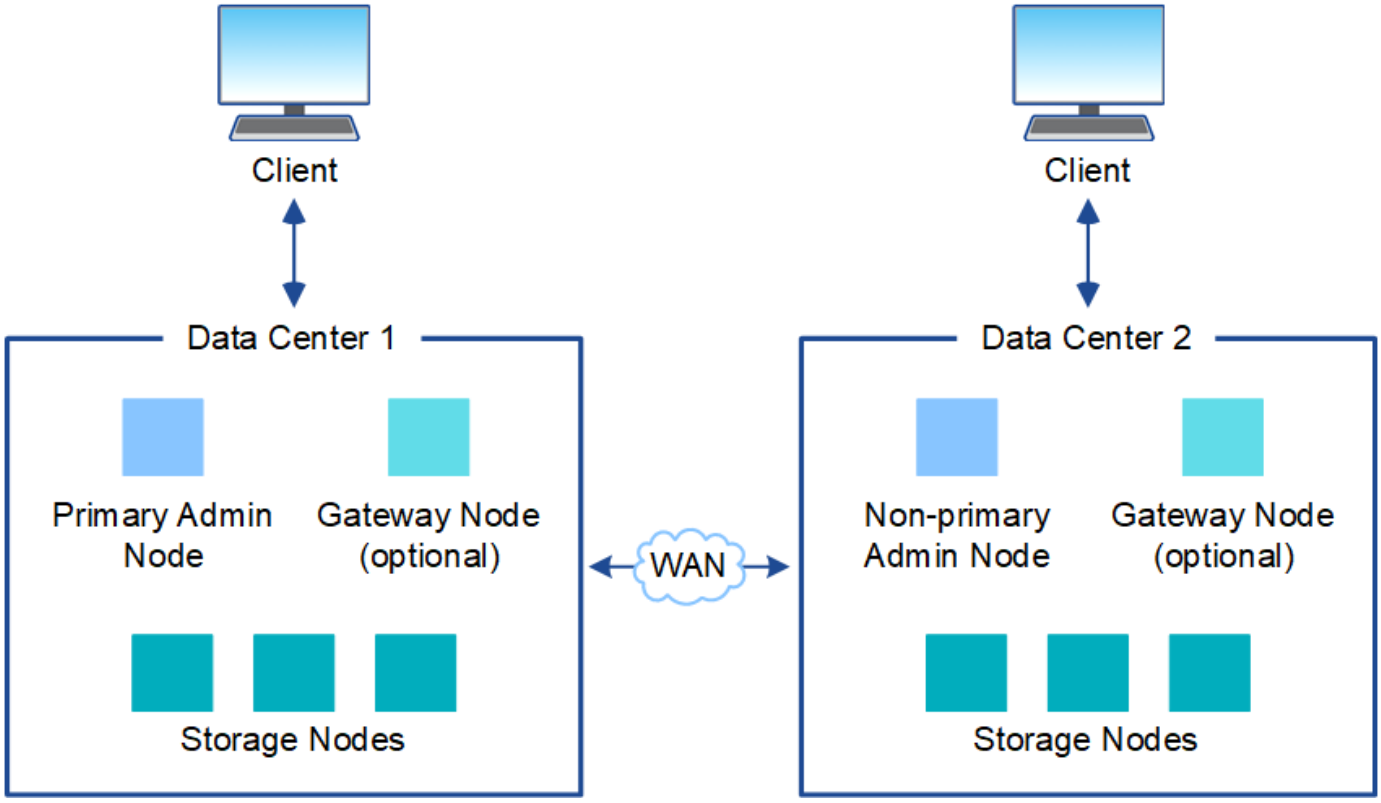
In un'implementazione con un singolo sito, l'infrastruttura e le operazioni del sistema StorageGRID sono centralizzate.



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.



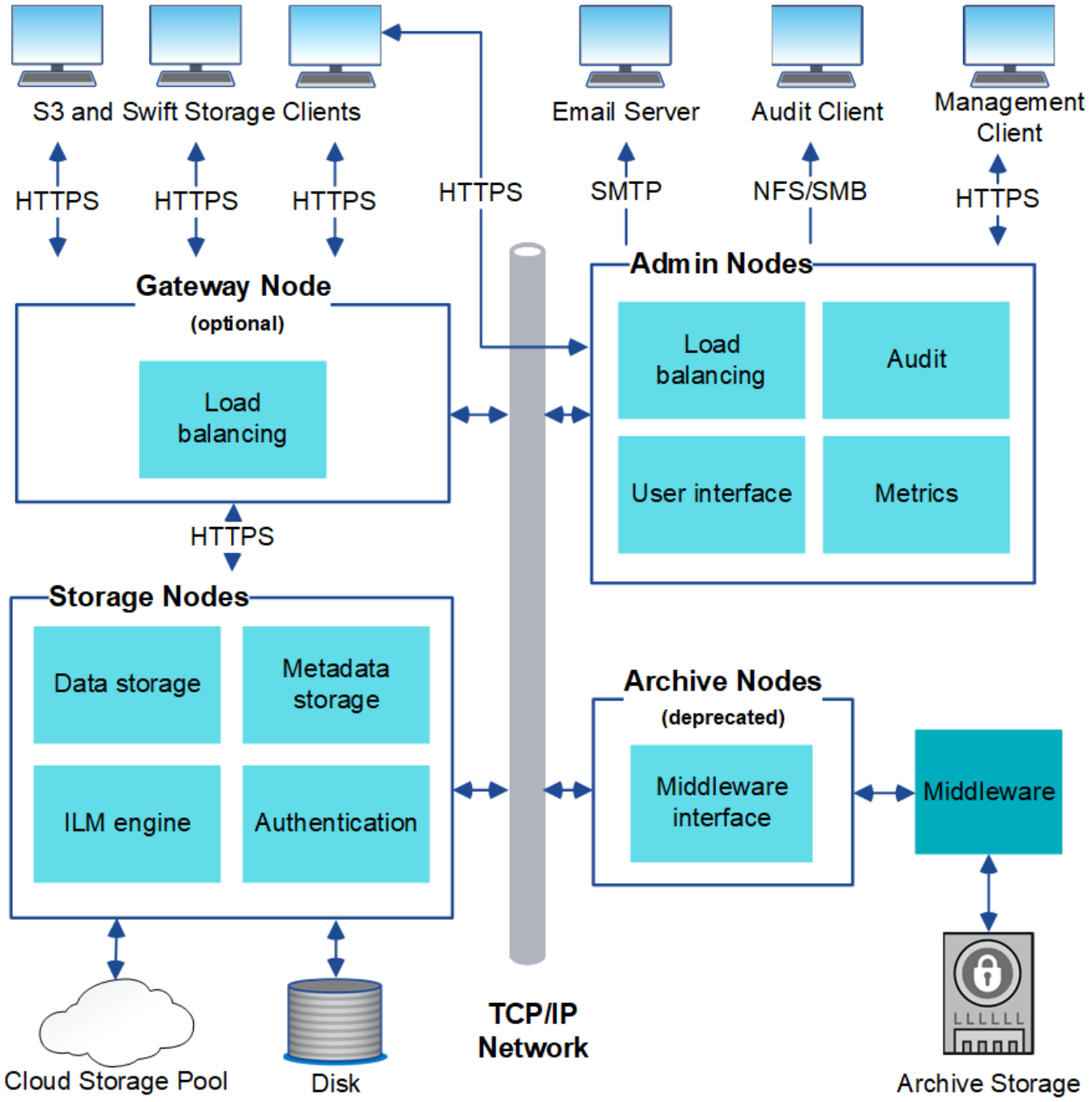
In un singolo data center possono inoltre esistere più siti logici per consentire l'utilizzo della replica distribuita e della codifica di cancellazione per aumentare la disponibilità e la resilienza.

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 oppure in pool di storage cloud, costituiti da bucket S3 esterni o container di storage Blob Azure.

Nodi e servizi Grid

Nodi di grid e servizi: Panoramica

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.

Tipi di nodi della griglia

Il sistema StorageGRID utilizza quattro tipi di nodi di rete:

Nodi di amministrazione

Fornire servizi di gestione quali configurazione, monitoraggio e logging 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.

Vedere "Che cos'è un nodo amministratore?"

Nodi di storage

Gestisci e archivia dati e metadati degli oggetti. Ciascun sito del sistema StorageGRID deve avere almeno tre nodi storage.

Vedere "Che cos'è un nodo di storage?"

Nodi gateway (opzionali)

Fornire un'interfaccia di 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.

Vedere "Che cos'è un nodo gateway?"

Nodi di archivio (deprecati)

Fornire un'interfaccia opzionale attraverso la quale archiviare i dati degli oggetti su nastro.

Vedere "Che cos'è un nodo di archiviazione?"

Nodi hardware e software

È possibile implementare nodi StorageGRID come nodi di appliance StorageGRID o come nodi basati sul software.

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.

Per ulteriori informazioni sulle appliance disponibili, vedere quanto segue:

- "Documentazione sull'appliance StorageGRID"
- "NetApp Hardware Universe"

Nodi basati su software

I nodi grid basati su software possono essere implementati come macchine virtuali VMware o all'interno di motori container su un host Linux.

- Macchina virtuale (VM) in VMware vSphere: Vedere "Installare StorageGRID su VMware".
- All'interno di un motore container su Red Hat Enterprise Linux: Vedere "Installare StorageGRID su Red Hat Enterprise Linux".
- All'interno di un motore container su Ubuntu o Debian: Vedere "Installare StorageGRID su Ubuntu o Debian".

Utilizzare "Tool di matrice di interoperabilità NetApp (IMT)" per determinare le versioni supportate.

Durante l'installazione iniziale di un nuovo nodo di storage basato su software, è possibile specificare che deve essere utilizzato solo per "memorizzazione dei metadati".

Servizi StorageGRID

Di seguito viene riportato un elenco completo dei servizi StorageGRID.

Servizio	Descrizione	Posizione
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.	Servizio di bilanciamento del carico su nodi amministrativi e nodi gateway
ADC (Administrative Domain Controller)	Mantiene le informazioni sulla topologia, fornisce servizi di autenticazione e risponde alle query provenienti dai servizi LDR e CMN.	Almeno tre nodi di archiviazione contenenti il servizio ADC in ciascun sito
AMS (Audit Management System)	Monitora e registra tutti gli eventi e le transazioni di sistema verificati in un file di log di testo.	Nodi di amministrazione
ARCO (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.	Nodi di archiviazione
Cassandra Reaper	Esegue la riparazione automatica dei metadati degli oggetti.	Nodi di storage

Servizio	Descrizione	Posizione
Servizio a pezzi	Gestisce i dati con codifica erasure e i frammenti di parità.	Nodi di storage
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.	Nodo amministratore primario
DDS (archiviazione dati distribuita)	Si interfaccia con il database Cassandra per gestire i metadati degli oggetti.	Nodi di storage
DMV (Data Mover)	Sposta i dati negli endpoint cloud.	Nodi di storage
Dynamic IP (dinamico)	Monitora la griglia per verificare la presenza di modifiche IP dinamiche e aggiorna le configurazioni locali.	Tutti i nodi
Grafana	Utilizzato per la visualizzazione delle metriche in Grid Manager.	Nodi di amministrazione
Alta disponibilità	Gestisce gli IP virtuali ad alta disponibilità sui nodi configurati nella pagina gruppi ad alta disponibilità. Questo servizio è anche noto come servizio keepalived.	Nodi Admin e Gateway
Identità (idnt)	Consente di federare le identità degli utenti da LDAP e Active Directory.	Nodi di storage che utilizzano il servizio ADC
Arbitro lambda	Gestisce le richieste S3 Select SelectObjectContent.	Tutti i nodi
Bilanciamento del carico (nginx-gw)	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. Questo servizio è noto anche come servizio nginx-gw.	Nodi Admin e Gateway
LDR (router di distribuzione locale)	Gestisce lo storage e il trasferimento dei contenuti all'interno della griglia.	Nodi di storage
Daemon di controllo del servizio informazioni MISCd	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.	Tutti i nodi

Servizio	Descrizione	Posizione
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.	Tutti i nodi
nginx-gw	Alimenta il servizio Load Balancer.	Nodi Admin e Gateway
NMS (Network Management System, sistema di gestione della rete)	Alimenta le opzioni di monitoraggio, reporting e configurazione visualizzate tramite Grid Manager.	Nodi di amministrazione
Persistenza	Gestisce i file sul disco root che devono persistere durante un riavvio.	Tutti i nodi
Prometheus	Raccoglie le metriche delle serie temporali dai servizi su tutti i nodi.	Nodi di amministrazione
RSM (macchina a stato replicato)	Garantisce che le richieste di servizio della piattaforma vengano inviate ai rispettivi endpoint.	Nodi di storage che utilizzano il servizio ADC
SSM (Server Status Monitor)	Monitora le condizioni dell'hardware e invia report al servizio NMS.	Un'istanza è presente su ogni nodo della griglia
Raccoglitore di tracce	Esegue la raccolta di tracce per raccogliere informazioni da utilizzare per il supporto tecnico. Il servizio di raccolta tracce utilizza il software open source Jaeger.	Nodi di amministrazione

Che cos'è un nodo amministratore?

I nodi di amministrazione forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. I nodi di amministrazione possono anche essere utilizzati per bilanciare il carico del traffico dei client S3 e Swift. Ogni grid deve avere un nodo di amministrazione primario e può avere un numero qualsiasi di nodi di amministrazione non primari per la ridondanza.

Differenze tra i nodi amministrativi primari e non primari

Quando si accede a Grid Manager o al tenant Manager, si sta effettuando la connessione a un nodo amministratore. È possibile connettersi a qualsiasi nodo amministratore e ciascun nodo amministratore visualizza una vista simile del sistema StorageGRID. Tuttavia, il nodo amministrativo primario fornisce più funzionalità rispetto ai nodi amministrativi non primari. Ad esempio, la maggior parte delle procedure di manutenzione deve essere eseguita dai nodi amministrativi primari.

La tabella riassume le capacità dei nodi amministrativi primari e non primari.

Funzionalità	Nodo amministratore primario	Nodo amministrativo non primario
Include il AMS servizio	Sì	Sì
Include il CMN servizio	Sì	No
Include il NMS servizio	Sì	Sì
Include il Prometheus servizio	Sì	Sì
Include il SSM servizio	Sì	Sì
Include il Bilanciamento del carico e. Alta disponibilità servizi	Sì	Sì
Supporta Management Application Program Interface (api di gestione)	Sì	Sì
Può essere utilizzato per tutte le attività di manutenzione relative alla rete, ad esempio la modifica dell'indirizzo IP e l'aggiornamento dei server NTP	Sì	No
Può eseguire il ribilanciamento EC dopo l'espansione del nodo storage	Sì	No
Può essere utilizzato per la procedura di ripristino del volume	Sì	Sì
Può raccogliere file di registro e dati di sistema da uno o più nodi	Sì	No
Invia notifiche di avviso, pacchetti AutoSupport e trap SNMP e informa	Sì. Agisce come mittente preferito.	Sì. Funge da mittente di standby.

nodo amministratore mittente preferito

Se la distribuzione StorageGRID include più nodi amministrativi, il nodo amministrativo primario è il mittente preferito per le notifiche di avviso, i pacchetti AutoSupport, le trap e le notifiche SNMP e le notifiche di allarme legacy.

Nelle normali operazioni di sistema, solo il mittente preferito invia le notifiche. Tuttavia, tutti gli altri nodi Admin monitorano il mittente preferito. Se viene rilevato un problema, gli altri nodi Admin fungono da *mittenti di standby*.

In questi casi potrebbero essere inviate più notifiche:

- Se i nodi Admin diventano "islanded" l'uno dall'altro, sia il mittente preferito che i mittenti in standby

tenteranno di inviare notifiche e potrebbero essere ricevute più copie delle notifiche.

- Se il mittente in standby rileva problemi con il mittente preferito e inizia a inviare notifiche, il mittente preferito potrebbe riacquistare la capacità di inviare notifiche. In questo caso, potrebbero essere inviate notifiche duplicate. Il mittente in standby interrompe l'invio di notifiche quando non rileva più errori sul mittente preferito.

> Quando si testano i pacchetti AutoSupport, tutti i nodi amministrativi inviano il test. Quando si verificano le notifiche di avviso, è necessario accedere a ogni nodo amministratore per verificare la connettività.

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
Audit Management System (AMS)	Tiene traccia dell'attività e degli eventi del sistema.
nodo di gestione della configurazione (CMN)	Gestisce la configurazione a livello di sistema.
[[alta disponibilità]]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]]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.
Management Application Program Interface (api di gestione)	Elabora le richieste provenienti dall'API Grid Management e dall'API Tenant Management.
Network Management System (NMS)	Fornisce funzionalità per Grid Manager.
Prometheus	Raccoglie e memorizza le metriche delle serie temporali dai servizi su tutti i nodi.
Server Status Monitor (SSM)	Monitora il sistema operativo e l'hardware sottostante.

Che cos'è un nodo di storage?

I nodi di storage gestiscono e memorizzano i dati e i metadati degli oggetti. I nodi di storage includono i servizi e i processi necessari per memorizzare, spostare, verificare e recuperare dati e metadati degli oggetti su disco.

Ciascun sito del sistema StorageGRID deve avere almeno tre nodi storage.

Tipi di nodi storage

Tutti i nodi storage installati prima di StorageGRID 11,8 memorizzano oggetti e metadati per tali oggetti. A partire da StorageGRID 11,8, è possibile scegliere il tipo di nodo di storage per i nuovi nodi di storage basati su software:

Nodi di storage a oggetti e metadati

Per impostazione predefinita, tutti i nuovi nodi di storage installati in StorageGRID 11,8 memorizzeranno oggetti e metadati.

Nodi di storage solo metadati (solo nodi basati su software)

È possibile specificare che un nuovo nodo di storage basato su software venga utilizzato per memorizzare solo i metadati. È inoltre possibile aggiungere un nodo di storage basato su software e solo sui metadati al sistema StorageGRID durante l'espansione del sistema StorageGRID.

> È possibile selezionare il tipo di nodo di storage solo quando si installa inizialmente il nodo basato su software o quando si installa il nodo basato su software durante l'espansione del sistema StorageGRID. Non è possibile modificare il tipo una volta completata l'installazione del nodo.

In genere non è necessario installare un nodo di soli metadati. Tuttavia, l'utilizzo di un nodo di archiviazione esclusivamente per i metadati può essere utile se il grid memorizza un numero molto elevato di piccoli oggetti. L'installazione di una capacità di metadati dedicata fornisce un migliore equilibrio tra lo spazio necessario per un numero molto elevato di piccoli oggetti e lo spazio necessario per i metadati per tutti questi oggetti.

Le risorse dei nodi di solo metadati basate su software devono corrispondere alle risorse dei nodi di storage esistenti. Ad esempio:

- Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:
  - 128 GB DI RAM
  - CPU a 8 core
  - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)
- Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuale con 24 GB di RAM, 8 core CPU e 3 TB o 4TB di memorizzazione di metadati, i nodi basati solo sui metadati del software devono utilizzare risorse simili (24 GB di RAM, 8 core CPU e 4TB di memorizzazione di metadati (rangedb/0).

Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve almeno StorageGRID corrispondere ai nodi storage dei siti StorageGRID esistenti e alle nuove risorse del sito.

Quando si installa un grid con nodi solo metadati basati su software, il grid deve anche contenere un numero minimo di nodi per lo storage a oggetti:

- Per un grid a sito singolo, vengono configurati almeno due nodi storage per oggetti e metadati.
- Per un grid multisito, per gli oggetti e i metadati viene configurato almeno un nodo di storage per sito.

I nodi di storage basati su software visualizzano un'indicazione di solo metadati per ogni nodo solo metadati in tutte le pagine che elencano il tipo di nodo di storage.

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. **Dettagli** Il servizio ADC (Administrative Domain Controller) autentica i nodi della griglia e le relative connessioni tra loro. Il servizio ADC è ospitato su un minimo di tre nodi di storage in un sito. Il servizio ADC mantiene le informazioni sulla topologia, inclusa la posizione e la disponibilità dei servizi. Quando un nodo della griglia richiede informazioni da un altro nodo della griglia o un'azione da eseguire da un altro nodo della griglia, contatta un servizio ADC per trovare il nodo della griglia migliore per elaborare la sua richiesta. Inoltre, il servizio ADC conserva una copia dei pacchetti di configurazione della distribuzione StorageGRID, consentendo a qualsiasi nodo di rete di recuperare le informazioni di configurazione correnti. Per facilitare le operazioni distribuite e islanded, ciascun servizio ADC sincronizza certificati, bundle di configurazione e informazioni sui servizi e sulla topologia con gli altri servizi ADC nel sistema StorageGRID. In generale, tutti i nodi di rete mantengono una connessione ad almeno un servizio ADC. In questo modo, i nodi della griglia accedono sempre alle informazioni più recenti. Quando i nodi di rete si connettono, memorizzano nella cache i certificati di altri nodi di rete, consentendo ai sistemi di continuare a funzionare con i nodi di rete noti anche quando un servizio ADC non è disponibile. I nuovi nodi di rete possono stabilire connessioni solo utilizzando un servizio ADC. La connessione di ciascun nodo di rete consente al servizio ADC di raccogliere informazioni sulla topologia. Queste informazioni sul nodo della griglia includono il carico della CPU, lo spazio su disco disponibile (se dotato di storage), i servizi supportati e l'ID del sito del nodo della griglia. Altri servizi richiedono al servizio ADC informazioni sulla topologia tramite query sulla topologia. Il servizio ADC risponde a ogni richiesta con le informazioni più recenti ricevute dal sistema StorageGRID.
Cassandra	Memorizza e protegge i metadati degli oggetti.

Servizio	Funzione dei tasti
Cassandra Reaper	Esegue la riparazione automatica dei metadati degli oggetti.
Chunk	Gestisce i dati con codifica erasure e i frammenti di parità.
Data Mover (dmv)	Sposta i dati nei pool di cloud storage.
Data store distribuito (DDS)	Monitora lo storage dei metadati degli oggetti. **Dettagli** Ogni nodo di storage include il servizio DDS (Distributed Data Store). Questo servizio si interfaccia con il database Cassandra per eseguire attività in background sui metadati degli oggetti archiviati nel sistema StorageGRID. Il servizio DDS tiene traccia del numero totale di oggetti acquisiti nel sistema StorageGRID e del numero totale di oggetti acquisiti attraverso ciascuna delle interfacce supportate dal sistema (S3 o Swift).
Identità (idnt)	Consente di federare le identità degli utenti da LDAP e Active Directory.

Servizio	Funzione dei tasti
Router di distribuzione locale (LDR)	Elabora le richieste del protocollo di storage a oggetti e gestisce i dati degli oggetti su disco.

Servizio	Funzione dei tasti
Replicated state Machine (RSM)	Garantisce che le richieste di servizi della piattaforma S3 vengano inviate ai rispettivi endpoint.
Server Status Monitor (SSM)	Monitora il sistema operativo e l'hardware sottostante.

StorageGRID gestendo i carichi di trasferimento dei dati e le funzioni di traffico dei dati.

Il servizio LDR gestisce le seguenti attività:

- Query
- Attività ILM (Information Lifecycle Management)
- Eliminazione di oggetti
- Storage di dati a oggetti
- Trasferimenti di dati a oggetti da un altro servizio LDR (nodo di storage)
- Gestione dello storage dei dati
- Interfacce di protocollo (S3 e Swift)

Il servizio LDR mappa inoltre ogni oggetto S3 e Swift al suo UUID univoco.

Archivi di oggetti

Lo storage dei dati sottostante di un servizio LDR è diviso in un numero fisso di archivi a oggetti (noti anche come volumi di storage). Ogni archivio di oggetti è un punto di montaggio separato.

Gli archivi di oggetti in un nodo di storage sono identificati da un numero esadecimale compreso tra 0000 e 002F, noto come ID del volume. Lo spazio è riservato nel primo archivio di oggetti (volume 0) per i metadati degli oggetti in un database Cassandra; qualsiasi spazio rimanente in tale volume viene utilizzato per i dati degli oggetti. Tutti gli altri archivi di oggetti vengono utilizzati esclusivamente per i dati degli oggetti, che includono copie replicate e frammenti con codifica di cancellazione.

Che cos'è un nodo gateway?

Nodi di gateway offrono un interfaccia di bilanciamento del carico dedicata che le applicazioni client S3 e Swift possono utilizzare per la connessione a StorageGRID. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo il carico di lavoro tra più nodi di storage. I nodi del gateway sono opzionali.

Il servizio di bilanciamento del carico è fornito su tutti i nodi amministrativi e su tutti i nodi gateway. Esegue la terminazione TLS (Transport Layer Security) delle richieste client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage. Il servizio di 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 configurare uno o più endpoint di bilanciamento del carico per definire la porta e il protocollo di rete (HTTPS o HTTP) utilizzati dalle richieste client in entrata e in uscita per accedere ai servizi di bilanciamento del carico sui nodi Gateway e Admin. L'endpoint di bilanciamento del carico definisce anche il tipo di client (S3 o Swift), la modalità di binding e, facoltativamente, un elenco di tenant consentiti o bloccati. Vedere "Considerazioni per il bilanciamento del carico".

Se necessario, puoi raggruppare le interfacce di rete di più nodi di gateway e nodi amministrativi in un gruppo ad alta disponibilità (ha). In caso di guasto dell'interfaccia attiva nel gruppo di ha, un'interfaccia di backup può gestire il workload dell'applicazione client. Vedere "Gestire i gruppi ad alta disponibilità (ha)"

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
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.

oggetti".

Che cos'è un nodo di archiviazione?

Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura.

> Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura. Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità.
>
> Anche l'opzione Cloud Tiering - Simple Storage Service (S3) è obsoleta. Se si utilizza attualmente un nodo di archiviazione con questa opzione, "Migrare gli oggetti in un pool di storage cloud" invece.
>
> Inoltre, è necessario rimuovere i nodi di archiviazione dai criteri ILM attivi in StorageGRID 11,7 o versioni precedenti. La rimozione dei dati degli oggetti memorizzati nei nodi di archiviazione semplificherà gli aggiornamenti futuri. Vedere "Utilizzo delle regole ILM e delle policy ILM".

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.

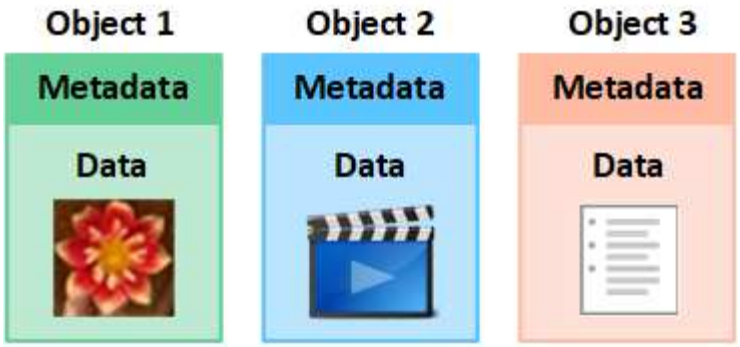
Come StorageGRID gestisce i dati

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.



Che cos'è un dato a oggetti?

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

Che cos'è il metadata a oggetti?

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".

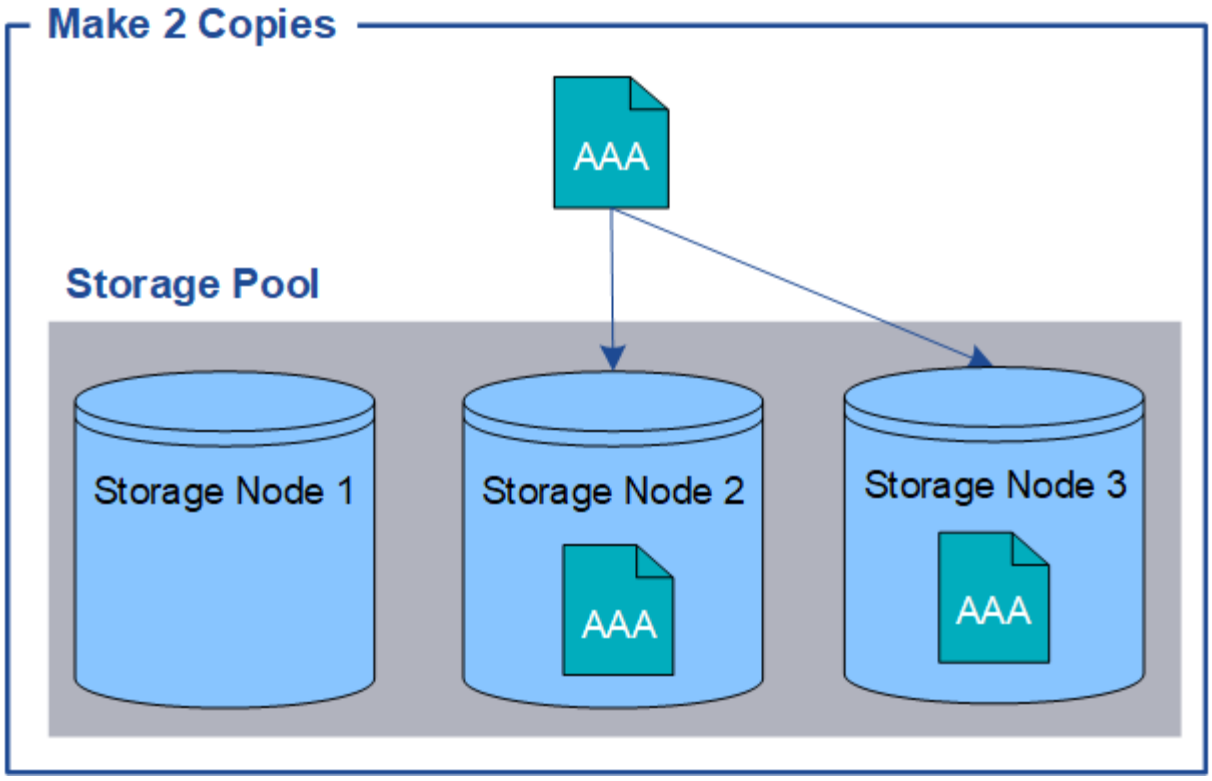
Come vengono protetti i dati a oggetti?

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.

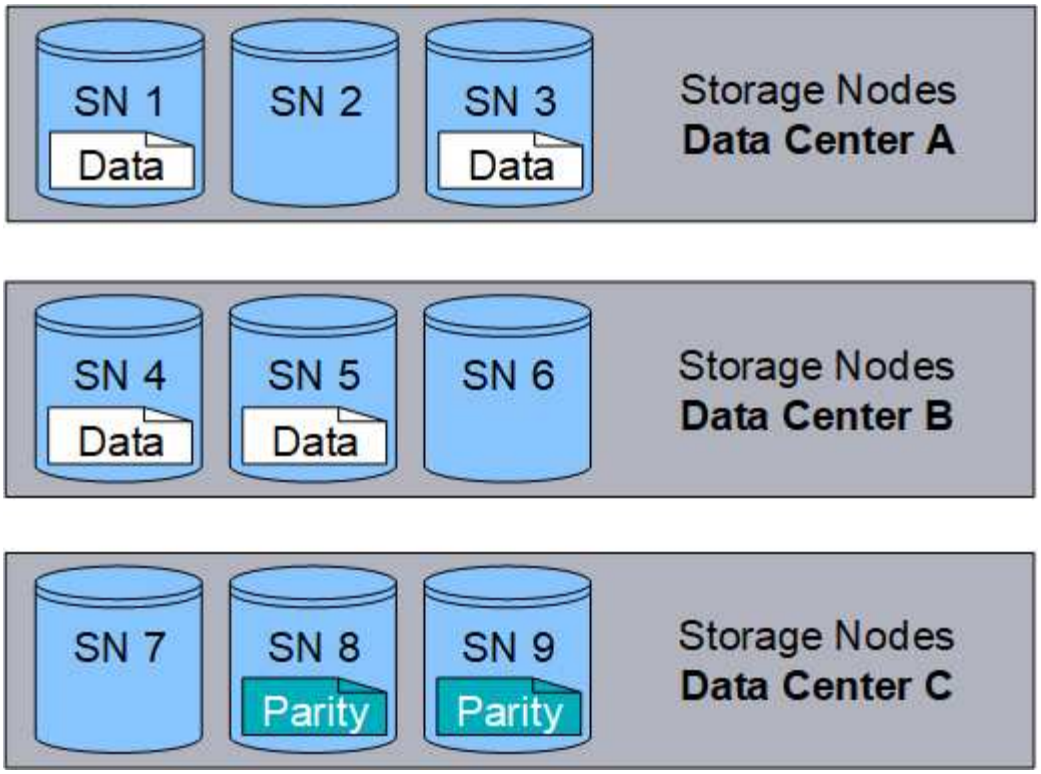
Nell'esempio seguente, la regola Make 2 copies specifica che due copie replicate di ciascun oggetto devono essere collocate in un pool di storage che contiene tre nodi di storage.



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 riassemblato 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

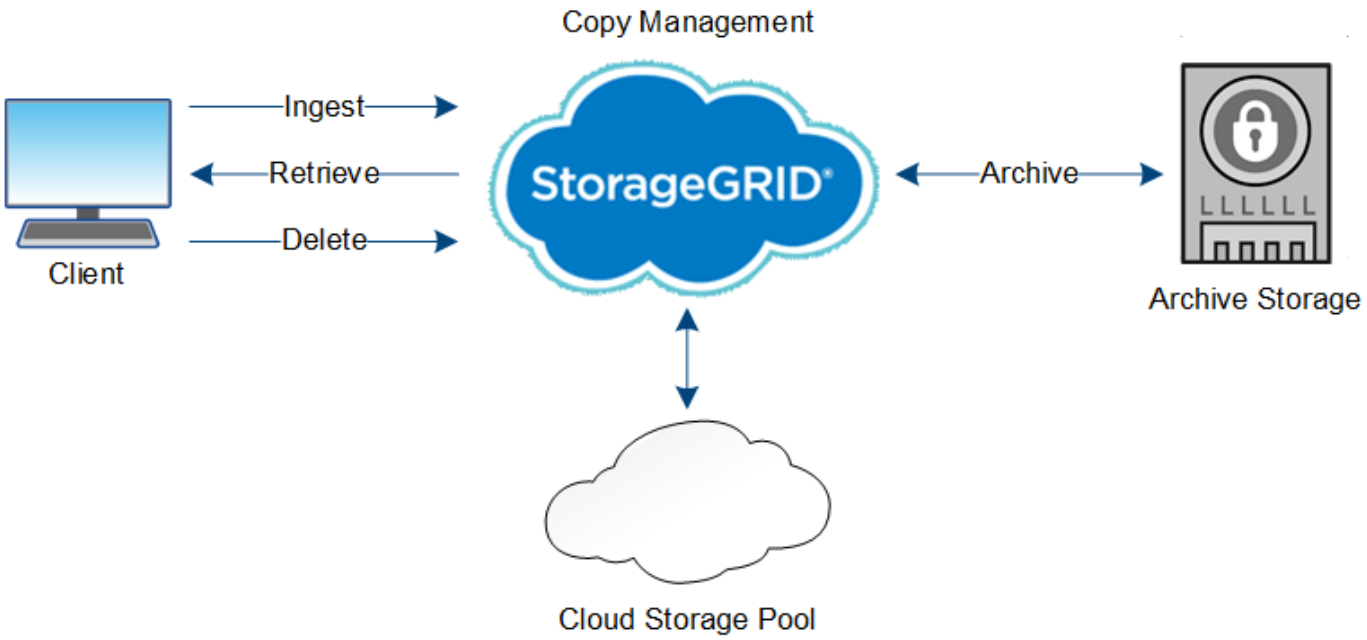
- "Gestire gli oggetti con ILM"
- "Utilizza la gestione del ciclo di vita delle informazioni"

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 con erasure coding in StorageGRID, come descritto dalle regole ILM nei criteri ILM attivi. 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

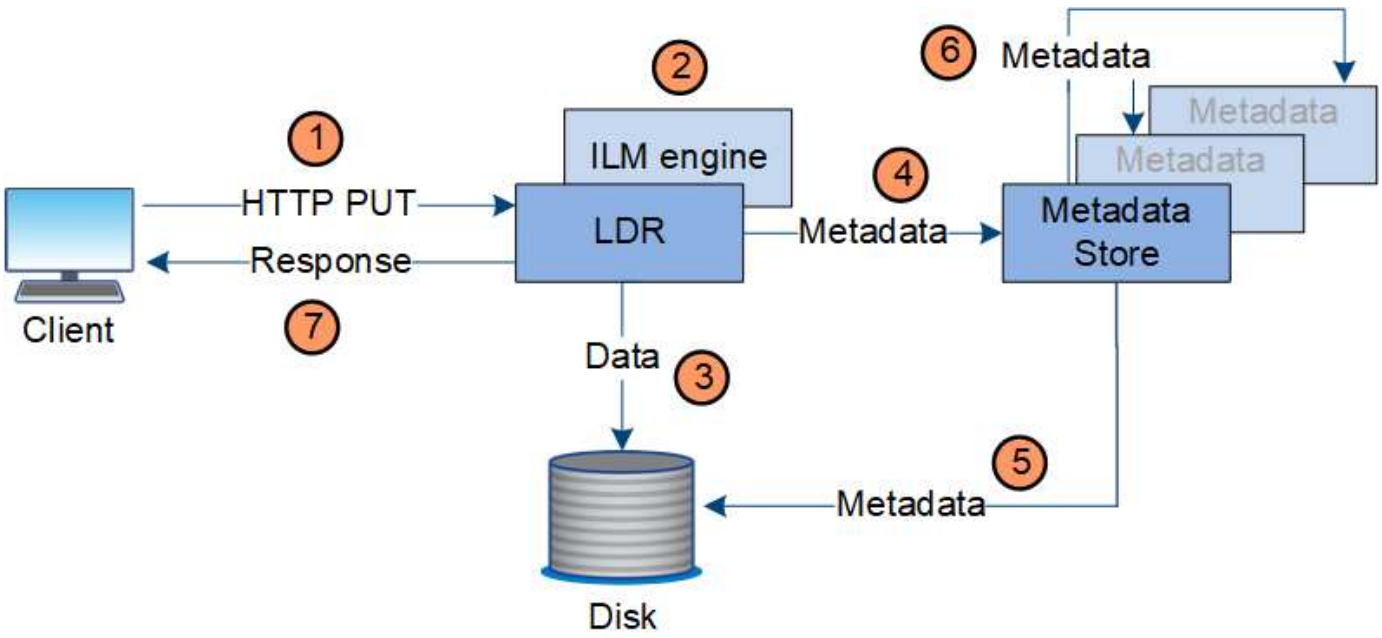
- "Gestire gli oggetti con ILM"
- "Utilizza la gestione del ciclo di vita delle informazioni"

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 sottoposta a erasure coding. (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 sono gestiti dalle policy ILM attive e dalle regole ILM associate. Le regole ILM eseguono copie replicate o con erasure coding per proteggere i dati degli oggetti da eventuali perdite.

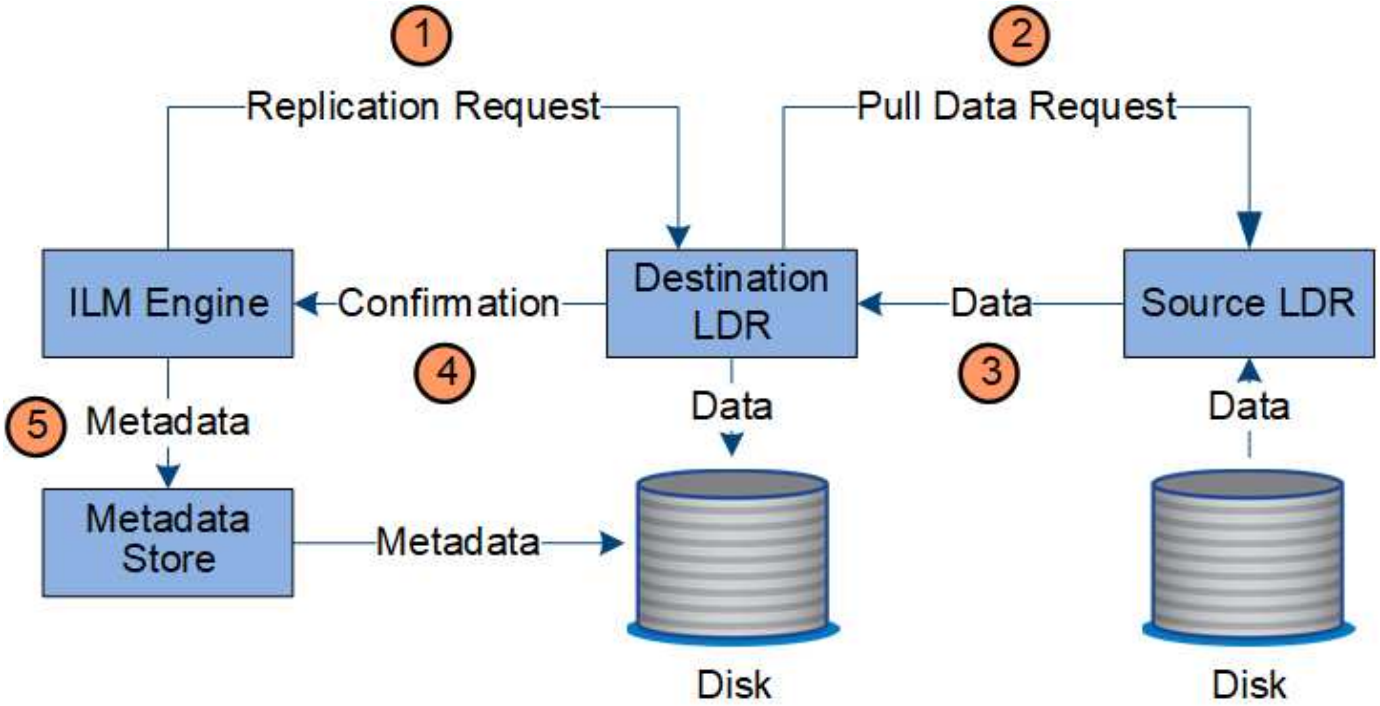
Potrebbero essere necessari diversi tipi o posizioni di copie di oggetti in momenti diversi della vita dell’oggetto. Le regole ILM vengono periodicamente valutate per garantire che gli oggetti vengano posizionati come richiesto.

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.

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.

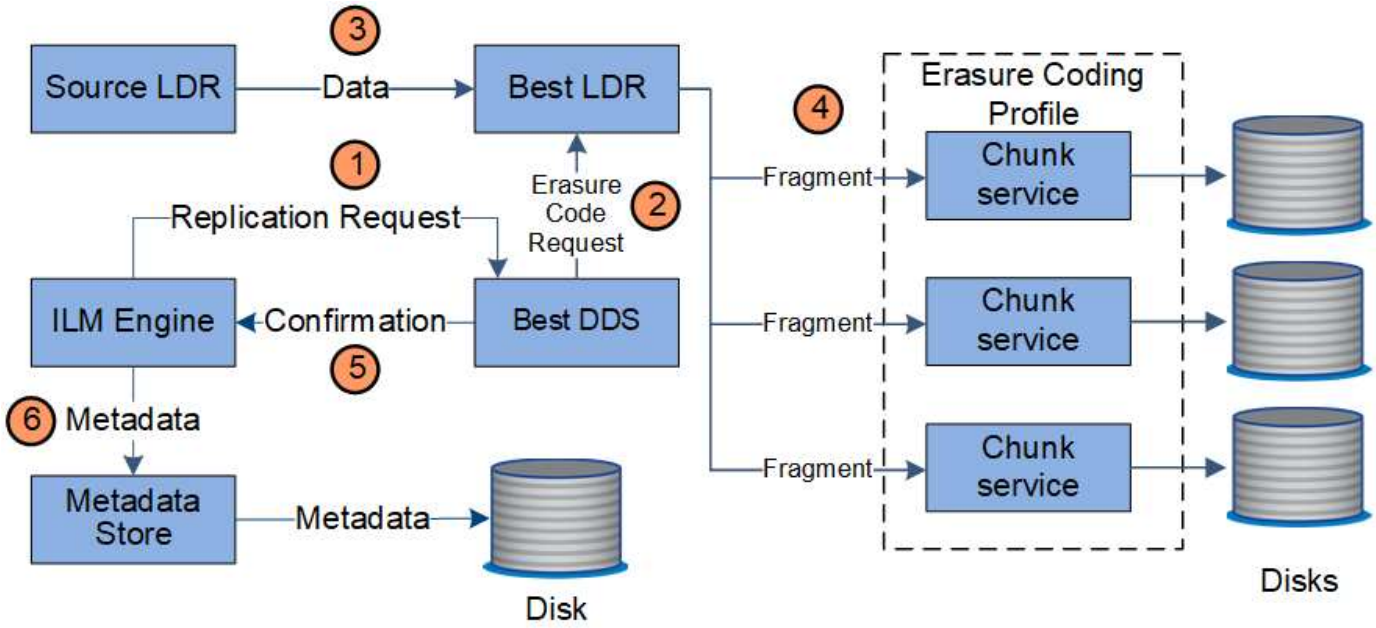


1. Il motore ILM interroga il servizio ADC per determinare il servizio LDR di destinazione migliore all'interno del pool di storage specificato dalla regola ILM. Quindi, invia al servizio LDR un comando per avviare la replica.
2. Il servizio LDR di destinazione interroga il servizio ADC per la migliore 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 creare copie codificate dei dati degli oggetti, lo schema di erasure coding applicabile suddivide i dati degli oggetti in fragment di dati e parità e distribuisce tali fragment nei nodi di storage configurati nel profilo di erasure coding.

Il motore ILM, che è un componente del servizio LDR, controlla l'erasure coding e garantisce che il profilo di erasure coding venga applicato ai dati dell'oggetto.

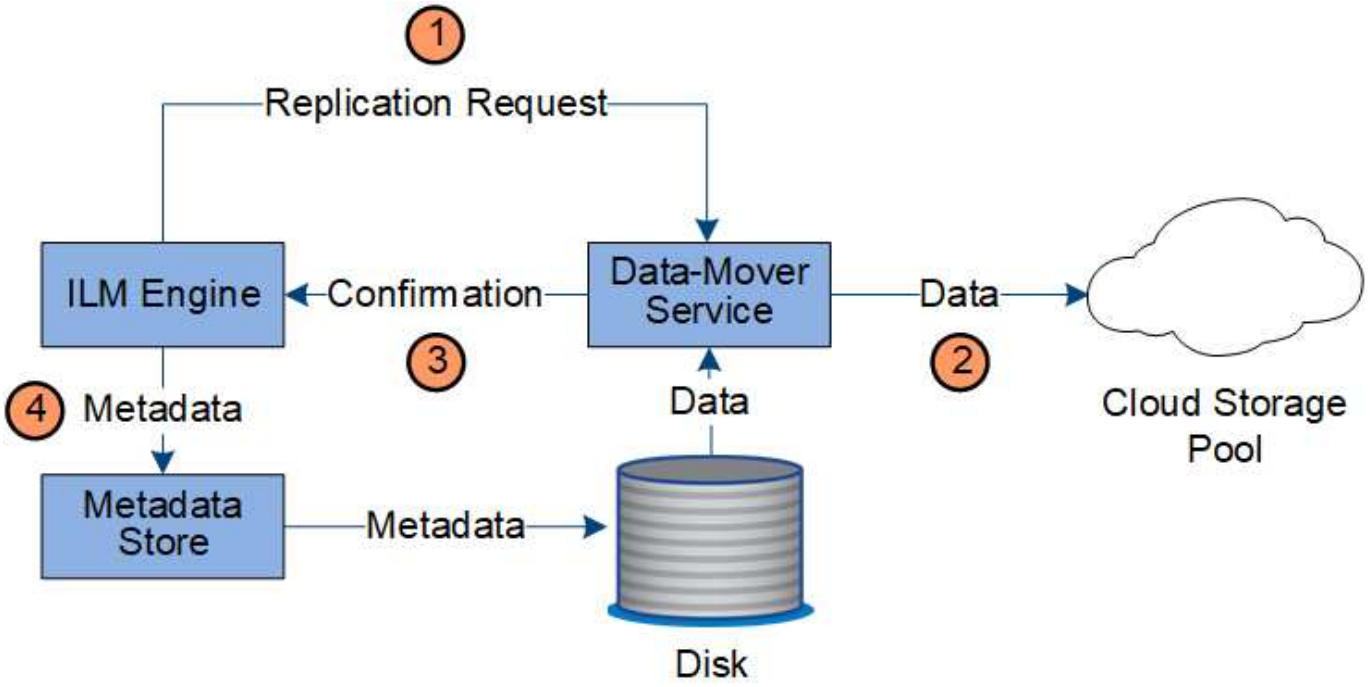


1. Il motore ILM interroga il servizio ADC per determinare quale servizio DDS può eseguire al meglio l'operazione di erasure coding. Una volta stabilito, il motore ILM invia una richiesta di "avvio" a tale servizio.
2. Il servizio DDS richiede a un LDR di eseguire la cancellazione del codice dei dati dell'oggetto.
3. Il servizio LDR di origine invia una copia al servizio LDR selezionato per la cancellazione del codice.
4. Dopo aver creato il numero appropriato di parità e frammenti di dati, il servizio LDR distribuisce questi frammenti nei nodi di storage (servizi Chunk) che costituiscono il pool di storage del profilo di erasure coding.
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.

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



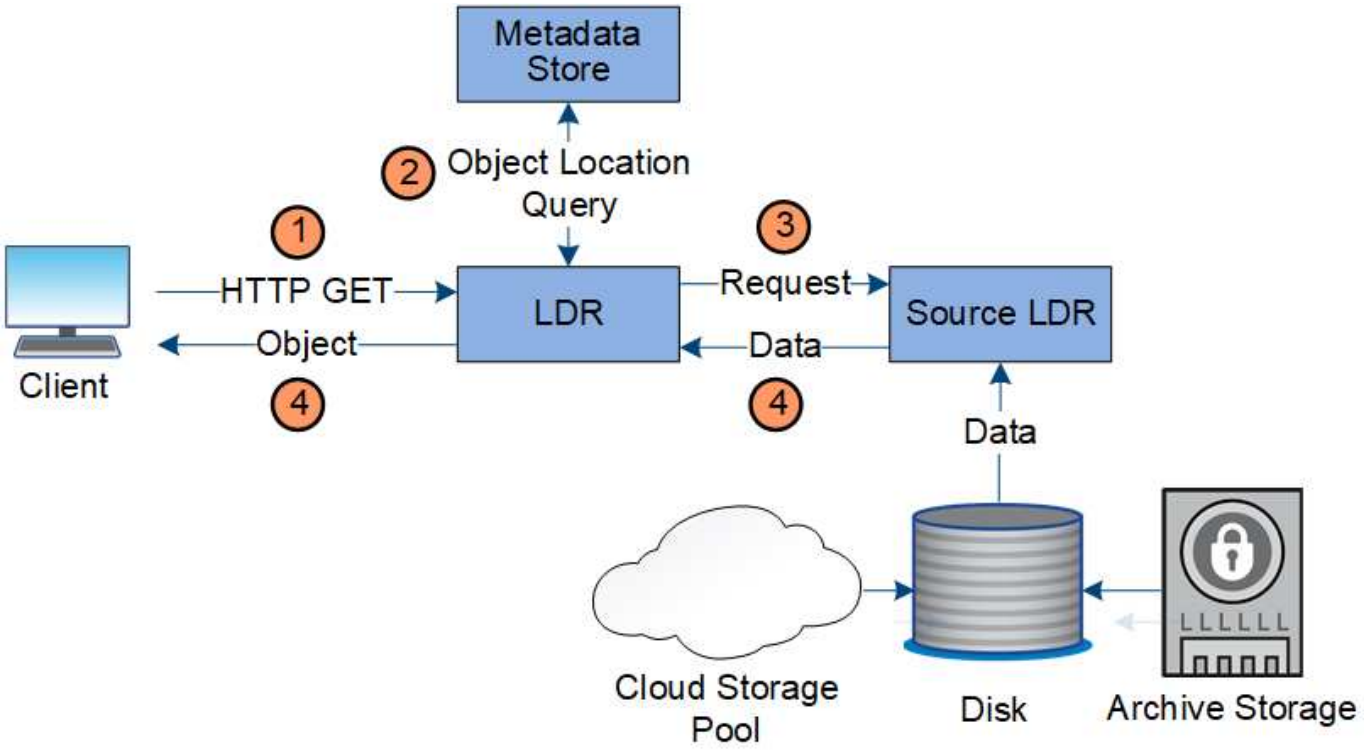
1. Il motore ILM seleziona un servizio Data Mover da replicare nel Cloud Storage Pool.
2. Il servizio Data Mover invia i dati dell'oggetto al Cloud Storage Pool.
3. Il servizio Data Mover notifica al motore ILM che i dati dell'oggetto sono stati memorizzati.
4. Il motore ILM aggiorna l'archivio di metadati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

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 nel Tier Azure Archive, l'applicazione client deve emettere una richiesta S3 RestoreObject per ripristinare una copia recuperabile in 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 soggetta a blocco legale non può essere eliminata da 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 blocco oggetti S3 abilitato vengono conservati da ILM "per sempre". 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.

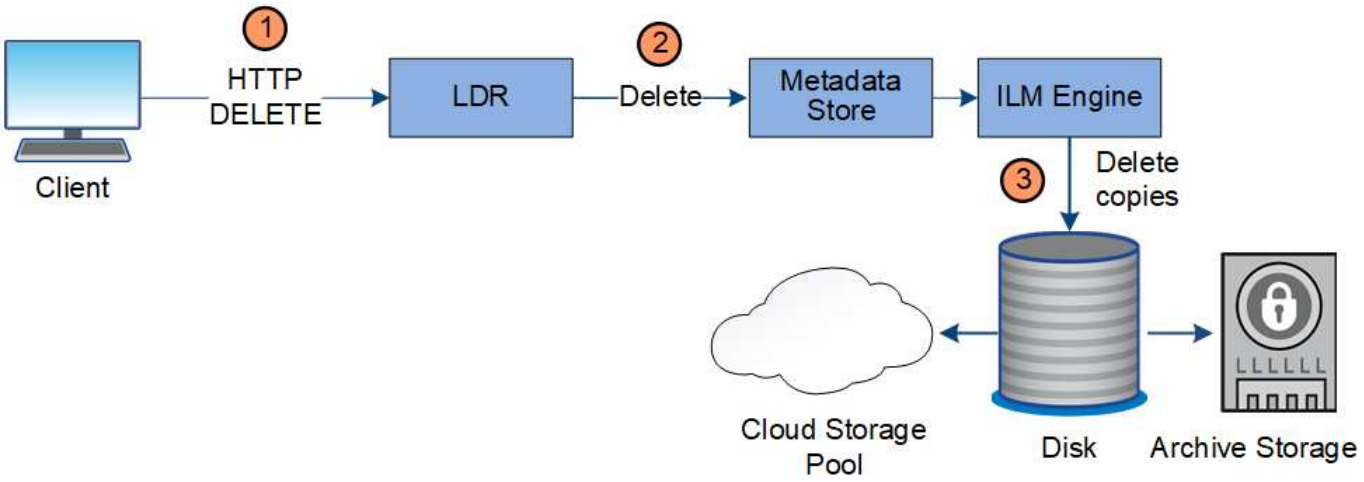
- Se i client S3 applicano al bucket una data di conservazione predefinita, non devono specificare una data di conservazione per ciascun oggetto.

- **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.
- **Elimina oggetti nel bucket**: Gli utenti di tenant Manager possono utilizzare questa opzione per rimuovere in modo permanente tutte le copie degli oggetti e delle versioni degli oggetti nei bucket selezionati 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.

> Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti che corrispondono al filtro del ciclo di vita. Di conseguenza, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni ILM per il posizionamento dell'oggetto.

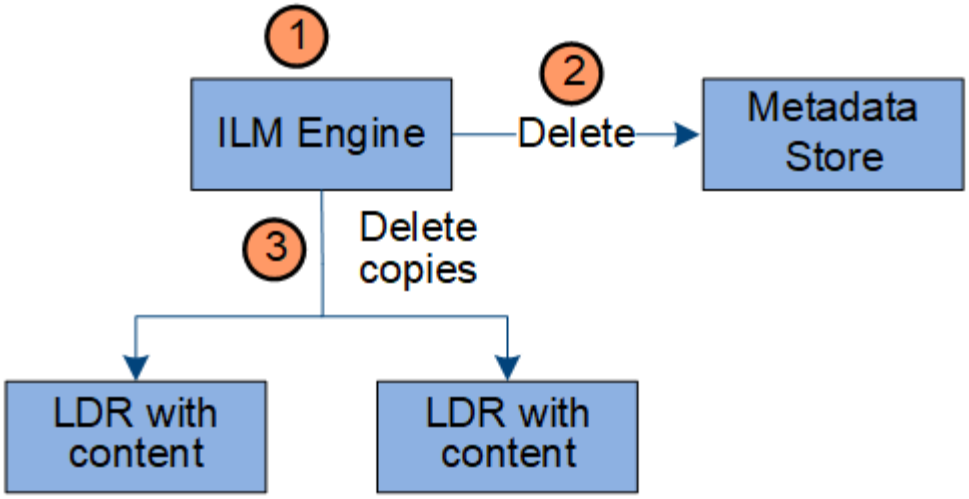
Vedere "Modalità di eliminazione degli oggetti" per ulteriori informazioni.

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.

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 il comportamento di acquisizione di 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.

Una griglia ha solo una policy attiva alla volta. Un criterio può contenere più regole.

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. È possibile eseguire la replica o l'erasure coding.
- Per le copie replicate, il numero di copie eseguite.
- Per le copie con erasure coding, è stato 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.

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applicano solo agli oggetti appartenenti al tenant A.
- Eseguire due copie replicate di tali oggetti e memorizzare ciascuna copia in un sito diverso.
- Conserva le due copie "per sempre", 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.
- Utilizzare l'opzione bilanciato 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

Le policy ILM attive del sistema StorageGRID controllano il posizionamento, la durata e il comportamento di acquisizione 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:

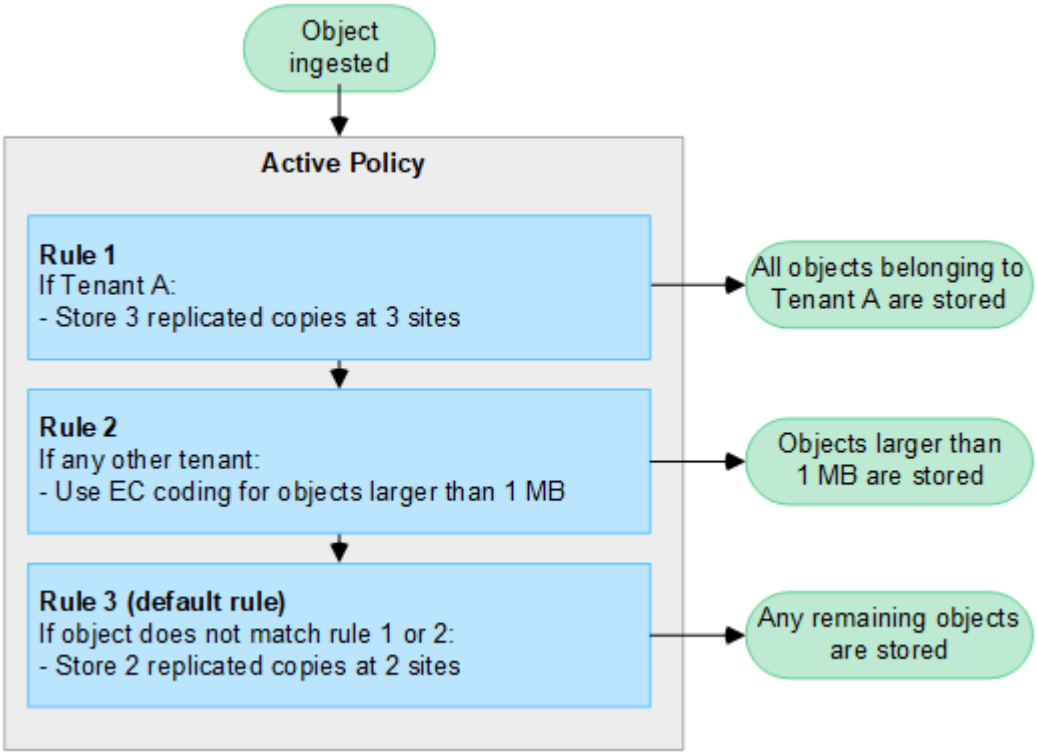
1. Se i filtri per la prima regola del criterio corrispondono a un oggetto, l'oggetto viene acquisito in base al comportamento di acquisizione di tale regola e memorizzato in base alle istruzioni di posizionamento di tale regola.
2. Se i filtri per la prima regola non corrispondono all'oggetto, l'oggetto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

Ad esempio, un criterio ILM potrebbe contenere tre regole ILM che specificano quanto segue:

- **Regola 1: Copie replicate per il tenant A**
  - Abbina tutti gli oggetti appartenenti al tenant A.
  - Memorizzare questi oggetti 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.
- **Regola 2: Erasure coding per oggetti superiori a 1 MB**
  - Associare 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.
  - Non corrisponde a oggetti di dimensioni pari o inferiori a 1 MB, pertanto questi oggetti vengono valutati in base alla regola 3.

- **Regola 3: 2 copie 2 data center** (impostazione predefinita)
  - È l'ultima regola predefinita del criterio. Non utilizza filtri.
  - Creare 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"

Esplora StorageGRID

Esplora Grid Manager

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

> Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere alle schermate di esempio di questa pagina.

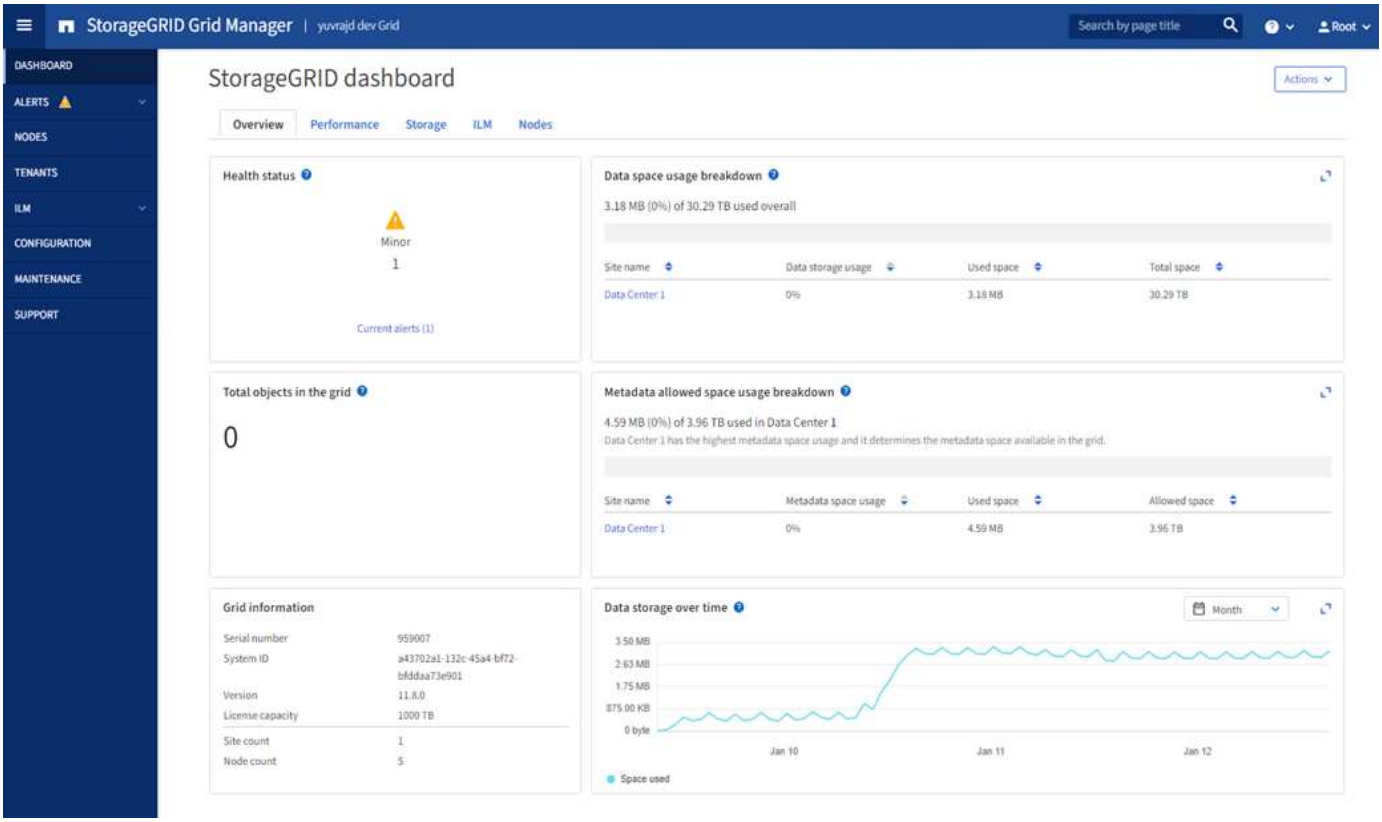
Quando si accede a Grid Manager, si sta effettuando la connessione a un nodo amministratore. Ogni sistema StorageGRID include un nodo di amministrazione primario e un numero qualsiasi di nodi di amministrazione non primari. È possibile connettersi a qualsiasi nodo amministratore e ciascun nodo amministratore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

È possibile accedere a Grid Manager utilizzando un "browser web supportato".

Dashboard di Grid Manager

Quando si accede per la prima volta a Grid Manager, è possibile utilizzare il dashboard per "monitorare le attività del sistema" a colpo d'occhio.

La dashboard contiene informazioni sullo stato e le performance del sistema, sull'utilizzo dello storage, sui processi ILM, sulle operazioni S3 e Swift e sui nodi della griglia. È possibile "configurare il cruscotto" selezionando da una raccolta di schede che contengono le informazioni necessarie per monitorare efficacemente il sistema.



Per una spiegazione delle informazioni visualizzate su ciascuna scheda, selezionare l'icona della guida per quella scheda.

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 del server di gestione delle chiavi (KMS). È possibile utilizzare **Cerca** per trovare le voci nella barra laterale di Grid Manager e nei menu Configurazione, manutenzione e supporto.

Menu Guida

Il menu della guida consente di accedere a:

- Il "FabricPool" e. "Impostazione S3" procedura guidata
- Il centro di documentazione StorageGRID per la versione corrente
- "Documentazione API"
- Informazioni sulla versione di StorageGRID attualmente installata

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.

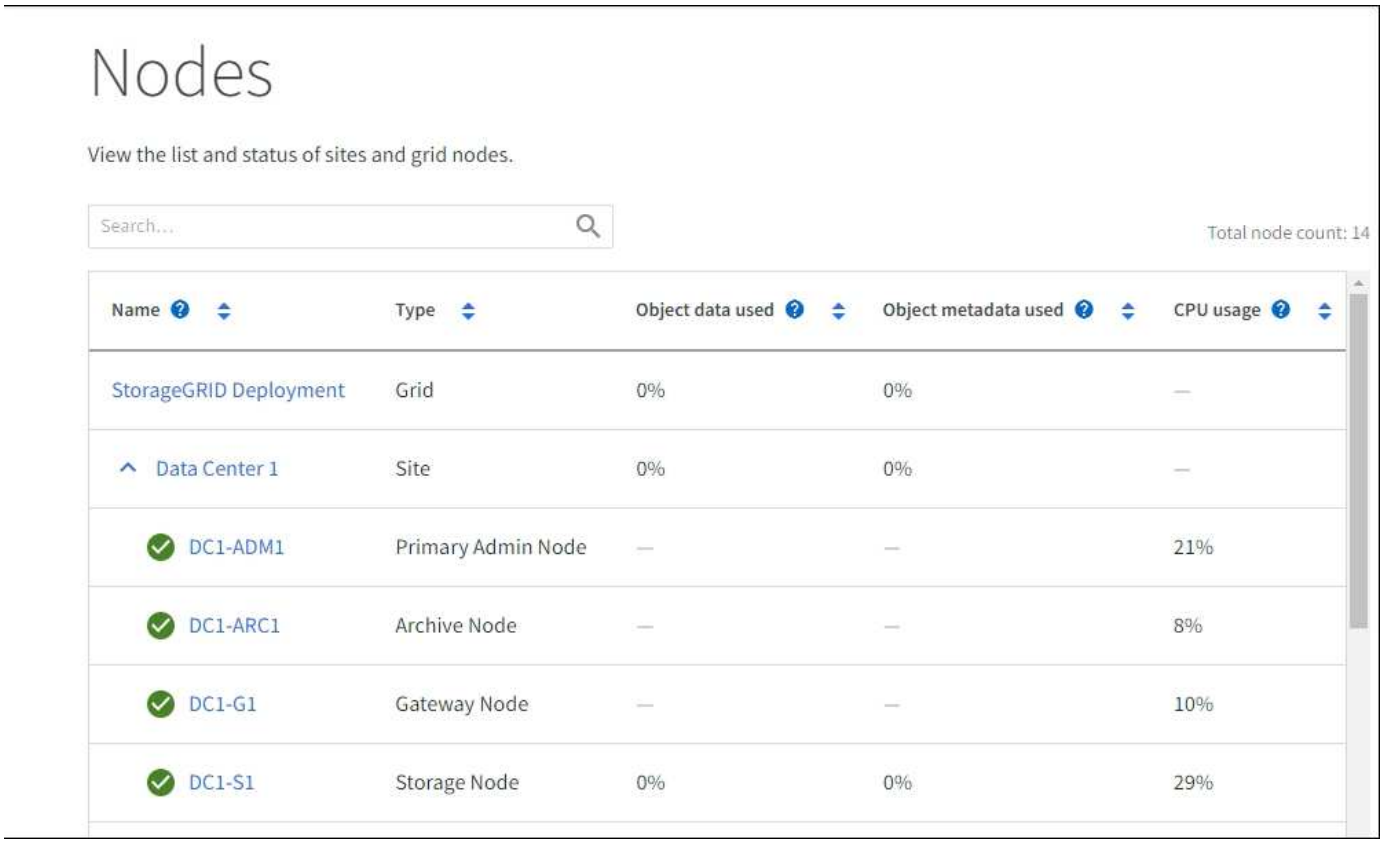
Dal menu Avvisi, è possibile effettuare le seguenti operazioni "gestire gli avvisi":

- 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

Pagina nodi

Il "Pagina nodi" visualizza le informazioni sull'intera griglia, su ciascun sito nella griglia e su ciascun nodo in un sito.

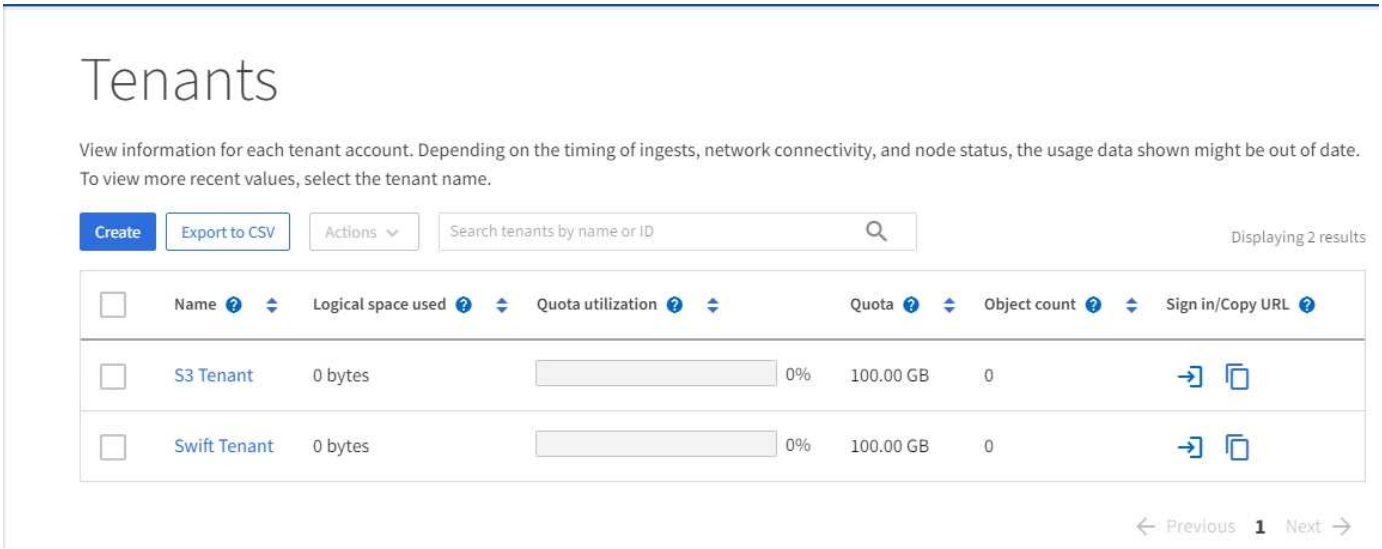
La home page dei nodi visualizza le metriche combinate per l'intera griglia. Per visualizzare le informazioni relative a un determinato sito o nodo, selezionare il sito o nodo.



Pagina tenant

Il "Tenant" consente di "creare e monitorare gli account tenant di storage" Per il tuo sistema StorageGRID. È necessario creare almeno un account tenant per specificare chi può memorizzare e recuperare gli oggetti e quali funzionalità sono disponibili.

La pagina tenant fornisce inoltre dettagli sull'utilizzo di ciascun tenant, tra cui la quantità di storage utilizzato e il numero di oggetti. Se si imposta una quota al momento della creazione del tenant, è possibile visualizzare la quantità di tale quota utilizzata.



Menu ILM

Il "Menu ILM" consente di "Configurare le regole e i criteri di gestione del ciclo di vita delle informazioni (ILM)" in grado di gestire durata e disponibilità dei dati. È inoltre possibile inserire un identificatore di oggetto per visualizzare i metadati relativi a tale oggetto.

Dal menu ILM è possibile visualizzare e gestire ILM:

- Regole
- Policy
- Tag policy
- Pool di storage
- Erasure coding
- Gradi di storage
- Regioni
- Ricerca dei metadati degli oggetti

Menu di configurazione

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

Attività di rete

Le attività di rete includono:

- "Gestione di gruppi ad alta disponibilità"
- "Gestione degli endpoint del bilanciamento del carico"
- "Configurazione dei nomi di dominio degli endpoint S3"
- "Gestione delle policy di classificazione del traffico"
- "Configurazione delle interfacce VLAN"

Attività di sicurezza

Le attività di sicurezza includono:

- "Gestione dei certificati di sicurezza"
- "Gestione dei controlli firewall interni"
- "Configurazione dei server di gestione delle chiavi"
- Configurazione delle impostazioni di sicurezza, tra cui "Policy TLS e SSH", "opzioni di protezione di rete e oggetti", e. "impostazioni di sicurezza dell'interfaccia".
- Configurazione delle impostazioni per "proxy di storage" o un "admin proxy (proxy amministratore)"

Attività di sistema

Le attività di sistema includono:

- Utilizzo di "federazione di grid" Per clonare le informazioni dell'account tenant e replicare i dati dell'oggetto tra due sistemi StorageGRID.
- Se si desidera, attivare "Compressione degli oggetti memorizzati" opzione.
- "Gestione del blocco oggetti S3"
- Informazioni sulle opzioni di storage, ad esempio "segmentazione degli oggetti" e. "filigrane dei volumi di storage".

Attività di monitoraggio

Le attività di monitoraggio includono:

- "Configurazione dei messaggi di audit e delle destinazioni dei log"
- "Utilizzo del monitoraggio SNMP"

Attività di controllo degli accessi

Le attività di controllo degli accessi includono:

- "Gestione dei gruppi di amministratori"
- "Gestione degli utenti amministratori"
- Modifica di "passphrase di provisioning" oppure "password della console dei nodi"
- "Utilizzo della federazione delle identità"
- "Configurazione di SSO"

Menu di manutenzione

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

Attività

Le attività di manutenzione includono:

- "Operazioni di decommissionamento" per rimuovere i nodi e i siti della griglia inutilizzati

- "Operazioni di espansione" per aggiungere nuovi nodi di griglia e siti
- "Procedure di ripristino del nodo Grid" per sostituire un nodo guasto e ripristinare i dati
- "Rinominare le procedure" per modificare i nomi di visualizzazione della griglia, dei siti e dei nodi
- "Operazioni di controllo dell'esistenza degli oggetti" per verificare l'esistenza (anche se non la correttezza) dei dati oggetto
- Esecuzione di un "riavvio in sequenza" per riavviare più nodi della griglia
- "Operazioni di ripristino dei volumi"

Sistema

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

- "Visualizzazione delle informazioni sulla licenza StorageGRID" oppure "aggiornamento delle informazioni sulla licenza"
- Generazione e download di "Pacchetto di ripristino"
- Esecuzione di aggiornamenti software StorageGRID, inclusi aggiornamenti software, hotfix e aggiornamenti del software SANtricity OS su alcune appliance
  - "Procedura di aggiornamento"
  - "Procedura di hotfix"
  - "Aggiorna il sistema operativo SANtricity sui controller di storage SG6000 utilizzando Grid Manager"
  - "Aggiorna il sistema operativo SANtricity sugli storage controller SG5700 usando Grid Manager"

Rete

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

- "Configurazione dei server DNS"
- "Aggiornamento delle subnet Grid Network in corso"
- "Gestione dei server NTP"

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 tre parti: Tools (Strumenti), Alarms (Allarmi) (legacy) e Other (Altro).

Strumenti

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

- "Configurare AutoSupport"
- "Eseguire la diagnostica" sullo stato corrente della griglia
- "Accedere alla struttura Grid Topology" per visualizzare informazioni dettagliate su nodi, servizi e attributi della griglia
- "Raccogliere i file di log e i dati di sistema"
- "Rivedere le metriche di supporto"

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)

Dal "Allarmi (legacy)" Nel menu supporto è possibile:

- Riesaminare gli allarmi correnti, storici e globali
- Impostare eventi personalizzati
- Configurazione "notifiche e-mail per gli allarmi legacy"

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

Altro

Dalla sezione Altro del menu supporto è possibile:

- Gestire "costo di collegamento"
- Visualizza "NMS (Network Management System)" voci
- Gestire "filigrane di archiviazione"

Esplora il tenant manager

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

Tenant Manager viene aggiornato con ogni versione e potrebbe non corrispondere alle schermate di esempio riportate in questa pagina.

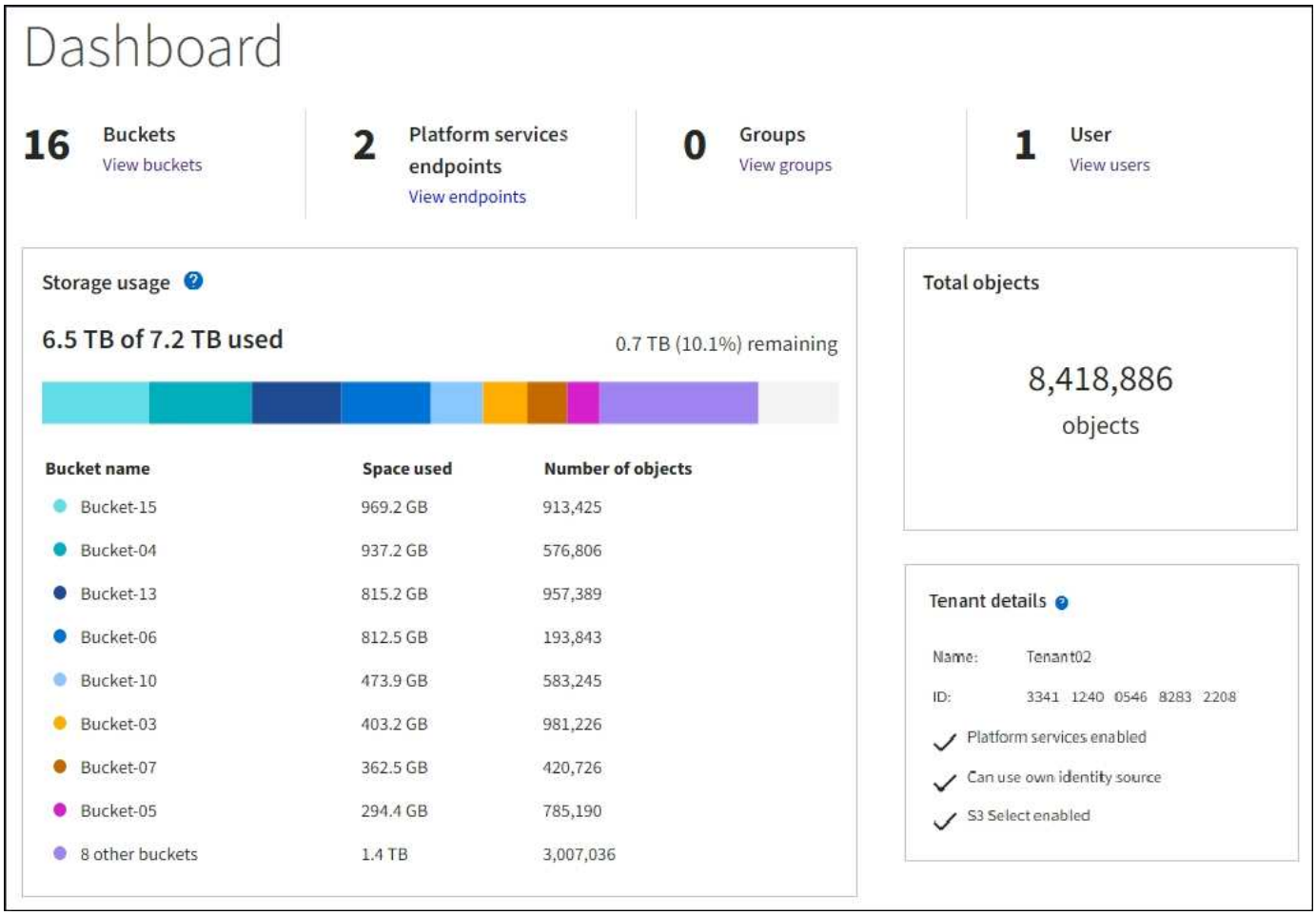
Quando gli utenti tenant accedono a Tenant Manager, si connettono a un nodo Admin.

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 (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, gestire ed eliminare i bucket, gestire gli endpoint dei servizi della piattaforma e visualizzare le connessioni di federazione di griglie che possono utilizzare.

Chiavi di accesso personali

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

- Gli utenti che dispongono dell'autorizzazione Gestisci le tue credenziali S3 possono creare o rimuovere le proprie chiavi di accesso S3.
- Gli utenti che dispongono dell'autorizzazione di accesso root 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 per i bucket:

- Creare bucket

- Attiva blocco oggetti S3 per un nuovo bucket (presuppone che il blocco oggetti S3 sia abilitato per il sistema StorageGRID)
- Aggiornare i valori di coerenza
- Attiva e disattiva gli ultimi aggiornamenti dell'orario di accesso
- Attivare o sospendere il controllo delle versioni degli oggetti
- Aggiorna la conservazione predefinita del blocco oggetti S3
- Configurare la condivisione delle risorse tra origini (CORS)
- Elimina tutti gli oggetti in un bucket
- Eliminare i bucket vuoti
- Utilizzare "S3 Console" per gestire gli oggetti bucket

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 Amazon Simple Notification Service.
- 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.

Connessioni a federazione di griglie

Se un amministratore della griglia ha abilitato l'utilizzo di una connessione a federazione di griglie per l'account tenant, un utente tenant S3 che dispone dell'autorizzazione di accesso root può visualizzare il nome della connessione e accedere alla pagina dei dettagli del bucket per ogni bucket che ha attivato la replica cross-grid, e visualizzare l'errore più recente che si verifica quando i dati del bucket venivano replicati nell'altra griglia della connessione. Vedere "Visualizza connessioni di federazione di griglie".

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.

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 "Scopri di più su StorageGRID".

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 i nodi appliance

- "Installare l'hardware dell'appliance"

Installare nodi basati su software

- "Installare StorageGRID su Red Hat Enterprise Linux"
- "Installare StorageGRID su Ubuntu o Debian"
- "Installare StorageGRID su VMware"

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 StorageGRID su Red Hat Enterprise Linux"
- "Installare StorageGRID su Ubuntu o Debian"
- "Installare StorageGRID su VMware"

Nodi appliance

- "Appliance di storage SG6160"
- "Appliance di storage SGF6112"
- "Appliance di storage SG6000"
- "Appliance di storage SG5800"
- "Appliance di storage SG5700"
- "Appliance per i servizi SG110 e SG1100"
- "Appliance di servizi SG100 e SG1000"

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 trovano 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 i controlli firewall" 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 Grid, 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 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.

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

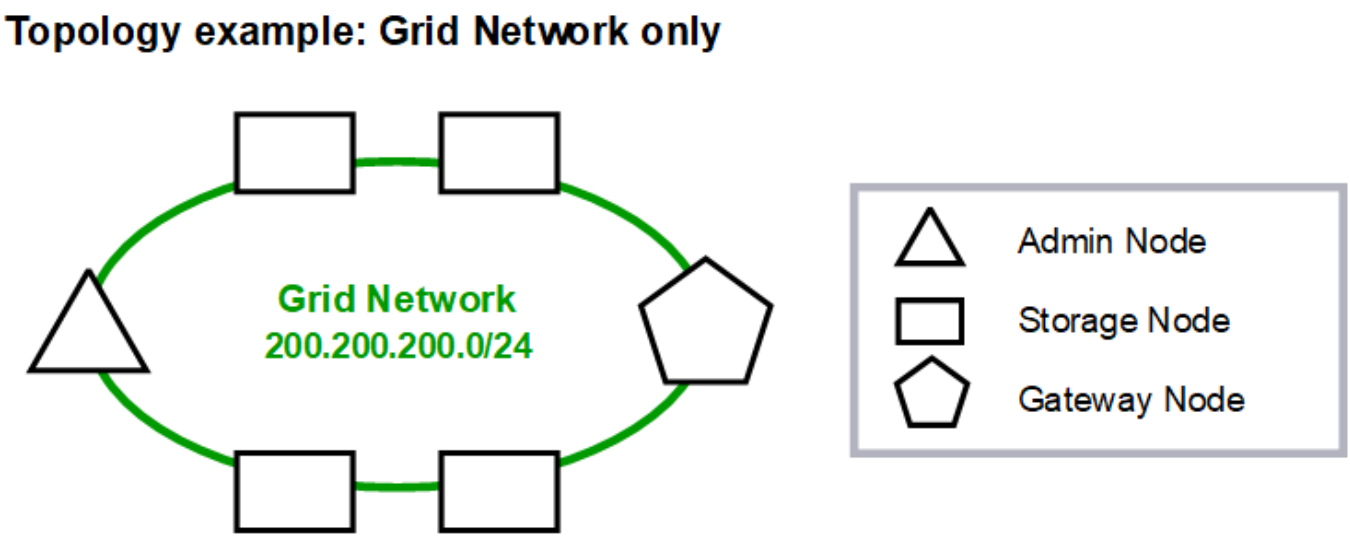
l'interfaccia eth0 per ciascun nodo della griglia.

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.



Provisioned

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

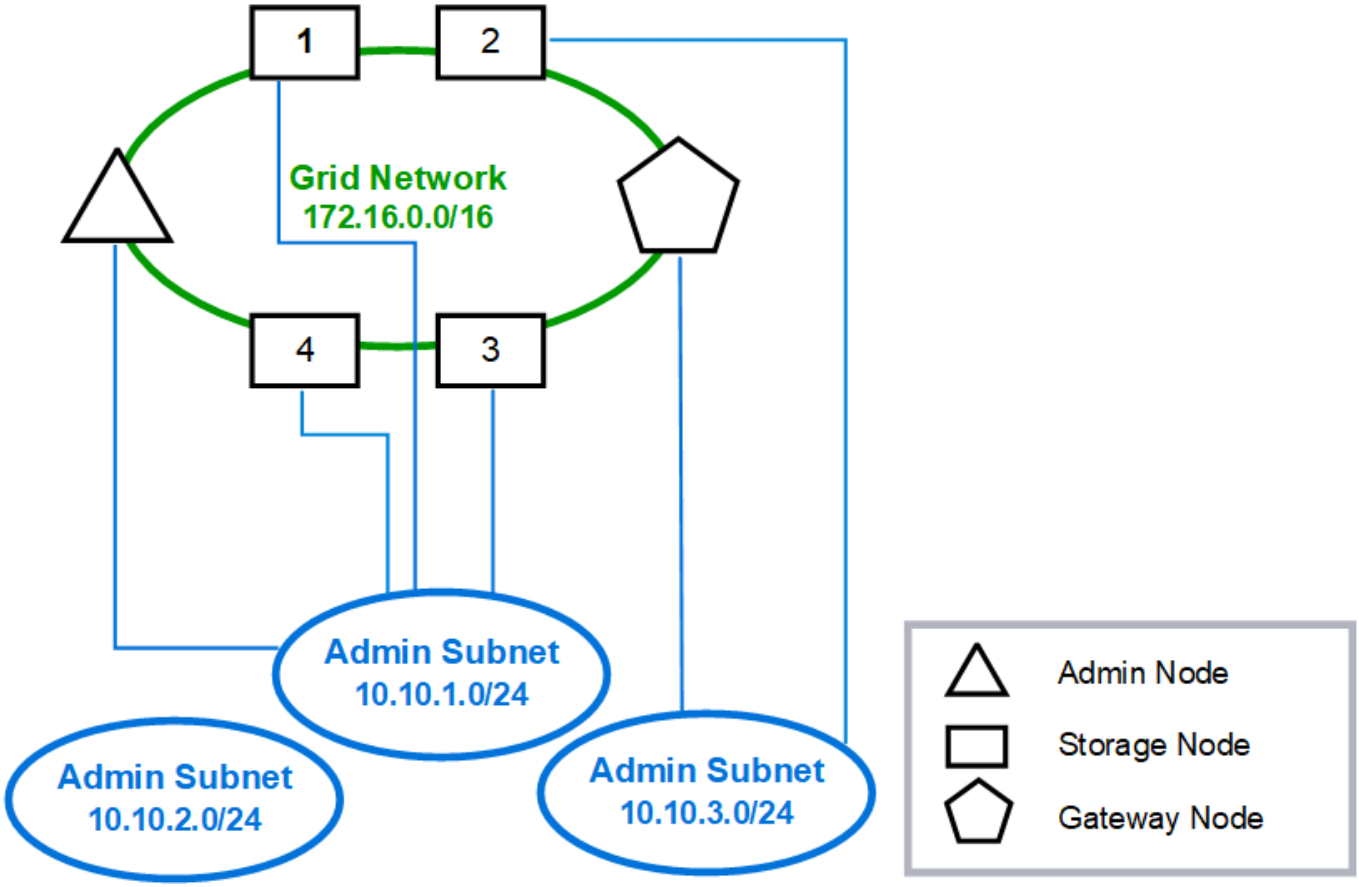
Disporre di una rete amministrativa è facoltativo. Un modo per utilizzare una rete amministrativa e una rete griglia consiste nel configurare una rete griglia instradabile e una rete amministrativa limitata per ciascun nodo.

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



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**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

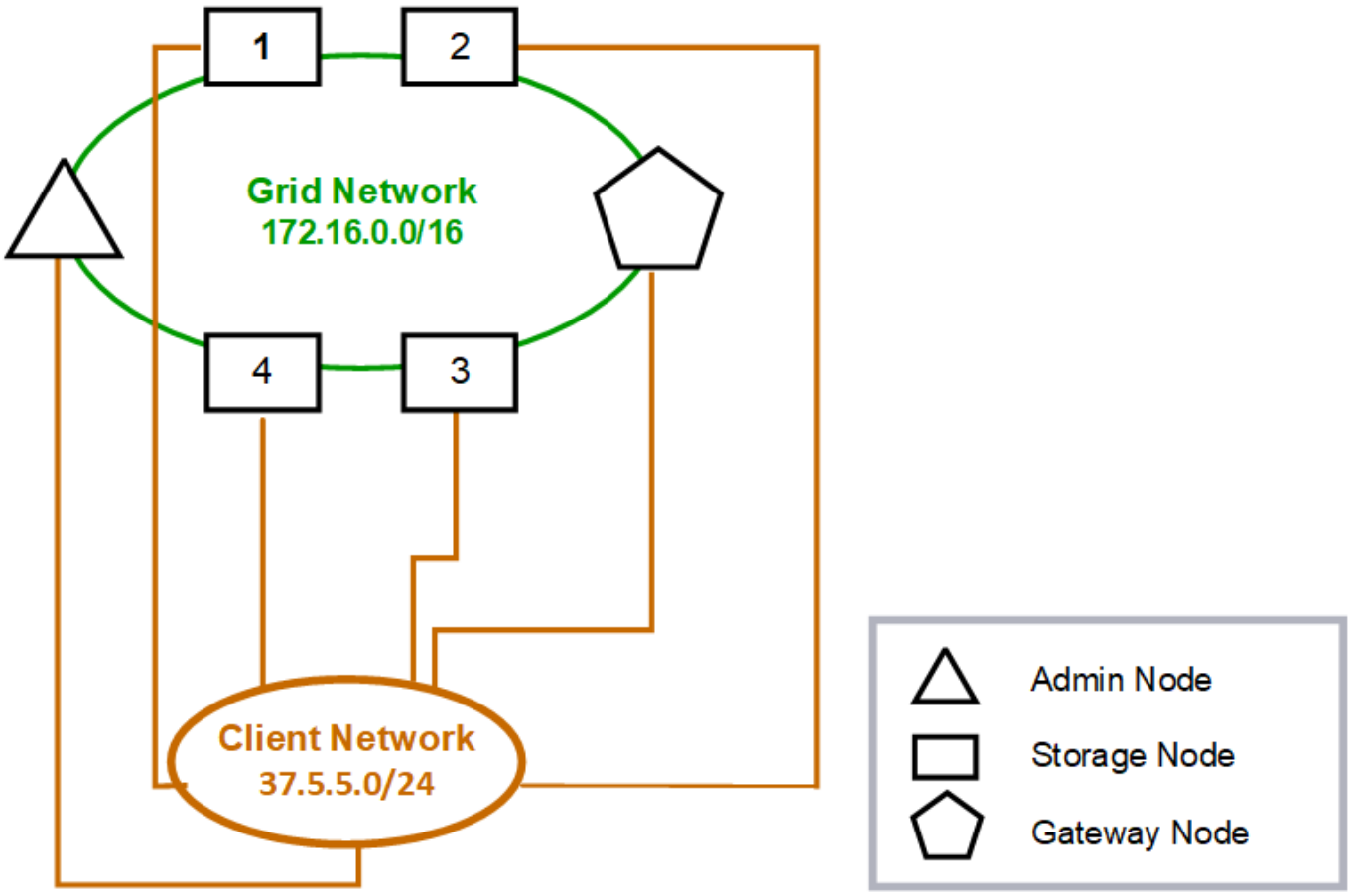
La disponibilità di una rete client è opzionale. L'utilizzo di una rete client consente di separare il traffico di rete client (ad esempio S3 e Swift) dal traffico interno della rete, consentendo una maggiore sicurezza delle reti di rete. Il traffico amministrativo può essere gestito dal client o dalla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



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	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

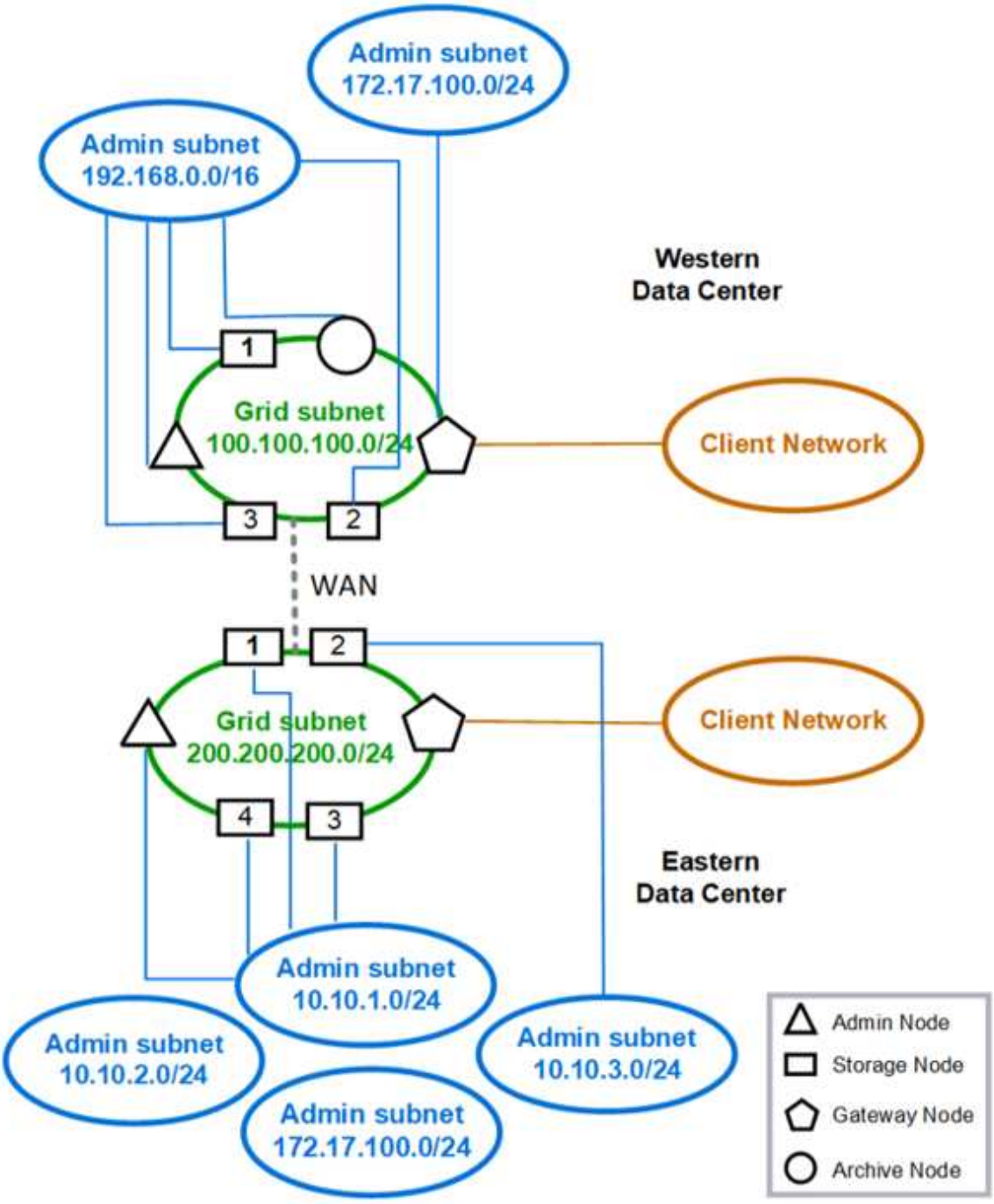
Topologia per tutte e tre le reti

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 è in grado di contattare 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.

I requisiti effettivi di larghezza di banda WAN minima dipendono dall'attività del client e dallo schema di protezione ILM. Per assistenza nella stima dei requisiti minimi di larghezza di banda della WAN, contatta il tuo consulente NetApp Professional Services.

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 la funzione 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.
- Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete di amministrazione o la rete client di alcun nodo:
  - 192.168.130.101

- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

  Ad esempio, non utilizzare i seguenti intervalli di subnet per la rete Grid, la rete amministrativa o la rete client di alcun nodo:

- 192.168.130.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 198.51.100.2 e 198.51.100.4

- 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 in AESL non possono sovrapporsi con le subnet in 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 dell'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 usi 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 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" 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 (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, 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 LAN minima per ciascun tipo di nodo StorageGRID e 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
	Larghezza di banda LAN minima	Amministratore	10 Gbps
1 Gbps	1 Gbps	Gateway	10 Gbps
1 Gbps	10 Gbps	Storage	10 Gbps
1 Gbps	10 Gbps	Archiviare	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)"
- "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. "Gestire 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 "Che cos'è un Cloud Storage Pool".

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 le reti VLAN per i servizi di piattaforma o i pool di cloud storage. 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 dell'appliance:

- "Modalità Port bond (SG6160)"
- "Modalità di port bond (SGF6112)"
- "Modalità Port Bond (controller SG6000-CN)"
- "Modalità di collegamento porte (controller SG5800)"
- "Modalità di collegamento porte (controller E5700SG)"
- "Modalità Port bond (SG110 e SG1100)"
- "Modalità Port Bond (SG100 e SG1000)"

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. Impossibile 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 connessioni in entrata a porte specifiche della rete di rete. 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 StorageGRID su Red Hat Enterprise Linux"
- "Installare StorageGRID su 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 StorageGRID su 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. Vedere "Opzionale: Consente di rimappare le porte di rete per l'appliance".

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.

Porta	TCP o UDP	Da	A.	Dettagli
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.
1055	TCP	Tutti i nodi	Nodo amministratore primario	Traffico interno per l'installazione, l'espansione, il ripristino 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.

Porta	TCP o UDP	Da	A.	Dettagli
5353	UDP	Tutti i nodi	Tutti i nodi	Fornisce il servizio DNS multicast (mDNS) utilizzato per le modifiche IP dell'intera griglia e per l'individuazione del nodo di amministrazione primario durante l'installazione, l'espansione e il ripristino. **Nota**: la configurazione di questa porta è facoltativa.
7001	TCP	Nodi di storage	Nodi di storage	Comunicazione cluster tra nodi Cassandra TLS.
7443	TCP	Tutti i nodi	Nodo amministratore primario	Traffico interno per installazione, espansione, ripristino, altre procedure di manutenzione e segnalazione degli errori.
8011	TCP	Tutti i nodi	Nodo amministratore primario	Traffico interno per l'installazione, l'espansione, il ripristino e altre procedure di manutenzione.
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 pacchetti AutoSupport da SANtricity System Manager di e-Series al nodo amministrativo primario.
10342	TCP	Tutti i nodi	Nodo amministratore primario	Traffico interno per l'installazione, l'espansione, il ripristino e altre procedure di manutenzione.
11139	TCP	Nodi di archiviazione/storage	Nodi di archiviazione/storage	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.

Porta	TCP o UDP	Da	A.	Dettagli
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.
18086	TCP	Tutti i nodi della griglia	Tutti i nodi storage	Traffico interno relativo al servizio LDR.
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.

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 rimapping delle porte, consultare le istruzioni di installazione:

- "Installare StorageGRID su Red Hat Enterprise Linux"
- "Installare StorageGRID su Ubuntu o Debian"
- "Installare StorageGRID su VMware"
- "Opzionale: Consente di rimappare le porte di rete per l'appliance"

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".

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 di 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.
53	TCP/UDP	DNS	Tutti i nodi	Server DNS	Utilizzato per DNS.
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.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
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.
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. **Nota:** il supporto per NFS è stato obsoleto e verrà rimosso in una versione futura.
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 richiesta solo se è abilitata l'esportazione di controllo 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 richiesta solo se è abilitata l'esportazione di controllo basata su SMB.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
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 richiesta solo se è abilitata l'esportazione di controllo basata su SMB.
161	TCP/UDP	SNMP	Client SNMP	Tutti i nodi	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. **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. **Nota:** per informazioni sull'utilizzo di SNMP con StorageGRID, contattare il proprio rappresentante NetApp.
162	TCP/UDP	Notifiche SNMP	Tutti i nodi	Destinazioni di notifica	Per impostazione predefinita, le notifiche e i trap SNMP in uscita sono impostati sulla porta UDP 162. **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. **Nota:** per informazioni sull'utilizzo di SNMP con StorageGRID, contattare il proprio rappresentante NetApp.
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.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
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. **Nota**: Se si chiudono le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati. Vedere "Configurare i controlli firewall" Per configurare gli indirizzi IP privilegiati.
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 sovrascrivere l'impostazione predefinita della porta HTTP di 443 quando creano un endpoint.
443	TCP	HTTPS	Nodi di storage	AWS	Le richieste dei Cloud Storage Pools vengono inviate alle 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 richiesta solo se è abilitata l'esportazione di controllo basata su SMB.
903	TCP	NFS	Client NFS	Nodi di amministrazione	Utilizzato dall'esportazione di audit basata su NFS (`rpc.mountd`). **Nota:** questa porta è necessaria solo se è abilitata l'esportazione di audit basata su NFS. **Nota:** il supporto per NFS è stato obsoleto e verrà rimosso in una versione futura.

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. **Nota:** il supporto per NFS è stato obsoleto e verrà rimosso in una versione futura.
5353	UDP	MDNS	Tutti i nodi	Tutti i nodi	Fornisce il servizio DNS multicast (mDNS) utilizzato per le modifiche IP dell'intera griglia e per l'individuazione del nodo di amministrazione primario durante l'installazione, l'espansione e il ripristino. **Nota**: la configurazione di questa porta è facoltativa.
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.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
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. **Nota**: Se si chiudono le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati. Vedere "Configurare i controlli firewall" Per configurare gli indirizzi IP privilegiati.
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.
9092	TCP	Kafka	Nodi di storage con ADC	Cluster Kafka	Utilizzato per i messaggi di Platform Services inviati a un cluster Kafka. I tenant possono sovrascrivere l'impostazione predefinita della porta Kafka di 9092 quando creano un endpoint.
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).
18083	TCP	HTTPS	Client Swift	Nodi di storage	Traffico client rapido direttamente ai nodi di storage (HTTPS).

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
18084	TCP	HTTP	Client S3	Nodi di storage	Traffico client S3 direttamente verso i nodi di archiviazione (HTTP).
18085	TCP	HTTP	Client Swift	Nodi di storage	Traffico client Swift direttamente verso i nodi di archiviazione (HTTP).
23000-23999	TCP	HTTPS	Tutti i nodi della griglia di origine per la replica cross-grid	Nodi di amministrazione e nodi gateway nella griglia di destinazione per la replica cross-grid	Questo intervallo di porte è riservato alle connessioni a federazione di griglie. Entrambe le griglie di una determinata connessione utilizzano la stessa porta.

Avvio rapido per StorageGRID

Seguire questi passaggi per configurare e utilizzare qualsiasi sistema StorageGRID.

Imparare, pianificare e raccogliere dati

Collaborate con il vostro account rappresentante NetApp per comprendere le opzioni e pianificare il vostro nuovo sistema StorageGRID. Considerare questi tipi di domande:

- Quanti dati a oggetti prevedete di memorizzare inizialmente e nel tempo?
- Quanti siti sono necessari?
- Quanti e quali tipi di nodi sono necessari per ciascun sito?
- Quali reti StorageGRID utilizzerai?
- Chi utilizzerà la griglia per memorizzare gli oggetti? Quali applicazioni utilizzeranno?
- Hai requisiti di sicurezza o storage speciali?
- È necessario rispettare i requisiti legali o normativi?

In alternativa, collaborate con il vostro consulente NetApp Professional Services per accedere al tool NetApp ConfigBuilder e completare un manuale di configurazione da utilizzare durante l'installazione e l'implementazione del nuovo sistema. È inoltre possibile utilizzare questo strumento per automatizzare la configurazione di qualsiasi appliance StorageGRID. Vedere "Automazione dell'installazione e della configurazione delle appliance".

Revisione "Scopri di più su StorageGRID" e a. "Linee guida per il networking".

Installare i nodi

Un sistema StorageGRID è costituito da singoli nodi basati su hardware e software. Installare innanzitutto l'hardware per ciascun nodo appliance e configurare ciascun host Linux o VMware.

Per completare l'installazione, installare il software StorageGRID su ogni appliance o host software e collegare i nodi in una griglia. Durante questa fase, vengono forniti i nomi di siti e nodi, i dettagli della subnet e gli indirizzi IP per i server NTP e DNS.

Scopri come:

- "Installare l'hardware dell'appliance"
- "Installare StorageGRID su Red Hat Enterprise Linux"
- "Installare StorageGRID su Ubuntu o Debian"
- "Installare StorageGRID su VMware"

Effettuare l'accesso e controllare lo stato del sistema

Non appena si installa l'Admin Node primario, è possibile accedere a Grid Manager. Da qui, è possibile esaminare lo stato generale del nuovo sistema, abilitare AutoSupport e le email di avviso e impostare i nomi di dominio degli endpoint S3.

Scopri come:

- "Accedi a Grid Manager"
- "Monitorare lo stato del sistema"
- "Configurare AutoSupport"
- "Imposta le notifiche via email per gli avvisi"
- "Configurare i nomi di dominio degli endpoint S3"

Configurare e gestire

Le attività di configurazione da eseguire per un nuovo sistema StorageGRID dipendono dal modo in cui si utilizzerà il grid. Come minimo, è possibile configurare l'accesso al sistema, utilizzare le procedure guidate FabricPool e S3 e gestire varie impostazioni di storage e sicurezza.

Scopri come:

- "Controllare l'accesso a StorageGRID"
- "Utilizzare l'installazione guidata S3"
- "Utilizzare l'installazione guidata di FabricPool"
- "Gestire la sicurezza"
- "Protezione avanzata del sistema"

Impostare ILM

È possibile controllare il posizionamento e la durata di ogni oggetto nel sistema StorageGRID configurando una policy di gestione del ciclo di vita delle informazioni (ILM) costituita da una o più regole ILM. Le regole ILM spiegano a StorageGRID come creare e distribuire copie di dati a oggetti e come gestirle nel tempo.

Scopri come: "Gestire gli oggetti con ILM"

6 USA StorageGRID

Una volta completata la configurazione iniziale, gli account tenant di StorageGRID possono utilizzare le applicazioni client S3 e Swift per acquisire, recuperare ed eliminare oggetti.

Scopri come:

- "Utilizzare un account tenant"
- "Utilizzare l'API REST S3"
- "Utilizzare l'API REST di Swift"

7 Monitorare e risolvere i problemi

Quando il sistema è attivo e in funzione, è necessario monitorarne regolarmente le attività e risolvere eventuali avvisi. È inoltre possibile configurare un server syslog esterno, utilizzare il monitoraggio SNMP o raccogliere dati aggiuntivi.

Scopri come:

- "Monitorare StorageGRID"
- "Risolvere i problemi relativi a StorageGRID"

8 Espansione, manutenzione e ripristino

È possibile aggiungere nodi o siti per espandere la capacità o le funzionalità del sistema. È inoltre possibile eseguire varie procedure di manutenzione per eseguire il ripristino in caso di guasti o per mantenere il sistema StorageGRID aggiornato e in grado di funzionare in modo efficiente.

Scopri come:

- "Espandere una griglia"
- "Mantenere la griglia"
- "Ripristinare i nodi"

Installazione, aggiornamento e correzione rapida StorageGRID

Appliance StorageGRID

Passare a. "Documentazione sull'appliance StorageGRID" Per scoprire come installare, configurare e gestire le appliance di storage e servizi StorageGRID.

Installare StorageGRID su Red Hat Enterprise Linux

Avvio rapido per l'installazione di StorageGRID su Red Hat Enterprise Linux

Per installare un nodo Red Hat Enterprise Linux (RHEL) Linux StorageGRID, procedere come segue.

1 **Preparazione**

- Scopri di più "Architettura StorageGRID e topologia di rete".
- Scopri le specifiche di "Networking StorageGRID".
- Raccogliere e preparare il "Informazioni e materiali richiesti".
- Preparare il necessario "CPU e RAM".
- Prevedere "requisiti di storage e performance".
- "Preparare i server Linux" Che ospiterà i nodi StorageGRID.

2 **Implementazione**

Implementare i nodi grid. Quando si implementano nodi grid, questi vengono creati come parte del sistema StorageGRID e connessi a una o più reti.

- Per distribuire i nodi grid basati su software sugli host preparati nel passaggio 1, utilizzare la riga di comando di Linux e. "file di configurazione dei nodi".
- Per implementare i nodi di appliance StorageGRID, segui la procedura "Avvio rapido per l'installazione dell'hardware".

3 **Configurazione**

Una volta distribuiti tutti i nodi, utilizzare il Grid Manager per "configurare la griglia e completare l'installazione".

Automatizzare l'installazione

Per risparmiare tempo e garantire coerenza, è possibile automatizzare l'installazione del servizio host StorageGRID e la configurazione dei nodi grid.

- Utilizza un framework di orchestrazione standard come Ansible, Puppet o Chef per automatizzare:

- Installazione di RHEL
- Configurazione di rete e storage
- Installazione del motore del container e del servizio host StorageGRID
- Implementazione di nodi grid virtuali

Vedere "Automatizzare l'installazione e la configurazione del servizio host StorageGRID".

- Dopo aver distribuito i nodi grid, "Automatizzare la configurazione del sistema StorageGRID" Utilizzo dello script di configurazione Python fornito nell'archivio di installazione.
- "Automatizzare l'installazione e la configurazione dei nodi grid delle appliance"
- Se si è uno sviluppatore avanzato di implementazioni StorageGRID, automatizzare l'installazione dei nodi grid utilizzando "API REST di installazione".

Pianificare e preparare l'installazione su Red Hat

Informazioni e materiali richiesti

Prima di installare StorageGRID, raccogliere e preparare le informazioni e il materiale necessari.

Informazioni richieste

Piano di rete

Quali reti intendi collegare a ogni nodo StorageGRID? StorageGRID supporta più reti per la separazione del traffico, la sicurezza e la convenienza amministrativa.

Vedere StorageGRID "Linee guida per il networking".

Informazioni di rete

A meno che non si utilizzi DHCP, gli indirizzi IP da assegnare a ciascun nodo della griglia e gli indirizzi IP dei server DNS e NTP.

Server per i nodi grid

Identificare un insieme di server (fisici, virtuali o entrambi) che, in aggregato, forniscono risorse sufficienti per supportare il numero e il tipo di nodi StorageGRID che si intende implementare.

> Se l'installazione di StorageGRID non utilizza nodi di storage (hardware) dell'appliance StorageGRID, è necessario utilizzare lo storage RAID hardware con cache di scrittura supportata dalla batteria (BBWC). StorageGRID non supporta l'utilizzo di reti VSAN (Virtual Storage Area Network), RAID software o nessuna protezione RAID.

Migrazione dei nodi (se necessaria)

Comprendere "requisiti per la migrazione dei nodi", se si desidera eseguire la manutenzione pianificata sugli host fisici senza alcuna interruzione del servizio.

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Materiali richiesti

Licenza NetApp StorageGRID

È necessario disporre di una licenza NetApp valida con firma digitale.

> Nell'archivio di installazione di StorageGRID è inclusa una licenza non di produzione, che può essere utilizzata per test e griglie di prova.

Archivio di installazione di StorageGRID

"Scaricare l'archivio di installazione di StorageGRID ed estrarre i file".

Laptop di assistenza

Il sistema StorageGRID viene installato tramite un laptop di assistenza.

Il laptop di assistenza deve disporre di:

- Porta di rete
- Client SSH (ad esempio, putty)
- "Browser Web supportato"

Documentazione StorageGRID

- "Note di rilascio"
- "Istruzioni per l'amministrazione di StorageGRID"

Scaricare ed estrarre i file di installazione di StorageGRID

È necessario scaricare l'archivio di installazione di StorageGRID ed estrarre i file richiesti.

Fasi

1. Accedere alla "Pagina dei download NetApp per StorageGRID".
2. Selezionare il pulsante per scaricare l'ultima versione oppure selezionare un'altra versione dal menu a discesa e selezionare **Go**.
3. Accedi con il nome utente e la password del tuo account NetApp.
4. Se viene visualizzata un'istruzione Caution/MustRead, leggerla e selezionare la casella di controllo.

> Dopo aver installato la release di StorageGRID, è necessario applicare le correzioni rapide richieste. Per ulteriori informazioni, consultare "procedura di hotfix nelle istruzioni di ripristino e manutenzione".

5. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).
6. Nella colonna **Installa StorageGRID**, selezionare il file .tgz o .zip per Red Hat Enterprise Linux.

> Selezionare `.zip` File se si esegue Windows sul laptop di assistenza.

7. Salvare ed estrarre il file di archivio.
8. Scegliere i file desiderati dal seguente elenco.

I file necessari dipendono dalla topologia di griglia pianificata e dal modo in cui verrà implementato il sistema StorageGRID.

> I percorsi elencati nella tabella sono relativi alla directory di primo livello installata dall'archivio di installazione estratto

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Pacchetto RPM per l'installazione delle immagini del nodo StorageGRID sui vostri host RHEL.
	Pacchetto RPM per l'installazione del servizio host StorageGRID sugli host RHEL.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per il ping federate.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di ruolo e playbook Ansible per la configurazione degli host RHEL per l'implementazione dei container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.

Percorso e nome del file	Descrizione
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Script di supporto chiamato dal compagno `storagegrid-ssoauth-azure.py` Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

Requisiti software per Red Hat Enterprise Linux

È possibile utilizzare una macchina virtuale per ospitare qualsiasi tipo di nodo StorageGRID. È necessaria una macchina virtuale per ogni nodo di griglia.

Per installare StorageGRID su Red Hat Enterprise Linux (RHEL), è necessario installare alcuni pacchetti software di terze parti. Alcune distribuzioni Linux supportate non contengono questi pacchetti per impostazione predefinita. Le versioni dei pacchetti software su cui vengono testate le installazioni di StorageGRID includono quelle elencate in questa pagina.

Se si seleziona un'opzione di installazione runtime di distribuzione Linux e contenitore che richiede uno qualsiasi di questi pacchetti e questi non vengono installati automaticamente dalla distribuzione Linux, installare una delle versioni elencate qui se disponibile presso il provider o il fornitore di supporto per la distribuzione Linux. In caso contrario, utilizzare le versioni predefinite dei pacchetti disponibili presso il fornitore.

Tutte le opzioni di installazione richiedono Podman o Docker. Non installare entrambi i pacchetti. Installare solo il pacchetto richiesto dall'opzione di installazione.

Versioni Python testate

- 3,5.2-2
- 3,6.8-2
- 3,6.8-38
- 3,6.9-1
- 3,7.3-1
- 3,8.10-0

- 3,9.2-1
- 3,9.10-2
- 3,9.16-1
- 3.10.6-1
- 3.11.2-6

Versioni di Podman testate

- 3,2.3-0
- 3,4.4+ds1
- 4,1.1-7
- 4,2.0-11
- 4,3.1+ds1-8+b1
- 4,4.1-8
- 4,4.1-12

Versioni di Docker testate

Il supporto di Docker è obsoleto e verrà rimosso in una release futura.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1
- Docker-CE 24,0.2-1
- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1.5-2

Requisiti di CPU e RAM

Prima di installare il software StorageGRID, verificare e configurare l'hardware in modo che sia pronto per il supporto del sistema StorageGRID.

Ogni nodo StorageGRID richiede le seguenti risorse minime:

- Core CPU: 8 per nodo
- RAM: Almeno 24 GB per nodo e da 2 a 16 GB in meno rispetto alla RAM totale del sistema, a seconda della RAM totale disponibile e della quantità di software non StorageGRID in esecuzione nel sistema

Le risorse dei nodi di solo metadati basate su software devono corrispondere alle risorse dei nodi di storage esistenti. Ad esempio:

- Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:

    - 128 GB DI RAM
    - CPU a 8 core
    - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)
- Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuale con 24 GB di RAM, 8 core CPU e 3 TB o 4TB di memorizzazione di metadati, i nodi basati solo sui metadati del software devono utilizzare risorse simili (24 GB di RAM, 8 core CPU e 4TB di memorizzazione di metadati (rangedb/0).

Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve almeno StorageGRID corrispondere ai nodi storage dei siti StorageGRID esistenti e alle nuove risorse del sito.

Assicurarsi che il numero di nodi StorageGRID che si intende eseguire su ciascun host fisico o virtuale non superi il numero di core CPU o la RAM fisica disponibile. Se gli host non sono dedicati all'esecuzione di StorageGRID (non consigliato), assicurarsi di prendere in considerazione i requisiti di risorse delle altre applicazioni.

> Monitorate regolarmente l'utilizzo di CPU e memoria per garantire che queste risorse continuino a soddisfare il vostro carico di lavoro. Ad esempio, raddoppiando l'allocazione di RAM e CPU per i nodi di storage virtuali si fornirebbero risorse simili a quelle fornite per i nodi di appliance StorageGRID. Inoltre, se la quantità di metadati per nodo supera i 500 GB, considerare l'aumento della RAM per nodo a 48 GB o più. Per informazioni sulla gestione dello storage dei metadati degli oggetti, sull'aumento dell'impostazione Metadata Reserved Space e sul monitoraggio dell'utilizzo di CPU e memoria, vedere le istruzioni per "amministrazione", "monitoraggio", e. "aggiornamento in corso" StorageGRID.

Se l'hyperthreading è attivato sugli host fisici sottostanti, è possibile fornire 8 core virtuali (4 core fisici) per nodo. Se l'hyperthreading non è attivato sugli host fisici sottostanti, è necessario fornire 8 core fisici per nodo.

Se si utilizzano macchine virtuali come host e si ha il controllo sulle dimensioni e sul numero di macchine virtuali, è necessario utilizzare una singola macchina virtuale per ciascun nodo StorageGRID e dimensionare di conseguenza la macchina virtuale.

Per le implementazioni in produzione, non è necessario eseguire più nodi di storage sullo stesso hardware di storage fisico o host virtuale. Ciascun nodo di storage in una singola implementazione StorageGRID deve trovarsi nel proprio dominio di errore isolato. È possibile massimizzare la durata e la disponibilità dei dati degli oggetti se si garantisce che un singolo guasto hardware possa avere un impatto solo su un singolo nodo di storage.

Vedere anche "Requisiti di storage e performance".

Requisiti di storage e performance

È necessario comprendere i requisiti di storage per i nodi StorageGRID, in modo da poter fornire spazio sufficiente per supportare la configurazione iniziale e l'espansione dello storage futura.

I nodi StorageGRID richiedono tre categorie logiche di storage:

- **Pool di container** — storage a Tier di performance (10.000 SAS o SSD) per i container di nodi, che verrà assegnato al driver di storage del motore di container quando si installa e configura il motore di container sugli host che supporteranno i nodi StorageGRID.
- **Dati di sistema** — storage a Tier di performance (10.000 SAS o SSD) per lo storage persistente per nodo dei dati di sistema e dei log delle transazioni, che i servizi host StorageGRID utilizzeranno e mapperanno

in singoli nodi.

- **Dati oggetto** — storage di livello Performance (10.000 SAS o SSD) e storage bulk di livello capacità (NL-SAS/SATA) per lo storage persistente di dati oggetto e metadati oggetto.

È necessario utilizzare i dispositivi a blocchi supportati da RAID per tutte le categorie di storage. I dischi non ridondanti, gli SSD o i JBOD non sono supportati. È possibile utilizzare lo storage RAID condiviso o locale per qualsiasi categoria di storage; tuttavia, se si desidera utilizzare la funzionalità di migrazione dei nodi in StorageGRID, è necessario memorizzare i dati di sistema e i dati degli oggetti sullo storage condiviso. Per ulteriori informazioni, vedere "Requisiti per la migrazione dei container di nodi".

Requisiti relativi alle performance

Le performance dei volumi utilizzati per il pool di container, i dati di sistema e i metadati degli oggetti influiscono in modo significativo sulle performance complessive del sistema. Per questi volumi, è necessario utilizzare storage di livello performance (10.000 SAS o SSD) per garantire prestazioni disco adeguate in termini di latenza, operazioni di input/output al secondo (IOPS) e throughput. È possibile utilizzare lo storage a Tier di capacità (NL-SAS/SATA) per lo storage persistente dei dati a oggetti.

I volumi utilizzati per il pool di container, i dati di sistema e i dati degli oggetti devono avere il caching write-back abilitato. La cache deve essere su un supporto protetto o persistente.

Requisiti degli host che utilizzano lo storage NetApp ONTAP

Se il nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verifica che il volume non disponga di una policy di tiering FabricPool abilitata. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

> Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

Numero di host richiesti

Ogni sito StorageGRID richiede almeno tre nodi di storage.

> In un'implementazione in produzione, non eseguire più di un nodo di storage su un singolo host fisico o virtuale. L'utilizzo di un host dedicato per ciascun nodo di storage fornisce un dominio di errore isolato.

È possibile implementare altri tipi di nodi, come ad esempio nodi di amministrazione o nodi gateway, sugli stessi host oppure implementarli sui propri host dedicati in base alle necessità.

Numero di volumi di storage per ciascun host

La seguente tabella mostra il numero di volumi di storage (LUN) richiesti per ciascun host e le dimensioni minime richieste per ogni LUN, in base ai nodi che verranno implementati su tale host.

La dimensione massima del LUN testato è di 39 TB.

> Questi numeri si riferiscono a ciascun host e non all'intera griglia.

Scopo del LUN	Categoria di storage	Numero di LUN	Dimensione minima/LUN
Pool di storage del motore di container	Pool di container	1	Numero totale di nodi × 100 GB
`/var/local` volume	Dati di sistema	1 per ogni nodo su questo host	90 GB
Nodo di storage	Dati dell'oggetto	3 per ciascun nodo di storage su questo host **Nota:** Un nodo di storage basato su software può avere da 1 a 16 volumi di storage; si consigliano almeno 3 volumi di storage.	12 TB (4 TB/LUN) VEDERE Requisiti di storage per i nodi di storage per ulteriori informazioni.
Nodo di storage (solo metadati)	Metadati dell'oggetto	1	4 TB vedere Requisiti di storage per i nodi di storage per ulteriori informazioni. **Nota**: È richiesto un solo rangedb per i nodi di archiviazione di solo metadati.
Registri di audit del nodo di amministrazione	Dati di sistema	1 per ogni nodo Admin su questo host	200 GB
Tabelle del nodo di amministrazione	Dati di sistema	1 per ogni nodo Admin su questo host	200 GB

A seconda del livello di audit configurato, la dimensione degli input dell'utente, come il nome della chiave a oggetti S3, Inoltre, la quantità di dati del registro di controllo da conservare potrebbe essere necessaria per aumentare la dimensione del LUN del registro di controllo su ciascun nodo di amministrazione.in genere, una griglia genera circa 1 KB di dati di controllo per ogni operazione S3, Ciò significa che un LUN da 200 GB supporterà 70 milioni di operazioni al giorno o 800 operazioni al secondo per due o tre giorni.

Spazio di storage minimo per un host

La seguente tabella mostra lo spazio di storage minimo richiesto per ciascun tipo di nodo. È possibile utilizzare questa tabella per determinare la quantità minima di storage da fornire all'host in ciascuna categoria di storage, in base ai nodi che verranno implementati su tale host.

Non è possibile utilizzare le snapshot dei dischi per ripristinare i nodi della griglia. Fare riferimento invece alla "recovery del nodo grid" procedure per ogni tipo di nodo.

Tipo di nodo	Pool di container	Dati di sistema	Dati dell'oggetto
Nodo di storage	100 GB	90 GB	4.000 GB
Nodo Admin	100 GB	490 GB (3 LUN)	*non applicabile*
Nodo gateway	100 GB	90 GB	*non applicabile*
Nodo di archiviazione	100 GB	90 GB	*non applicabile*

Esempio: Calcolo dei requisiti di storage per un host

Si supponga di voler implementare tre nodi sullo stesso host: Un nodo di storage, un nodo di amministrazione e un nodo gateway. È necessario fornire un minimo di nove volumi di storage all'host. Sono necessari almeno 300 GB di storage a Tier di performance per i container di nodi, 670 GB di storage a Tier di performance per i dati di sistema e i log delle transazioni e 12 TB di storage a Tier di capacità per i dati a oggetti.

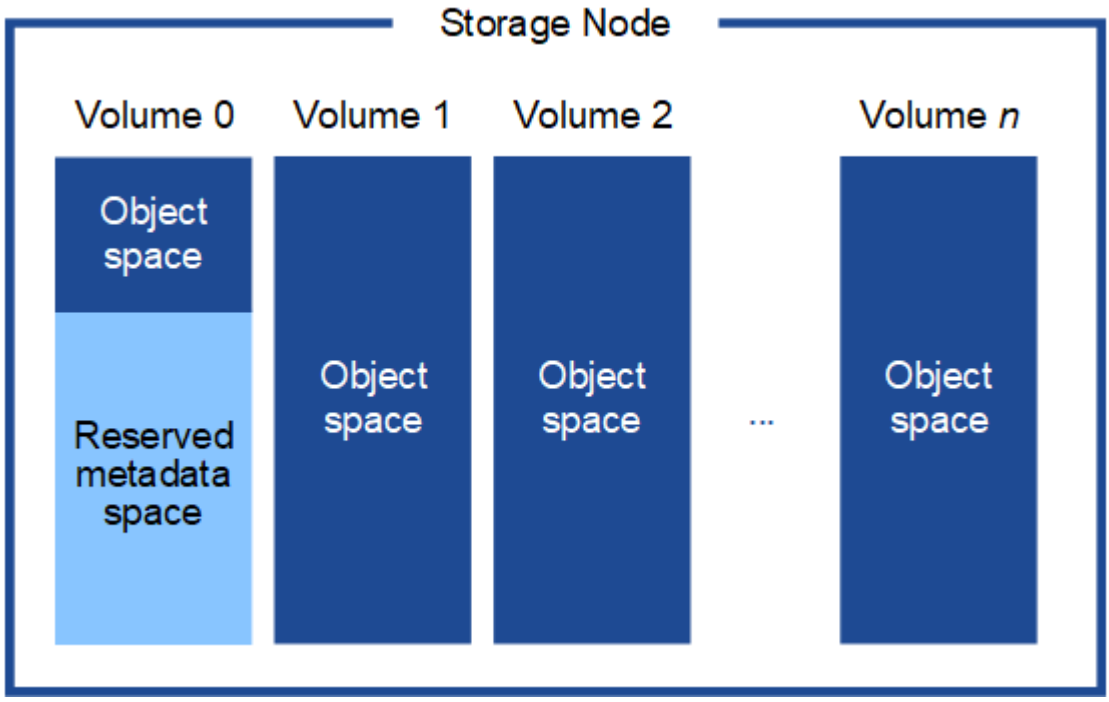
Tipo di nodo	Scopo del LUN	Numero di LUN	Dimensione del LUN
Nodo di storage	Pool di storage del motore di container	1	300 GB (100 GB/nodo)
Nodo di storage	`/var/local` volume	1	90 GB
Nodo di storage	Dati dell'oggetto	3	12 TB (4 TB/LUN)
Nodo Admin	`/var/local` volume	1	90 GB
Nodo Admin	Registri di audit del nodo di amministrazione	1	200 GB
Nodo Admin	Tabelle del nodo di amministrazione	1	200 GB
Nodo gateway	`/var/local` volume	1	90 GB
Totale		**9**	**Pool di container:** 300 GB **Dati di sistema:** 670 GB **Dati oggetto:** 12,000 GB

Requisiti di storage per i nodi di storage

Un nodo di storage basato su software può avere da 1 a 16 volumi di storage: Si consiglia di utilizzare almeno -3 volumi di storage. Ogni volume di storage deve essere pari o superiore a 4 TB.

Un nodo di storage dell'appliance può avere fino a 48 volumi di storage.

Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di storage 0 di ciascun nodo di storage. Qualsiasi spazio rimanente sul volume di storage 0 e qualsiasi altro volume di storage nel nodo di storage viene utilizzato esclusivamente per i dati a oggetti.



Per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti del sistema in ogni sito. Le tre copie dei metadati degli oggetti sono distribuite in modo uniforme in tutti i nodi di storage di ciascun sito.

Quando si installa un grid con nodi di storage solo metadati, il grid deve anche contenere un numero minimo di nodi per lo storage a oggetti. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

- Per un grid a sito singolo, vengono configurati almeno due nodi storage per oggetti e metadati.
- Per un grid multisito, per gli oggetti e i metadati viene configurato almeno un nodo di storage per sito.

Quando si assegna spazio al volume 0 di un nuovo nodo di storage, è necessario assicurarsi che vi sia spazio sufficiente per la porzione di tale nodo di tutti i metadati dell'oggetto.

- È necessario assegnare almeno 4 TB al volume 0.

  Se si utilizza un solo volume di storage per un nodo di storage e si assegnano 4 TB o meno al volume, il nodo di storage potrebbe entrare nello stato di sola lettura dello storage all'avvio e memorizzare solo i metadati degli oggetti.

  Se si assegnano meno di 500 GB al volume 0 (solo per uso non in produzione), il 10% della capacità del volume di storage viene riservato ai metadati.

- Le risorse dei nodi di solo metadati basate su software devono corrispondere alle risorse dei nodi di storage esistenti. Ad esempio:

- Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:
  - 128 GB DI RAM
  - CPU a 8 core
  - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)
- Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuale con 24 GB di RAM, 8 core CPU e 3 TB o 4TB di memorizzazione di metadati, i nodi basati solo sui metadati del software devono utilizzare risorse simili (24 GB di RAM, 8 core CPU e 4TB di memorizzazione di metadati (rangedb/0).

  Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve almeno StorageGRID corrispondere ai nodi storage dei siti StorageGRID esistenti e alle nuove risorse del sito.

- Se si sta installando un nuovo sistema (StorageGRID 11.6 o superiore) e ciascun nodo di storage dispone di almeno 128 GB di RAM, assegnare 8 TB o più al volume 0. L'utilizzo di un valore maggiore per il volume 0 può aumentare lo spazio consentito per i metadati su ciascun nodo di storage.
- Quando si configurano diversi nodi di storage per un sito, utilizzare la stessa impostazione per il volume 0, se possibile. Se un sito contiene nodi di storage di dimensioni diverse, il nodo di storage con il volume più piccolo 0 determinerà la capacità dei metadati di quel sito.

Per ulteriori informazioni, visitare il sito Web all'indirizzo "Gestire lo storage dei metadati degli oggetti".

Requisiti per la migrazione dei container di nodi

La funzione di migrazione dei nodi consente di spostare manualmente un nodo da un host all'altro. In genere, entrambi gli host si trovano nello stesso data center fisico.

La migrazione dei nodi consente di eseguire la manutenzione fisica degli host senza interrompere le operazioni di grid. Tutti i nodi StorageGRID vengono spostati uno alla volta su un altro host prima di portare l'host fisico offline. La migrazione dei nodi richiede solo un breve downtime per ciascun nodo e non deve influire sul funzionamento o sulla disponibilità dei servizi grid.

Se si desidera utilizzare la funzionalità di migrazione dei nodi StorageGRID, l'implementazione deve soddisfare requisiti aggiuntivi:

- Nomi di interfaccia di rete coerenti tra gli host di un singolo data center fisico
- Storage condiviso per i metadati StorageGRID e i volumi di repository di oggetti accessibili da tutti gli host in un singolo data center fisico. Ad esempio, è possibile utilizzare gli storage array NetApp e-Series.

Se si utilizzano host virtuali e il layer hypervisor sottostante supporta la migrazione delle macchine virtuali, è possibile utilizzare questa funzionalità invece della funzionalità di migrazione dei nodi in StorageGRID. In questo caso, è possibile ignorare questi requisiti aggiuntivi.

Prima di eseguire la migrazione o la manutenzione dell'hypervisor, arrestare correttamente i nodi. Consultare le istruzioni per "chiusura di un nodo di rete".

VMware Live Migration non supportato

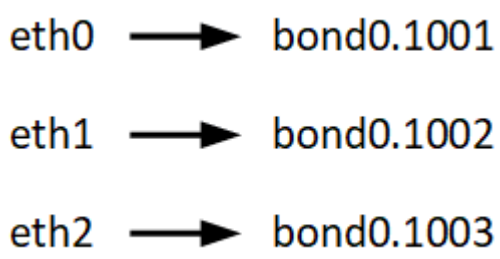
Quando si esegue l'installazione bare-metal su macchine virtuali VMware, OpenStack Live Migration e VMware Live vMotion causano l'aumento del tempo di clock della macchina virtuale e non sono supportati per nodi grid di qualsiasi tipo. Anche se rari, tempi di clock errati possono causare la perdita di dati o aggiornamenti della configurazione.

La migrazione a freddo è supportata. Durante la migrazione a freddo, i nodi StorageGRID vengono arrestati prima della migrazione tra host. Consultare le istruzioni per "chiusura di un nodo di rete".

Nomi di interfaccia di rete coerenti

Per spostare un nodo da un host a un altro, il servizio host StorageGRID deve avere una certa certezza che la connettività di rete esterna del nodo nella sua posizione corrente possa essere duplicata nella nuova posizione. Questa sicurezza viene ottenuta grazie all'utilizzo di nomi di interfaccia di rete coerenti negli host.

Si supponga, ad esempio, che StorageGRID NodeA in esecuzione sull'host 1 sia stato configurato con le seguenti mappature di interfaccia:



Il lato sinistro delle frecce corrisponde alle interfacce tradizionali visualizzate all'interno di un container StorageGRID (ovvero le interfacce griglia, Amministratore e rete client, rispettivamente). Il lato destro delle frecce corrisponde alle interfacce host effettive che forniscono queste reti, che sono tre interfacce VLAN subordinate allo stesso legame di interfaccia fisico.

Supponiamo ora di voler migrare NodeA in Host2. Se l'host 2 ha anche interfacce denominate bond0.1001, bond0.1002 e bond0.1003, il sistema consentirà lo spostamento, supponendo che le interfacce con nome simile forniscano la stessa connettività sull'host 2 di quella sull'host 1. Se l'host 2 non dispone di interfacce con gli stessi nomi, lo spostamento non sarà consentito.

Esistono diversi modi per ottenere un nome coerente dell'interfaccia di rete tra più host; vedere "Configurazione della rete host" per alcuni esempi.

Storage condiviso

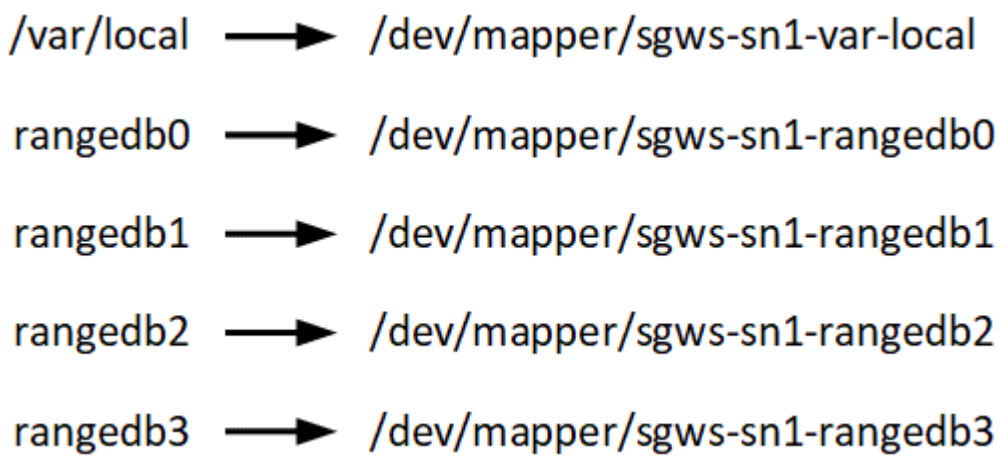
Per ottenere migrazioni dei nodi rapide e a basso overhead, la funzionalità di migrazione dei nodi StorageGRID non sposta fisicamente i dati dei nodi. La migrazione dei nodi viene invece eseguita come coppia di operazioni di esportazione e importazione, come segue:

1. Durante l'operazione di "esportazione dei nodi", una piccola quantità di dati di stato persistenti viene estratta dal contenitore di nodi in esecuzione sull'host e memorizzata nella cache sul volume di dati di sistema di quel nodo. Quindi, il contenitore di nodi su Hosta viene decreato.
2. Durante l'operazione di "importazione nodo", viene creata un'istanza del contenitore di nodo sull'HostB che utilizza la stessa interfaccia di rete e le mappature di archiviazione di blocco in vigore sull'Hosta. Quindi, i dati dello stato persistente memorizzati nella cache vengono inseriti nella nuova istanza.

Data questa modalità operativa, tutti i dati di sistema e i volumi di storage a oggetti del nodo devono essere accessibili sia da host che da host B affinché la migrazione sia consentita e funzioni. Inoltre, devono essere stati mappati nel nodo utilizzando nomi che sono garantiti per fare riferimento alle stesse LUN su Hosta e HostB.

Nell'esempio riportato di seguito viene illustrata una soluzione per il mapping dei dispositivi a blocchi per un nodo di storage StorageGRID, in cui il multipathing DM è in uso sugli host e il campo alias è stato utilizzato in

`/etc/multipath.conf` fornire nomi di dispositivi a blocchi coerenti e intuitivi disponibili su tutti gli host.



Preparare gli host (Red Hat)

Come cambiano le impostazioni dell'intero host durante l'installazione

Nei sistemi bare metal, StorageGRID apporta alcune modifiche all'intero host `sysctl` impostazioni.

Vengono apportate le seguenti modifiche:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
```

```
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

```
# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Installare Linux

È necessario installare StorageGRID su tutti i grid host Red Hat Enterprise Linux. Per un elenco delle versioni supportate, utilizza lo strumento matrice di interoperabilità NetApp.

Assicurarsi che il sistema operativo sia aggiornato al kernel Linux 4.15 o superiore.

Fasi

1. Installare Linux su tutti gli host grid fisici o virtuali in base alle istruzioni del distributore o alla procedura standard.

   Se si utilizza il programma di installazione standard di Linux, NetApp consiglia di selezionare la configurazione del software "nodo di elaborazione", se disponibile, o l'ambiente di base "installazione minima". Non installare ambienti desktop grafici.

2. Assicurarsi che tutti gli host abbiano accesso ai repository dei pacchetti, incluso il canale Extra.

   Questi pacchetti aggiuntivi potrebbero essere necessari più avanti in questa procedura di installazione.

3. Se lo swap è attivato:

   a. Eseguire il seguente comando: `$ sudo swapoff --all`

   b. Rimuovere tutte le voci di swap da `/etc/fstab` per mantenere le impostazioni.

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

Configurare la rete host (Red Hat Enterprise Linux)

Dopo aver completato l'installazione di Linux sugli host, potrebbe essere necessario eseguire alcune configurazioni aggiuntive per preparare un set di interfacce di rete su ciascun host adatte per il mapping nei nodi StorageGRID che verranno implementati in seguito.

Prima di iniziare

- Hai esaminato il "Linee guida per il networking StorageGRID".
- Sono state esaminate le informazioni su "requisiti per la migrazione dei container di nodi".
- Se si utilizzano host virtuali, è stato letto il Considerazioni e consigli per la clonazione degli indirizzi MAC prima di configurare la rete host.

Se si utilizzano macchine virtuali come host, selezionare VMXNET 3 come scheda di rete virtuale. L'adattatore di rete VMware E1000 ha causato problemi di connettività con i container StorageGRID implementati su determinate distribuzioni di Linux.

A proposito di questa attività

I nodi Grid devono essere in grado di accedere alla rete Grid e, facoltativamente, alle reti Admin e Client. È possibile fornire questo accesso creando mappature che associano l'interfaccia fisica dell'host alle interfacce virtuali per ciascun nodo della griglia. Quando si creano interfacce host, utilizzare nomi descrittivi per facilitare l'implementazione su tutti gli host e per abilitare la migrazione.

La stessa interfaccia può essere condivisa tra l'host e uno o più nodi. Ad esempio, è possibile utilizzare la stessa interfaccia per l'accesso all'host e l'accesso alla rete di amministrazione del nodo, per facilitare la manutenzione di host e nodi. Sebbene sia possibile condividere la stessa interfaccia tra l'host e i singoli nodi, tutti devono avere indirizzi IP diversi. Gli indirizzi IP non possono essere condivisi tra nodi o tra l'host e qualsiasi nodo.

È possibile utilizzare la stessa interfaccia di rete host per fornire l'interfaccia di rete griglia per tutti i nodi StorageGRID sull'host; è possibile utilizzare un'interfaccia di rete host diversa per ciascun nodo oppure eseguire operazioni intermedie. Tuttavia, in genere, non è possibile fornire la stessa interfaccia di rete host delle interfacce Grid e Admin Network per un singolo nodo o Grid Network per un nodo e Client Network per un altro.

Puoi completare questa attività in molti modi. Ad esempio, se gli host sono macchine virtuali e si stanno implementando uno o due nodi StorageGRID per ciascun host, è possibile creare il numero corretto di interfacce di rete nell'hypervisor e utilizzare un mapping 1-to-1. Se si implementano più nodi su host bare metal per uso in produzione, è possibile sfruttare il supporto dello stack di rete Linux per VLAN e LACP per la fault tolerance e la condivisione della larghezza di banda. Le sezioni seguenti forniscono approcci dettagliati per entrambi questi esempi. Non è necessario utilizzare nessuno di questi esempi: È possibile utilizzare qualsiasi approccio che soddisfi le proprie esigenze.

> Non utilizzare dispositivi bond o bridge direttamente come interfaccia di rete container. In questo modo si potrebbe impedire l'avvio del nodo causato da un problema del kernel con l'utilizzo di MACVLAN con dispositivi bond e bridge nello spazio dei nomi container. Utilizzare invece un dispositivo non-bond, ad esempio una coppia VLAN o Virtual Ethernet (veth). Specificare questo dispositivo come interfaccia di rete nel file di configurazione del nodo.

Informazioni correlate

"Creazione di file di configurazione del nodo"

Considerazioni e consigli per la clonazione degli indirizzi MAC

La clonazione dell'indirizzo MAC fa in modo che il container utilizzi l'indirizzo MAC dell'host e l'host utilizzi l'indirizzo MAC di un indirizzo specificato o generato in modo casuale. È necessario utilizzare la clonazione dell'indirizzo MAC per evitare l'utilizzo di configurazioni di rete in modalità promiscua.

Abilitazione della clonazione MAC

In alcuni ambienti, la sicurezza può essere migliorata mediante la clonazione dell'indirizzo MAC, in quanto consente di utilizzare una NIC virtuale dedicata per Admin Network, Grid Network e Client Network. Il fatto che il container utilizzi l'indirizzo MAC della scheda NIC dedicata sull'host consente di evitare l'utilizzo di configurazioni di rete promiscue mode.

> La clonazione dell'indirizzo MAC è destinata all'utilizzo con le installazioni di server virtuali e potrebbe non funzionare correttamente con tutte le configurazioni fisiche delle appliance.

Se un nodo non si avvia a causa di un'interfaccia di destinazione per la clonazione MAC occupata, potrebbe essere necessario impostare il collegamento su "inattivo" prima di avviare il nodo. Inoltre, è possibile che l'ambiente virtuale impedisca la clonazione MAC su un'interfaccia di rete mentre il collegamento è attivo. Se un nodo non riesce a impostare l'indirizzo MAC e si avvia a causa di un'interfaccia occupata, impostare il collegamento su "inattivo" prima di avviare il nodo potrebbe risolvere il problema.

La clonazione dell'indirizzo MAC è disattivata per impostazione predefinita e deve essere impostata mediante le chiavi di configurazione del nodo. È necessario attivarlo quando si installa StorageGRID.

Per ogni rete è disponibile una chiave:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Impostando la chiave su "true", il container utilizza l'indirizzo MAC della NIC dell'host. Inoltre, l'host utilizzerà l'indirizzo MAC della rete container specificata. Per impostazione predefinita, l'indirizzo del contenitore è un indirizzo generato in modo casuale, ma se ne è stato impostato uno utilizzando `_NETWORK_MAC` chiave di configurazione del nodo, viene utilizzato l'indirizzo. L'host e il container avranno sempre indirizzi MAC diversi.

L'attivazione della clonazione MAC su un host virtuale senza attivare anche la modalità promiscua sull'hypervisor potrebbe causare l'interruzione del funzionamento della rete host Linux che utilizza l'interfaccia dell'host.

Casi di utilizzo della clonazione MAC

Esistono due casi di utilizzo da considerare con la clonazione MAC:

- CLONAZIONE MAC non abilitata: Quando `_CLONE_MAC` La chiave nel file di configurazione del nodo non è impostata, o impostata su "false", l'host utilizzerà il MAC NIC host e il container avrà un MAC generato da StorageGRID, a meno che non sia specificato un MAC in `_NETWORK_MAC` chiave. Se un indirizzo è impostato in `_NETWORK_MAC` il contenitore avrà l'indirizzo specificato in `_NETWORK_MAC` chiave. Questa configurazione delle chiavi richiede l'utilizzo della modalità promiscua.
- CLONAZIONE MAC abilitata: Quando `_CLONE_MAC` La chiave nel file di configurazione del nodo è impostata su "true", il container utilizza il MAC NIC host e l'host utilizza un MAC generato da StorageGRID, a meno che non sia specificato un MAC in `_NETWORK_MAC` chiave. Se un indirizzo è impostato in `_NETWORK_MAC` l'host utilizza l'indirizzo specificato invece di quello generato. In questa configurazione di chiavi, non si dovrebbe utilizzare la modalità promiscua.

Se non si desidera utilizzare la clonazione dell'indirizzo MAC e si desidera consentire a tutte le interfacce di ricevere e trasmettere dati per indirizzi MAC diversi da quelli assegnati dall'hypervisor, Assicurarsi che le proprietà di sicurezza a livello di switch virtuale e gruppo di porte siano impostate su **Accept** per modalità promiscuous, modifiche indirizzo MAC e trasmissione forgiata. I valori impostati sullo switch virtuale possono essere sovrascritti dai valori a livello di gruppo di porte, quindi assicurarsi che le impostazioni siano le stesse in entrambe le posizioni.

Per attivare la clonazione MAC, consultare "istruzioni per la creazione dei file di configurazione del nodo".

Esempio di clonazione MAC

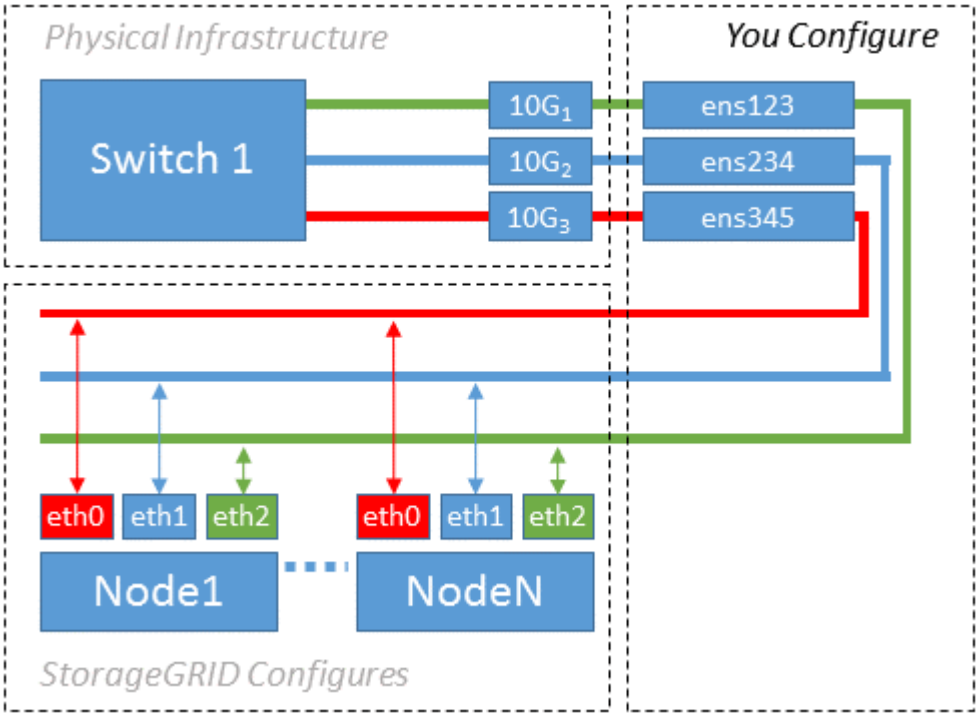
Esempio di clonazione MAC abilitata con un host con indirizzo MAC 11:22:33:44:55:66 per l'interfaccia ens256 e le seguenti chiavi nel file di configurazione del nodo:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Risultato: Il MAC host per ens256 è b2:9c:02:c2:27:10 e il MAC Admin Network è 11:22:33:44:55:66

Esempio 1: Mappatura 1 a 1 su NIC fisiche o virtuali

L'esempio 1 descrive una semplice mappatura dell'interfaccia fisica che richiede una configurazione minima o nulla sul lato host.



Il sistema operativo Linux crea `ensXYZ` si interfaccia automaticamente durante l'installazione o l'avvio o quando le interfacce vengono aggiunte a caldo. Non è richiesta alcuna configurazione se non quella di garantire che le interfacce siano impostate in modo che si avviino automaticamente dopo l'avvio. È necessario determinare quale `ensXYZ` Corrisponde a quale rete StorageGRID (griglia, amministratore o client) in modo da poter fornire le mappature corrette in un secondo momento del processo di configurazione.

Si noti che la figura mostra più nodi StorageGRID; tuttavia, normalmente si utilizza questa configurazione per macchine virtuali a nodo singolo.

Se lo switch 1 è uno switch fisico, configurare le porte collegate alle interfacce da 10G1 a 10G3 per la modalità di accesso e posizionarle sulle VLAN appropriate.

Esempio 2: Collegamento LACP con VLAN

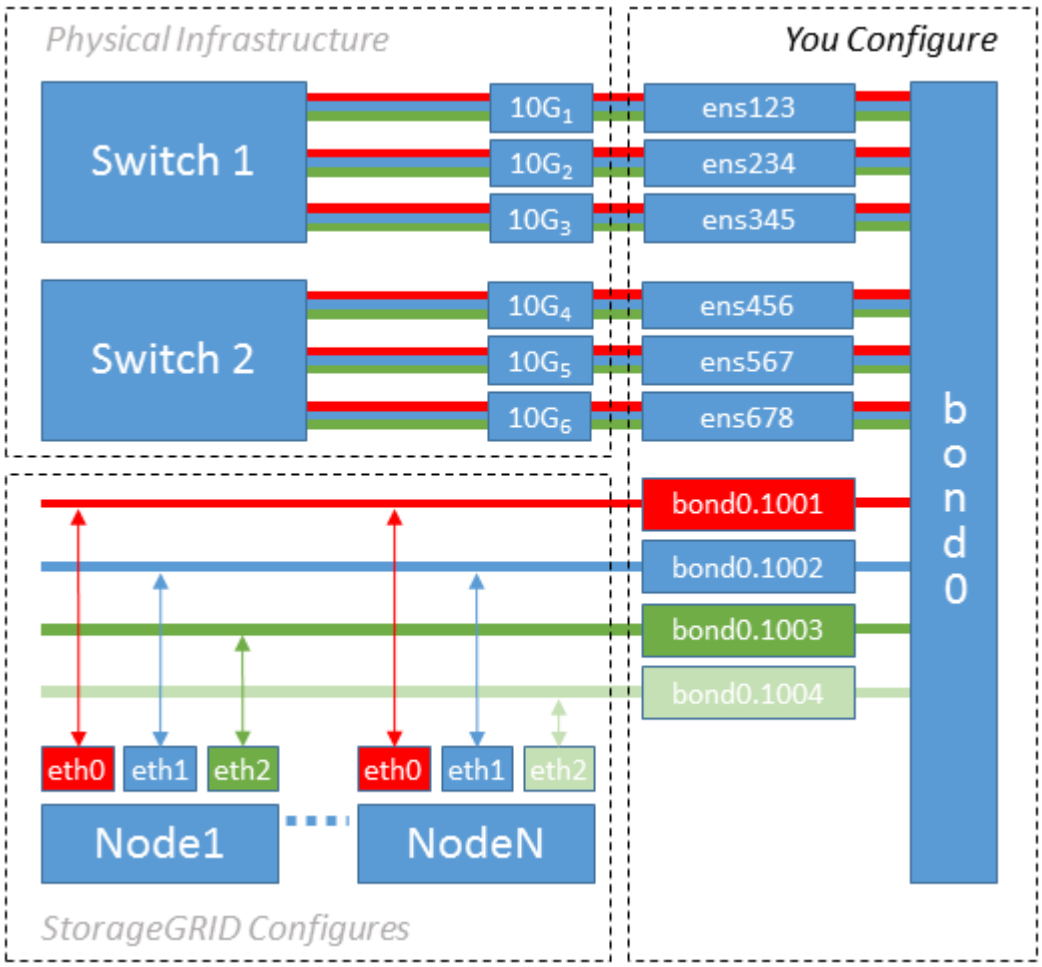
A proposito di questa attività

L'esempio 2 presuppone che si abbia familiarità con il bonding delle interfacce di rete e con la creazione di interfacce VLAN sulla distribuzione Linux in uso.

L'esempio 2 descrive uno schema generico, flessibile e basato su VLAN che facilita la condivisione di tutta la larghezza di banda di rete disponibile in tutti i nodi su un singolo host. Questo esempio è particolarmente applicabile agli host bare metal.

Per comprendere questo esempio, si supponga di disporre di tre subnet separate per le reti Grid, Admin e Client in ogni data center. Le sottoreti si trovano su VLAN separate (1001, 1002 e 1003) e vengono presentate all'host su una porta di trunk collegata LACP (bond0). Configurare tre interfacce VLAN sul bond: Bond0.1001, bond0.1002 e bond0.1003.

Se si richiedono VLAN e subnet separate per le reti di nodi sullo stesso host, è possibile aggiungere interfacce VLAN sul collegamento e mapparle nell'host (come illustrato nella figura come bond0.1004).



Fasi

1. Aggregare tutte le interfacce di rete fisiche che verranno utilizzate per la connettività di rete StorageGRID in un unico collegamento LACP.

   Utilizzare lo stesso nome per il bond su ogni host. Ad esempio, `bond0`.

2. Creare interfacce VLAN che utilizzano questo collegamento come "dispositivo fisico" associato utilizzando la convenzione di denominazione dell'interfaccia VLAN standard `physdev-name.VLAN ID`.

   I passi 1 e 2 richiedono una configurazione appropriata sugli edge switch che terminano le altre estremità

dei collegamenti di rete. Le porte degli edge switch devono anche essere aggregate in un canale di porta LACP, configurate come trunk e in grado di passare tutte le VLAN richieste.

Vengono forniti file di configurazione dell'interfaccia di esempio per questo schema di configurazione di rete per host.

Informazioni correlate

"Esempio di /etc/sysconfig/network-scripts"

Configurare lo storage host

È necessario allocare volumi di storage a blocchi a ciascun host.

Prima di iniziare

Sono stati esaminati i seguenti argomenti, che forniscono le informazioni necessarie per eseguire questa attività:

"Requisiti di storage e performance"

"Requisiti per la migrazione dei container di nodi"

A proposito di questa attività

Quando si allocano i volumi di storage a blocchi (LUN) agli host, utilizzare le tabelle in "requisiti di archiviazione" per determinare quanto segue:

- Numero di volumi richiesti per ciascun host (in base al numero e ai tipi di nodi che verranno implementati su tale host)
- Categoria di storage per ciascun volume (ovvero dati di sistema o dati oggetto)
- Dimensione di ciascun volume

Quando si distribuiscono i nodi StorageGRID sull'host, verranno utilizzate queste informazioni e il nome persistente assegnato da Linux a ciascun volume fisico.

> Non è necessario partizionare, formattare o montare nessuno di questi volumi; è sufficiente assicurarsi che siano visibili agli host.

> È necessaria una sola LUN per i dati degli oggetti per i nodi di storage basati solo sui metadati.

Evitare di utilizzare file speciali "RAW" del dispositivo (`/dev/sdb`, ad esempio) mentre si compone l'elenco dei nomi dei volumi. Questi file possono cambiare durante i riavvii dell'host, il che avrà un impatto sul corretto funzionamento del sistema. Se si utilizzano LUN iSCSI e multipathing di Device Mapper, considerare l'utilizzo di alias multipath in `/dev/mapper` Directory, soprattutto se la topologia SAN include percorsi di rete ridondanti per lo storage condiviso. In alternativa, è possibile utilizzare i softlink creati dal sistema in `/dev/disk/by-path/` per i nomi persistenti dei dispositivi.

Ad esempio:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

I risultati saranno diversi per ogni installazione.

Assegnare nomi descrittivi a ciascuno di questi volumi di storage a blocchi per semplificare l'installazione iniziale di StorageGRID e le future procedure di manutenzione. Se si utilizza il driver multipath del device mapper per l'accesso ridondante ai volumi di storage condivisi, è possibile utilizzare `alias` nel campo `/etc/multipath.conf` file.

Ad esempio:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

In questo modo, gli alias verranno visualizzati come dispositivi a blocchi in `/dev/mapper` directory sull'host, che consente di specificare un nome semplice e facilmente validato ogni volta che un'operazione di configurazione o manutenzione richiede la specifica di un volume di storage a blocchi.

> Se si imposta lo storage condiviso per supportare la migrazione dei nodi StorageGRID e si utilizza il multipathing di Device Mapper, è possibile creare e installare un file comune `/etc/multipath.conf` su tutti gli host co-locati. Assicurarsi di utilizzare un volume di storage diverso per il motore dei container su ciascun host. L'utilizzo di alias e l'inclusione del nome host di destinazione nell'alias per ogni LUN del volume di storage del motore di container faciliteranno la memorizzazione ed è consigliato.

Informazioni correlate

"Configurare il volume di storage del motore dei container"

Configurare il volume di storage del motore dei container

Prima di installare il motore dei container (Docker o Podman), potrebbe essere necessario formattare il volume di storage e montarlo.

A proposito di questa attività

È possibile saltare questi passaggi se si intende utilizzare lo storage locale per il volume di storage Docker o Podman e si dispone di spazio sufficiente sulla partizione host contenente `/var/lib/docker` Per Docker e. `/var/lib/containers` Per Podman.

Podman è supportato solo su Red Hat Enterprise Linux (RHEL).

Fasi

1. Creare un file system sul volume di storage del motore dei container:

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

2. Montare il volume di storage del motore dei container:
   - Per Docker:

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

   - Per Podman:

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

3. Aggiungere una voce per container-storage-volume-device a /etc/fstab.

   Questo passaggio garantisce che il volume di storage venga rimontato automaticamente dopo il riavvio dell'host.

Installare Docker

Il sistema StorageGRID viene eseguito su Red Hat Enterprise Linux come una raccolta di container. Se si è scelto di utilizzare il motore Docker Container, seguire questa procedura per installare Docker. In caso contrario, Installare Podman.

Fasi

1. Installare Docker seguendo le istruzioni per la distribuzione Linux.

   Se Docker non è incluso nella distribuzione Linux, è possibile scaricarlo dal sito Web di Docker.

2. Assicurarsi che Docker sia stato attivato e avviato eseguendo i seguenti due comandi:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Verificare di aver installato la versione prevista di Docker inserendo quanto segue:

```
sudo docker version
```

Le versioni del client e del server devono essere 1.11.0 o successive.

Installare Podman

Il sistema StorageGRID viene eseguito su Red Hat Enterprise Linux come una raccolta di container. Se hai scelto di utilizzare il motore container Podman, segui questa procedura per installare Podman. In caso contrario, Installare Docker.

Podman è supportato solo su Red Hat Enterprise Linux (RHEL).

Fasi

1. Installare Podman e Podman-Docker seguendo le istruzioni per la distribuzione Linux.

Devi anche installare il pacchetto Podman-Docker quando installi Podman.

2. Verificare di aver installato la versione prevista di Podman e Podman-Docker inserendo quanto segue:

```
sudo docker version
```

Il pacchetto Podman-Docker consente di utilizzare i comandi Docker.

Le versioni Client e Server devono essere 3.2.3 o successive.

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

Installare i servizi host StorageGRID

Si utilizza il pacchetto RPM di StorageGRID per installare i servizi host di StorageGRID.

A proposito di questa attività

Queste istruzioni descrivono come installare i servizi host dai pacchetti RPM. In alternativa, è possibile utilizzare i metadati del repository Yum inclusi nell'archivio di installazione per installare i pacchetti RPM in remoto. Consultare le istruzioni del repository Yum per il sistema operativo Linux in uso.

Fasi

1. Copiare i pacchetti RPM di StorageGRID in ciascuno degli host o renderli disponibili nello storage condiviso.

   Ad esempio, inserirli in `/tmp` directory, in modo da poter utilizzare il comando di esempio nel passaggio successivo.

2. Accedere a ciascun host come root o utilizzando un account con autorizzazione sudo ed eseguire i seguenti comandi nell'ordine specificato:

   ```
   sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
   ```

   ```
   sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
   ```

   È necessario installare prima il pacchetto immagini e poi il pacchetto servizi.

   Se i pacchetti sono inseriti in una directory diversa da `/tmp`, modificare il comando in modo che rifletta il percorso utilizzato.

Automatizzare l'installazione di StorageGRID su Red Hat Enterprise Linux

È possibile automatizzare l'installazione del servizio host StorageGRID e la configurazione dei nodi di rete.

L'automazione della distribuzione può essere utile in uno dei seguenti casi:

- Si utilizza già un framework di orchestrazione standard, ad esempio Ansible, Puppet o Chef, per implementare e configurare host fisici o virtuali.
- Si intende implementare più istanze di StorageGRID.
- Si sta implementando un'istanza di StorageGRID grande e complessa.

Il servizio host StorageGRID viene installato da un pacchetto e gestito da file di configurazione. È possibile creare i file di configurazione utilizzando uno dei seguenti metodi:

- "Creare i file di configurazione" durante un'installazione manuale.
- Preparare i file di configurazione in anticipo (o a livello di programmazione) per consentire l'installazione automatica utilizzando framework di orchestrazione standard, come descritto in questo articolo.

  StorageGRID fornisce script Python opzionali per automatizzare la configurazione delle appliance StorageGRID e dell'intero sistema StorageGRID (il "grid"). È possibile utilizzare questi script direttamente o controllarli per imparare a utilizzare "API REST per l'installazione di StorageGRID" nei tool di

configurazione e implementazione grid ti sviluppi da soli.

Automatizzare l'installazione e la configurazione del servizio host StorageGRID

È possibile automatizzare l'installazione del servizio host StorageGRID utilizzando framework di orchestrazione standard come Ansible, Puppet, Chef, Fabric o SaltStack.

Il servizio host di StorageGRID è confezionato in un RPM ed è gestito da file di configurazione che è possibile preparare in anticipo (o a livello di programmazione) per consentire l'installazione automatica. Se già utilizzi un framework di orchestrazione standard per installare e configurare RHEL, aggiungere StorageGRID ai tuoi playbook o alle tue ricette dovrebbe essere semplice.

Vedere l'esempio di Ansible Role and Playbook in `/extras` cartella fornita con l'archivio di installazione. Il playbook Ansible mostra come `storagegrid` Role prepara l'host e installa StorageGRID sui server di destinazione. È possibile personalizzare il ruolo o il manuale in base alle esigenze.

> Il manuale di esempio non include i passaggi necessari per creare dispositivi di rete prima di avviare il servizio host StorageGRID. Aggiungi questi passaggi prima di finalizzare e utilizzare il playbook.

È possibile automatizzare tutti i passaggi per la preparazione degli host e l'implementazione dei nodi virtual grid.

Esempio di Ansible role and playbook

Ad esempio, il ruolo e il playbook Ansible vengono forniti con l'archivio di installazione nel `/extras` cartella. Il playbook Ansible mostra come `storagegrid` Il ruolo prepara gli host e installa StorageGRID sui server di destinazione. È possibile personalizzare il ruolo o il manuale in base alle esigenze.

Automatizzare la configurazione di StorageGRID

Una volta implementati i nodi grid, è possibile automatizzare la configurazione del sistema StorageGRID.

Prima di iniziare

- Si conosce la posizione dei seguenti file dall'archivio di installazione.

Nome file	Descrizione
configure-storagegrid.py	Script Python utilizzato per automatizzare la configurazione
configure-storagegrid.sample.json	File di configurazione di esempio da utilizzare con lo script
configure-storagegrid.blank.json	File di configurazione vuoto da utilizzare con lo script

- È stato creato un `configure-storagegrid.json` file di configurazione. Per creare questo file, è possibile modificare il file di configurazione di esempio (`configure-storagegrid.sample.json`) o il file di configurazione vuoto (`configure-storagegrid.blank.json`).

A proposito di questa attività

È possibile utilizzare `configure-storagegrid.py` Script Python e il `configure-storagegrid.json` File di configurazione per automatizzare la configurazione del sistema StorageGRID.

È inoltre possibile configurare il sistema utilizzando Grid Manager o l'API di installazione.

Fasi

1. Accedere alla macchina Linux in uso per eseguire lo script Python.
2. Passare alla directory in cui è stato estratto l'archivio di installazione.

   Ad esempio:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   dove `platform` è `debs`, `rpms`, o. `vsphere`.

3. Eseguire lo script Python e utilizzare il file di configurazione creato.

   Ad esempio:

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Risultato

Un pacchetto di ripristino `.zip` il file viene generato durante il processo di configurazione e scaricato nella directory in cui si esegue il processo di installazione e configurazione. È necessario eseguire il backup del file del pacchetto di ripristino in modo da poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi della griglia. Ad esempio, copiarla in una posizione di rete sicura e di backup e in una posizione di cloud storage sicura.

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.

Se è stata specificata la generazione di password casuali, aprire `Passwords.txt` E cercare le password necessarie per accedere al sistema StorageGRID.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Il sistema StorageGRID viene installato e configurato quando viene visualizzato un messaggio di conferma.

```
StorageGRID has been configured and installed.
```

Informazioni correlate

"Panoramica dell'API REST per l'installazione"

Implementare nodi grid virtuali (Red Hat)

Creare file di configurazione dei nodi per le implementazioni di Red Hat Enterprise Linux

I file di configurazione dei nodi sono piccoli file di testo che forniscono le informazioni necessarie al servizio host StorageGRID per avviare un nodo e collegarlo alla rete appropriata e bloccare le risorse di storage. I file di configurazione dei nodi vengono utilizzati per i nodi virtuali e non per i nodi appliance.

Posizione dei file di configurazione dei nodi

Posizionare il file di configurazione per ogni nodo StorageGRID in `/etc/storagegrid/nodes` directory sull'host in cui verrà eseguito il nodo. Ad esempio, se si intende eseguire un nodo Admin, un nodo Gateway e un nodo Storage sull'host, è necessario inserire tre file di configurazione del nodo `/etc/storagegrid/nodes` Su host.

È possibile creare i file di configurazione direttamente su ciascun host utilizzando un editor di testo, ad esempio vim o nano, oppure crearli altrove e spostarli su ciascun host.

Denominazione dei file di configurazione dei nodi

I nomi dei file di configurazione sono significativi. Il formato è `node-name.conf`, dove `node-name` è un nome assegnato al nodo. Questo nome viene visualizzato nel programma di installazione di StorageGRID e viene utilizzato per le operazioni di manutenzione dei nodi, ad esempio la migrazione dei nodi.

I nomi dei nodi devono seguire queste regole:

- Deve essere unico
- Deve iniziare con una lettera
- Può contenere i caratteri Da A a Z e da a a z
- Può contenere i numeri da 0 a 9
- Può contenere uno o più trattini (-)
- Non deve contenere più di 32 caratteri, ad eccezione di `.conf` interno

Qualsiasi file in `/etc/storagegrid/nodes` che non seguono queste convenzioni di denominazione non verranno analizzata dal servizio host.

Se è stata pianificata una topologia multi-sito per il proprio grid, uno schema di denominazione tipico dei nodi potrebbe essere:

```
site-nodetype-nodenumber.conf
```

Ad esempio, è possibile utilizzare `dc1-adm1.conf` Per il primo nodo Admin nel data center 1, e. `dc2-sn3.conf` Per il terzo nodo di storage nel data center 2. Tuttavia, è possibile utilizzare qualsiasi schema desiderato, purché tutti i nomi dei nodi seguano le regole di denominazione.

Contenuto di un file di configurazione del nodo

Un file di configurazione contiene coppie chiave/valore, con una chiave e un valore per riga. Per ogni coppia chiave/valore, attenersi alle seguenti regole:

- La chiave e il valore devono essere separati da un segno di uguale (=) e spazio vuoto opzionale.
- Le chiavi non possono contenere spazi.
- I valori possono contenere spazi incorporati.
- Qualsiasi spazio iniziale o finale viene ignorato.

La tabella seguente definisce i valori per tutte le chiavi supportate. Ogni chiave ha una delle seguenti designazioni:

- **Obbligatorio**: Richiesto per ogni nodo o per i tipi di nodo specificati
- **Best practice**: Facoltativo, anche se consigliato
- **Opzionale**: Opzionale per tutti i nodi

Chiavi di rete Admin

ADMIN_IP

Valore	Designazione
Grid Network IPv4 address del nodo di amministrazione principale per la griglia a cui appartiene questo nodo. Utilizzare lo stesso valore specificato per GRID_NETWORK_IP per il nodo Grid con NODE_TYPE = VM_Admin_Node e ADMIN_ROLE = Primary. Se si omette questo parametro, il nodo tenta di rilevare un nodo Admin primario utilizzando mDNS. "In che modo i nodi della griglia rilevano il nodo di amministrazione primario" **Nota**: Questo valore viene ignorato e potrebbe essere proibito sul nodo di amministrazione primario.	Best practice

ADMIN_NETWORK_CONFIG

Valore	Designazione
DHCP, STATICO O DISATTIVATO	Opzionale

ADMIN_NETWORK_ESL

Valore	Designazione
Elenco separato da virgole delle subnet nella notazione CIDR a cui il nodo deve comunicare utilizzando il gateway Admin Network. Esempio: `172.16.0.0/21,172.17.0.0/21`	Opzionale

ADMIN_NETWORK_GATEWAY

Valore	Designazione

Indirizzo IPv4 del gateway Admin Network locale per questo nodo. Deve trovarsi nella subnet definita da ADMIN_NETWORK_IP e ADMIN_NETWORK_MASK. Questo valore viene ignorato per le reti configurate con DHCP.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessario se `ADMIN_NETWORK_ESL` viene specificato. Facoltativo altrimenti.

ADMIN_NETWORK_IP

Valore	Designazione

Indirizzo IPv4 di questo nodo nella rete di amministrazione. Questa chiave è necessaria solo quando ADMIN_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessario quando ADMIN_NETWORK_CONFIG = STATICO.
	
	Facoltativo altrimenti.

ADMIN_NETWORK_MAC

Valore	Designazione
L'indirizzo MAC dell'interfaccia Admin Network nel contenitore. Questo campo è facoltativo. Se omesso, viene generato automaticamente un indirizzo MAC. Devono essere 6 coppie di cifre esadecimali separate da due punti. Esempio: `b2:9c:02:c2:27:10`	Opzionale

ADMIN_NETWORK_MASK

Valore	Designazione

Netmask IPv4 per questo nodo, sulla rete di amministrazione. Specificare questa chiave quando ADMIN_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessario se viene specificato ADMIN_NETWORK_IP e ADMIN_NETWORK_CONFIG = STATICO.
	
	Facoltativo altrimenti.

ADMIN_NETWORK_MTU

Valore	Designazione

MTU (Maximum Transmission Unit) per questo nodo nella rete di amministrazione. Non specificare se ADMIN_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omesso, viene utilizzato 1500.
 	
Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito.
 	
IMPORTANTE: Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.
 	
Esempi:
 	
`1500`
 	
`8192`
	Opzionale

ADMIN_NETWORK_TARGET

Valore	Designazione

Nome del dispositivo host che verrà utilizzato per l'accesso alla rete amministrativa dal nodo StorageGRID. Sono supportati solo i nomi delle interfacce di rete. In genere, si utilizza un nome di interfaccia diverso da quello specificato per GRID_NETWORK_TARGET o CLIENT_NETWORK_TARGET.
 	
Nota: Non utilizzare dispositivi bond o bridge come destinazione di rete. Configurare una VLAN (o un'altra interfaccia virtuale) sulla parte superiore del dispositivo bond oppure utilizzare una coppia di bridge e Virtual Ethernet (veth).
 	
Best practice:specificare un valore anche se questo nodo inizialmente non dispone di un indirizzo IP Admin Network. Quindi, è possibile aggiungere un indirizzo IP Admin Network in un secondo momento, senza dover riconfigurare il nodo sull'host.
 	
Esempi:
 	
`bond0.1002`
 	
`ens256`
	Best practice

ADMIN_NETWORK_TARGET_TYPE

Valore	Designazione
Interfaccia (questo è l'unico valore supportato).	Opzionale

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o Falso Impostare la chiave su "true" per fare in modo che il container StorageGRID utilizzi l'indirizzo MAC dell'interfaccia host di destinazione sulla rete di amministrazione. **Best practice:** nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare la chiave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per ulteriori informazioni sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Ubuntu o Debian)"	Best practice

RUOLO_AMMINISTRATORE

Valore	Designazione
Primario o non primario Questa chiave è necessaria solo quando NODE_TYPE = VM_Admin_Node; non specificarla per altri tipi di nodo.	Necessario quando NODE_TYPE = VM_Admin_Node Facoltativo altrimenti.

Bloccare le chiavi del dispositivo

BLOCK_DEVICE_AUDIT_LOGS

Valore	Designazione

Percorso e nome del file speciale del dispositivo a blocchi utilizzato da questo nodo per la memorizzazione persistente dei registri di controllo.
 	
Esempi:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	Richiesto per i nodi con NODE_TYPE = VM_Admin_NODE. Non specificarlo per altri tipi di nodi.

BLOCK_DEVICE_RANGEDB_NNN

Valore	Designazione

Percorso e nome del file speciale del dispositivo a blocchi utilizzato da questo nodo per lo storage a oggetti persistente. Questa chiave è necessaria solo per i nodi con NODE_TYPE = VM_Storage_Node; non specificarla per altri tipi di nodo.
 	
È necessario solo BLOCK_DEVICE_RANGEDB_000; gli altri sono facoltativi. Il dispositivo a blocchi specificato per BLOCK_DEVICE_RANGEDB_000 deve essere di almeno 4 TB; gli altri possono essere più piccoli.
 	
Non lasciare lacune. Se si specifica BLOCK_DEVICE_RANGEDB_005, è necessario specificare ANCHE BLOCK_DEVICE_RANGEDB_004.
 	
Nota: Per la compatibilità con le implementazioni esistenti, sono supportate chiavi a due cifre per i nodi aggiornati.
 	
Esempi:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	Richiesti:
	
	BLOCK_DEVICE_RANGEDB_000
	
	Opzionale:
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002
	
	BLOCK_DEVICE_RANGEDB_003
	
	BLOCK_DEVICE_RANGEDB_004
	
	BLOCK_DEVICE_RANGEDB_005
	
	BLOCK_DEVICE_RANGEDB_006
	
	BLOCK_DEVICE_RANGEDB_007
	
	BLOCK_DEVICE_RANGEDB_008
	
	BLOCK_DEVICE_RANGEDB_009
	
	BLOCK_DEVICE_RANGEDB_010
	
	BLOCK_DEVICE_RANGEDB_011
	
	BLOCK_DEVICE_RANGEDB_012
	
	BLOCK_DEVICE_RANGEDB_013
	
	BLOCK_DEVICE_RANGEDB_014
	
	BLOCK_DEVICE_RANGEDB_015

BLOCK_DEVICE_TABLES

Valore	Designazione

Percorso e nome del file speciale del dispositivo a blocchi utilizzato da questo nodo per l'archiviazione persistente delle tabelle di database. Questa chiave è necessaria solo per i nodi con NODE_TYPE = VM_Admin_Node; non specificarla per altri tipi di nodo.
 	
Esempi:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	Obbligatorio

BLOCK_DEVICE_VAR_LOCAL

Valore	Designazione

Percorso e nome del file speciale del dispositivo di blocco utilizzato da questo nodo per ITS `/var/local` storage persistente.
 	
Esempi:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	Obbligatorio

Chiavi di rete client

CONFIGURAZIONE_RETE_CLIENT

Valore	Designazione
DHCP, STATICO O DISATTIVATO	Opzionale

GATEWAY_RETE_CLIENT

Valore	Designazione

Indirizzo IPv4 del gateway di rete client locale per questo nodo, che deve trovarsi sulla subnet definita da CLIENT_NETWORK_IP e CLIENT_NETWORK_MASK. Questo valore viene ignorato per le reti configurate con DHCP.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Opzionale

IP_RETE_CLIENT

Valore	Designazione

Indirizzo IPv4 di questo nodo sulla rete client.
 	
Questa chiave è necessaria solo quando CLIENT_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessario quando CLIENT_NETWORK_CONFIG = STATICO
	
	Facoltativo altrimenti.

CLIENT_NETWORK_MAC

Valore	Designazione
L'indirizzo MAC dell'interfaccia di rete client nel contenitore. Questo campo è facoltativo. Se omesso, viene generato automaticamente un indirizzo MAC. Devono essere 6 coppie di cifre esadecimali separate da due punti. Esempio: `b2:9c:02:c2:27:20`	Opzionale

CLIENT_NETWORK_MASK

Valore	Designazione

Netmask IPv4 per questo nodo sulla rete client.
 	
Specificare questa chiave quando CLIENT_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessario se viene specificato CLIENT_NETWORK_IP e CLIENT_NETWORK_CONFIG = STATICO
	
	Facoltativo altrimenti.

MTU_RETE_CLIENT

Valore	Designazione

MTU (Maximum Transmission Unit) per questo nodo sulla rete client. Non specificare se CLIENT_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omesso, viene utilizzato 1500.
 	
Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito.
 	
IMPORTANTE: Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.
 	
Esempi:
 	
`1500`
 	
`8192`
	Opzionale

DESTINAZIONE_RETE_CLIENT

Valore	Designazione

Nome del dispositivo host che verrà utilizzato per l'accesso alla rete client dal nodo StorageGRID. Sono supportati solo i nomi delle interfacce di rete. In genere, si utilizza un nome di interfaccia diverso da quello specificato per GRID_NETWORK_TARGET o ADMIN_NETWORK_TARGET.
 	
Nota: Non utilizzare dispositivi bond o bridge come destinazione di rete. Configurare una VLAN (o un'altra interfaccia virtuale) sulla parte superiore del dispositivo bond oppure utilizzare una coppia di bridge e Virtual Ethernet (veth).
 	
Best practice: specificare un valore anche se questo nodo inizialmente non avrà un indirizzo IP di rete client. Quindi, è possibile aggiungere un indirizzo IP di rete client in un secondo momento, senza dover riconfigurare il nodo sull'host.
 	
Esempi:
 	
`bond0.1003`
 	
`ens423`
	Best practice

TIPO_DESTINAZIONE_RETE_CLIENT

Valore	Designazione
Interfaccia (solo valore supportato).	Opzionale

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o Falso Impostare la chiave su "true" per fare in modo che il container StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete client. **Best practice:** nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per ulteriori informazioni sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Ubuntu o Debian)"	Best practice

Chiavi di rete della griglia

GRID_NETWORK_CONFIG

Valore	Designazione
STATICO o DHCP Se non specificato, il valore predefinito è STATICO.	Best practice

GRID_NETWORK_GATEWAY

Valore	Designazione
Indirizzo IPv4 del gateway Grid Network locale per questo nodo, che deve trovarsi sulla subnet definita da GRID_NETWORK_IP e GRID_NETWORK_MASK. Questo valore viene ignorato per le reti configurate con DHCP. Se Grid Network è una singola subnet senza gateway, utilizzare l'indirizzo del gateway standard per la subnet (X. YY.Z.1) o il valore GRID_NETWORK_IP di questo nodo; entrambi i valori semplificheranno le future espansioni Grid Network.	Obbligatorio

IP_RETE_GRIGLIA

Valore	Designazione

Indirizzo IPv4 di questo nodo sulla rete griglia. Questa chiave è necessaria solo quando GRID_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessario quando GRID_NETWORK_CONFIG = STATICO
	
	Facoltativo altrimenti.

GRID_NETWORK_MAC

Valore	Designazione
L'indirizzo MAC dell'interfaccia Grid Network nel contenitore. Devono essere 6 coppie di cifre esadecimali separate da due punti. Esempio: `b2:9c:02:c2:27:30`	Opzionale Se omesso, viene generato automaticamente un indirizzo MAC.

GRID_NETWORK_MASK

Valore	Designazione

Netmask IPv4 per questo nodo sulla rete griglia. Specificare questa chiave quando GRID_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessario quando viene specificato GRID_NETWORK_IP e GRID_NETWORK_CONFIG = STATICO.
	
	Facoltativo altrimenti.

GRID_NETWORK_MTU

Valore	Designazione

MTU (Maximum Transmission Unit) per questo nodo sulla rete di rete. Non specificare se GRID_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omesso, viene utilizzato 1500.
 	
Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito.
 	
IMPORTANTE: Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.
 	
IMPORTANTE: Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete.
 	
Esempi:
 	
`1500`
 	
`8192`
	Opzionale

GRID_NETWORK_TARGET

Valore	Designazione

Nome del dispositivo host che verrà utilizzato per l'accesso alla rete griglia dal nodo StorageGRID. Sono supportati solo i nomi delle interfacce di rete. In genere, si utilizza un nome di interfaccia diverso da quello specificato per ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET.
 	
Nota: Non utilizzare dispositivi bond o bridge come destinazione di rete. Configurare una VLAN (o un'altra interfaccia virtuale) sulla parte superiore del dispositivo bond oppure utilizzare una coppia di bridge e Virtual Ethernet (veth).
 	
Esempi:
 	
`bond0.1001`
 	
`ens192`
	Obbligatorio

GRID_NETWORK_TARGET_TYPE

Valore	Designazione
Interfaccia (questo è l'unico valore supportato).	Opzionale

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o Falso Impostare il valore della chiave su "true" per fare in modo che il contenitore StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete di rete. **Best practice:** nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per ulteriori informazioni sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Ubuntu o Debian)"	Best practice

Interfaces key

INTERFACE_TARGET_nnnn

Valore	Designazione
Nome e descrizione opzionale per un'interfaccia aggiuntiva che si desidera aggiungere a questo nodo. È possibile aggiungere più interfacce aggiuntive a ciascun nodo. Per *nnnnn*, specificare un numero univoco per ogni voce di INTERFACCIA_TARGET che si sta aggiungendo. Per il valore, specificare il nome dell'interfaccia fisica sull'host bare-metal. Quindi, facoltativamente, aggiungere una virgola e fornire una descrizione dell'interfaccia, che viene visualizzata nella pagina delle interfacce VLAN e nella pagina dei gruppi ha. Esempio: `INTERFACE_TARGET_0001=ens256, Trunk` Se si aggiunge un'interfaccia di linea, è necessario configurare un'interfaccia VLAN in StorageGRID. Se si aggiunge un'interfaccia di accesso, è possibile aggiungerla direttamente a un gruppo ha; non è necessario configurare un'interfaccia VLAN.	Opzionale

Chiave RAM massima

MAXIMUM_RAM

Valore	Designazione

La quantità massima di RAM che questo nodo può consumare. Se questa chiave viene omessa, il nodo non presenta limitazioni di memoria. Quando si imposta questo campo per un nodo a livello di produzione, specificare un valore di almeno 24 GB e da 16 a 32 GB inferiore alla RAM totale di sistema.
 	
Nota: Il valore RAM influisce sullo spazio riservato ai metadati effettivi di un nodo. Vedere "Descrizione di Metadata Reserved Space".
 	
Il formato di questo campo è *`numberunit`*, dove *`unit`* può essere `b`, `k`, `m`, o. `g`.
 	
Esempi:
 	
`24g`
 	
`38654705664b`
 	
Nota: Se si desidera utilizzare questa opzione, è necessario abilitare il supporto del kernel per i gruppi di memoria.
	Opzionale

Chiave del tipo di nodo

NODE_TYPE

Valore	Designazione
Tipo di nodo: Nodo_amministrazione_VM Nodo_storage_VM Nodo_archivio_VM Gateway VM_API	Obbligatorio

Tasti di rimappatura delle porte

PORT_REMAP

Valore	Designazione
Consente di rimapare qualsiasi porta utilizzata da un nodo per comunicazioni interne al nodo di rete o comunicazioni esterne. Il rimapping delle porte è necessario se i criteri di rete aziendali limitano una o più porte utilizzate da StorageGRID, come descritto in "Comunicazioni interne al nodo di rete" oppure "Comunicazioni esterne". **IMPORTANTE**: Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico. **Nota**: Se è impostato solo PORT_REMAP, il mapping specificato viene utilizzato per le comunicazioni in entrata e in uscita. Se VIENE specificato anche PORT_REMAP_INBOUND, PORT_REMAP si applica solo alle comunicazioni in uscita. Il formato utilizzato è: *`network type/protocol/default port used by grid node/new port`*, dove *`network type`* è grid, admin o client, e. *`protocol`* è tcp o udp. Esempio: `PORT_REMAP = client/tcp/18082/443`	Opzionale

PORT_REMAP_INBOUND

Valore	Designazione

Consente di rimapare le comunicazioni in entrata alla porta specificata. Se si specifica PORT_REMAP_INBOUND ma non si specifica un valore per PORT_REMAP, le comunicazioni in uscita per la porta rimangono invariate. **IMPORTANTE**: Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico. Il formato utilizzato è: *`network type/protocol/remapped port /default port used by grid node`*, dove *`network type`* è grid, admin o client, e. *`protocol`* è tcp o udp. Esempio: `PORT_REMAP_INBOUND = grid/tcp/3022/22`	Opzionale

In che modo i nodi della griglia rilevano il nodo di amministrazione primario

I nodi Grid comunicano con il nodo Admin primario per la configurazione e la gestione. Ciascun nodo della griglia deve conoscere l'indirizzo IP del nodo di amministrazione primario sulla rete di griglia.

Per garantire che un nodo Grid possa accedere al nodo Admin primario, è possibile eseguire una delle seguenti operazioni durante l'implementazione del nodo:

- È possibile utilizzare IL parametro ADMIN_IP per inserire manualmente l'indirizzo IP del nodo di amministrazione primario.
- È possibile omettere il parametro ADMIN_IP per fare in modo che il nodo Grid rilevi automaticamente il valore. Il rilevamento automatico è particolarmente utile quando Grid Network utilizza DHCP per assegnare l'indirizzo IP al nodo di amministrazione primario.

Il rilevamento automatico del nodo di amministrazione primario viene eseguito utilizzando un sistema di nomi di dominio multicast (mDNS). Al primo avvio, il nodo di amministrazione primario pubblica il proprio indirizzo IP utilizzando mDNS. Gli altri nodi della stessa sottorete possono quindi ricercare l'indirizzo IP e acquisirlo automaticamente. Tuttavia, poiché il traffico IP multicast non è normalmente instradabile attraverso le sottoreti, i nodi su altre sottoreti non possono acquisire direttamente l'indirizzo IP del nodo di amministrazione primario.

Se si utilizza la ricerca automatica:

- È necessario includere l'impostazione ADMIN_IP per almeno un nodo Grid su qualsiasi subnet a cui non è collegato direttamente il nodo Admin primario. Questo nodo della griglia pubblicherà quindi l'indirizzo IP del nodo di amministrazione primario per gli altri nodi della subnet da rilevare con mDNS.
- Assicurarsi che l'infrastruttura di rete supporti il passaggio del traffico IP multi-cast all'interno di una subnet.

File di configurazione del nodo di esempio

È possibile utilizzare i file di configurazione dei nodi di esempio per configurare i file di configurazione dei nodi per il sistema StorageGRID. Gli esempi mostrano i file di configurazione dei nodi per tutti i tipi di nodi griglia.

Per la maggior parte dei nodi, è possibile aggiungere le informazioni di indirizzamento di Admin e Client Network (IP, mask, gateway e così via) quando si configura la griglia utilizzando Grid Manager o l'API di installazione. L'eccezione è il nodo di amministrazione principale. Se si desidera accedere all'indirizzo IP Admin Network del nodo di amministrazione principale per completare la configurazione della griglia (ad esempio perché la rete di griglia non viene instradata), è necessario configurare la connessione Admin Network per il nodo di amministrazione primario nel relativo file di configurazione del nodo. Questo è illustrato nell'esempio.

> Negli esempi, la destinazione di rete client è stata configurata come Best practice, anche se la rete client è disattivata per impostazione predefinita.

Esempio per nodo amministratore primario

Nome file di esempio: `/etc/storagegrid/nodes/dc1-adm1.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Esempio per nodo di storage

Esempio di nome del file: `/etc/storagegrid/nodes/dc1-sn1.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Esempio per nodo di archivio

Esempio di nome del file: `/etc/storagegrid/nodes/dc1-arc1.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Esempio per Gateway Node

Esempio di nome del file: `/etc/storagegrid/nodes/dc1-gw1.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Esempio di nodo amministrativo non primario

Esempio di nome del file: `/etc/storagegrid/nodes/dc1-adm2.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Convalidare la configurazione StorageGRID

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

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

```
sudo storagegrid node validate all
```

Se i file sono corretti, l'output mostra **PASSED** per ciascun file di configurazione, come mostrato nell'esempio.

> Quando si utilizza un solo LUN sui nodi solo metadati, è possibile che venga visualizzato un messaggio di avviso che può essere ignorato.

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

Per un'installazione automatica, è possibile eliminare questo output utilizzando `-q` oppure `--quiet` in `storagegrid` command (ad esempio, `storagegrid --quiet…`). Se si elimina l'output, il comando avrà un valore di uscita diverso da zero se vengono rilevati avvisi o errori di configurazione.

Se i file di configurazione non sono corretti, i problemi vengono visualizzati come **WARNING** e **ERROR**, come mostrato nell'esempio. Se vengono rilevati errori di configurazione, è necessario correggerli prima di procedere con l'installazione.

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

Avviare il servizio host StorageGRID

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

Fasi

1. Eseguire i seguenti comandi su ciascun host:

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

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

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

3. Se un nodo restituisce lo stato "Not Running" (non in esecuzione) o "Stopped" (arrestato), eseguire il comando seguente:

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

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

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

Configurare la griglia e completare l'installazione (Red Hat)

Accedere a Grid Manager

Il Gestore griglia consente di definire tutte le informazioni necessarie per configurare il sistema StorageGRID.

Prima di iniziare

Il nodo di amministrazione primario deve essere implementato e aver completato la sequenza di avvio iniziale.

Fasi

1. Aprire il browser Web e accedere a uno dei seguenti indirizzi:

   `https://primary_admin_node_ip`

   `client_network_ip`

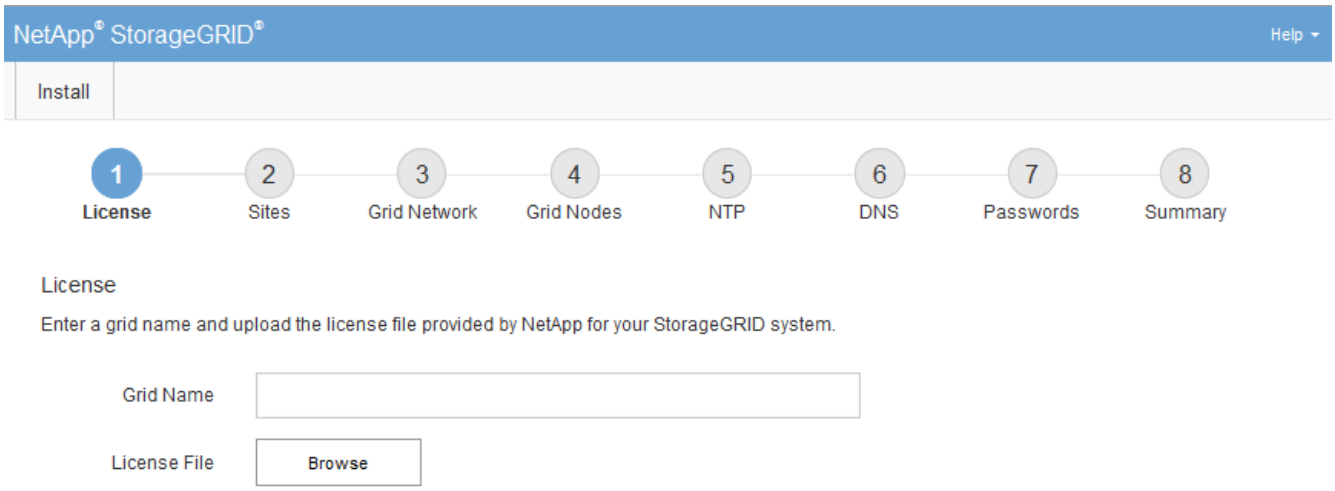
   In alternativa, è possibile accedere a Grid Manager dalla porta 8443:

   `https://primary_admin_node_ip:8443`

   > È possibile utilizzare l'indirizzo IP per l'indirizzo IP del nodo di amministrazione primario sulla rete griglia o sulla rete di amministrazione, a seconda della configurazione di rete.

2. Selezionare **Installa un sistema StorageGRID**.

   Viene visualizzata la pagina utilizzata per configurare un sistema StorageGRID.



Specificare le informazioni sulla licenza StorageGRID

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

Fasi

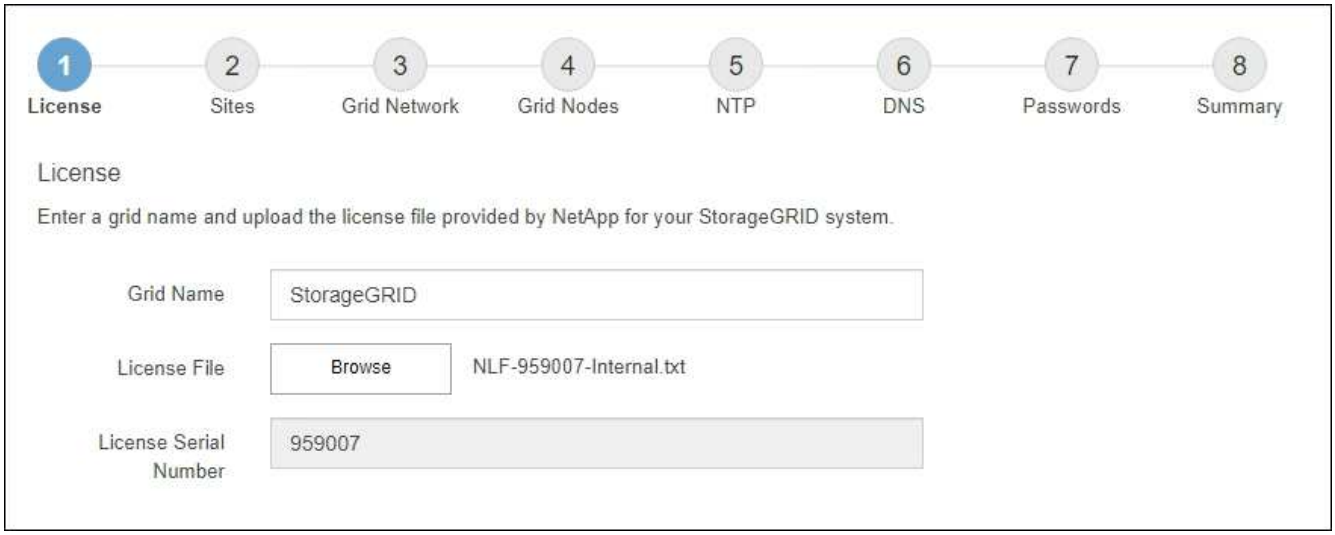
1. Nella pagina licenza, immettere un nome significativo per il sistema StorageGRID nel campo **Nome griglia**.

   Dopo l'installazione, il nome viene visualizzato nella parte superiore del menu Nodes (nodi).

2. Selezionare **Sfoglia**, individuare il file di licenza NetApp (`NLF-unique-id.txt`), quindi selezionare **Apri**.

   Il file di licenza viene validato e viene visualizzato il numero di serie.

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



3. Selezionare **Avanti**.

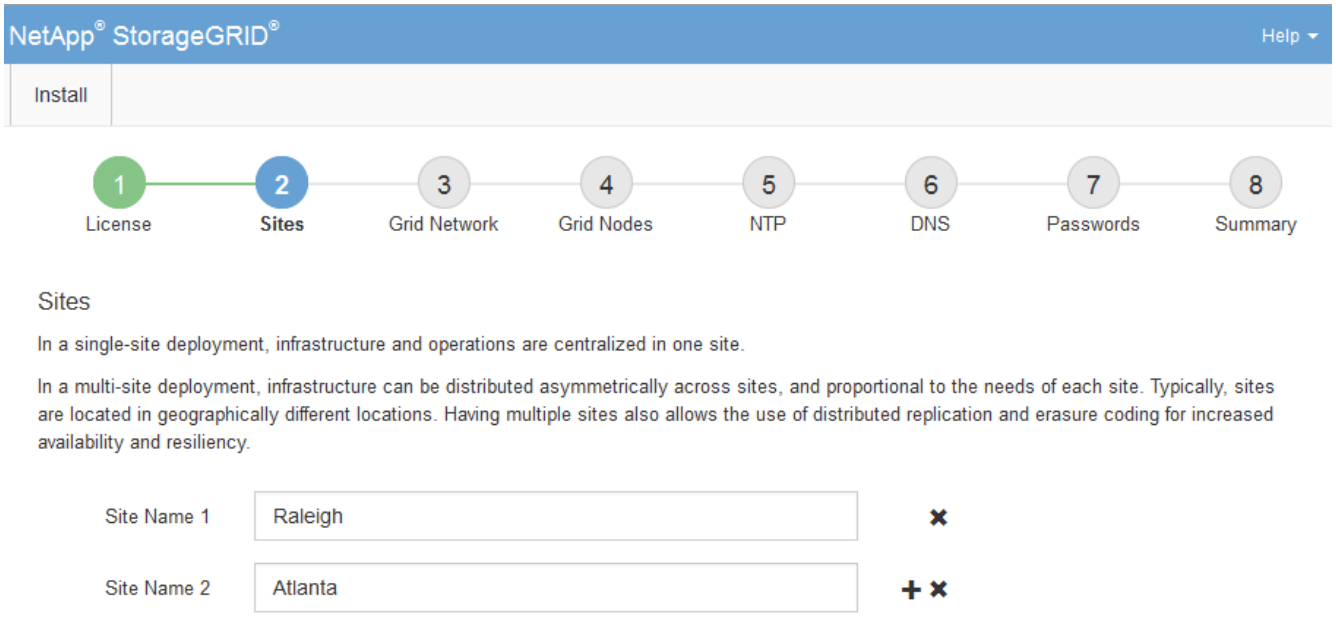
Aggiungere siti

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

Fasi

1. Nella pagina Siti, immettere il nome del sito *.
2. Per aggiungere altri siti, fare clic sul segno più accanto all'ultima voce del sito e inserire il nome nella nuova casella di testo **Nome sito**.

   Aggiungi tutti i siti aggiuntivi necessari per la topologia della griglia. È possibile aggiungere fino a 16 siti.



3. Fare clic su **Avanti**.

Specificare le subnet Grid Network

È necessario specificare le subnet utilizzate nella rete Grid.

A proposito di questa attività

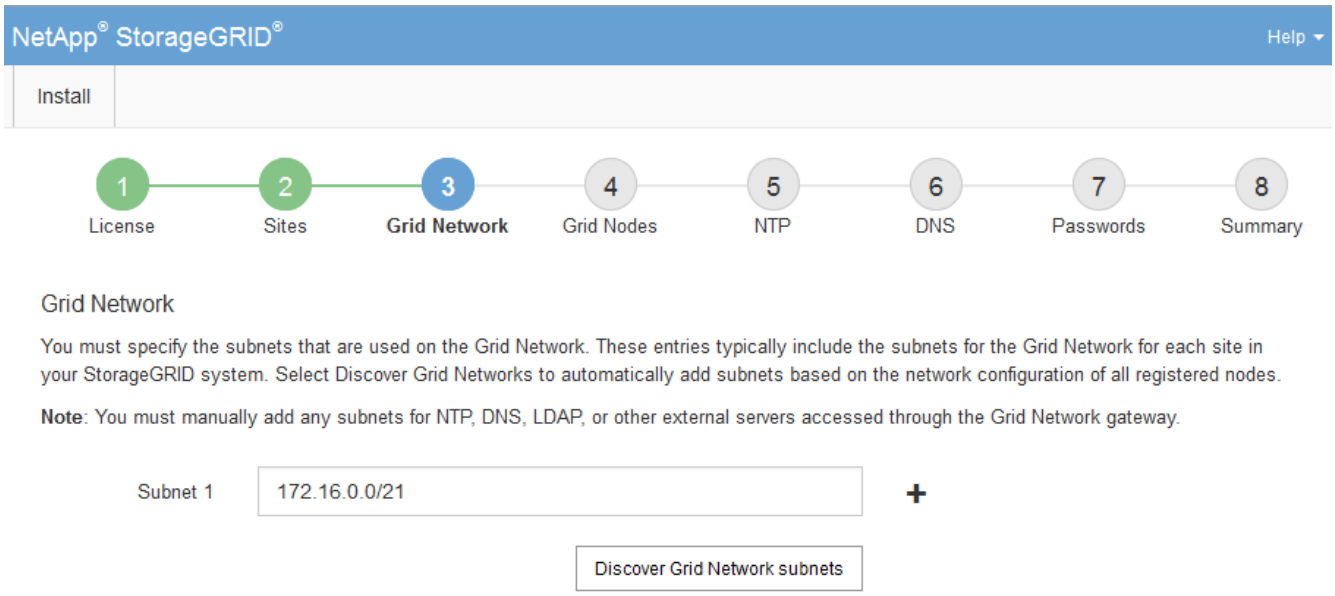
Le voci della subnet includono le subnet della rete di rete per ciascun sito del sistema StorageGRID, nonché le subnet che devono essere raggiungibili tramite la rete di rete.

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

Fasi

1. Specificare l'indirizzo di rete CIDR per almeno una rete griglia nella casella di testo **Subnet 1**.
2. Fare clic sul segno più accanto all'ultima voce per aggiungere una voce di rete aggiuntiva.

   Se è già stato implementato almeno un nodo, fare clic su **Discover Grid Networks Subnet** (rileva subnet Grid Network) per compilare automaticamente Grid Network Subnet List (elenco subnet Grid Network) con le subnet segnalate dai nodi Grid registrati con Grid Manager.



3. Fare clic su **Avanti**.

Approvare i nodi griglia in sospeso

È necessario approvare ciascun nodo della griglia prima che possa unirsi al sistema StorageGRID.

Prima di iniziare

Hai implementato tutti i nodi grid delle appliance virtuali e StorageGRID.

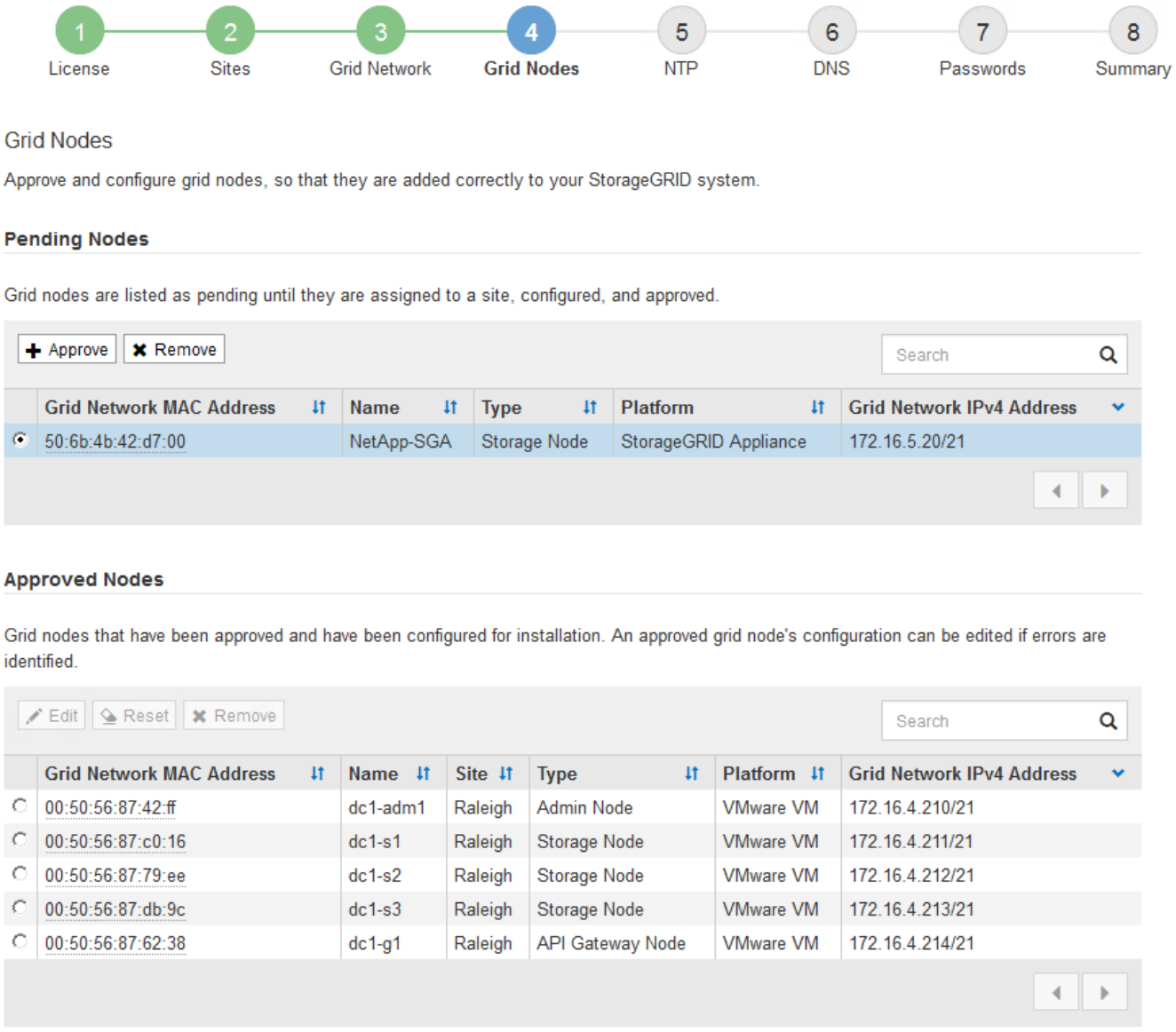
> È più efficiente eseguire una singola installazione di tutti i nodi, piuttosto che installare alcuni nodi ora e alcuni nodi successivamente.

Fasi

1. Esaminare l'elenco Pending Nodes (nodi in sospeso) e confermare che mostra tutti i nodi della griglia implementati.

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

2. Selezionare il pulsante di opzione accanto al nodo in sospeso che si desidera approvare.



3. Fare clic su **approva**.
4. In General Settings (Impostazioni generali), modificare le impostazioni per le seguenti proprietà, in base alle necessità:
   - **Sito**: Il nome di sistema del sito per questo nodo della griglia.
   - **Name**: Il nome del sistema per il nodo. Il nome predefinito corrisponde al nome specificato al momento della configurazione del nodo.

     I nomi di sistema sono necessari per le operazioni StorageGRID interne e non possono essere modificati dopo aver completato l'installazione. Tuttavia, durante questa fase del processo di installazione, è possibile modificare i nomi di sistema in base alle esigenze.

   - **Ruolo NTP**: Ruolo NTP (Network Time Protocol) del nodo Grid. Le opzioni disponibili sono **automatico**, **primario** e **Client**. Selezionando **automatico**, il ruolo primario viene assegnato ai nodi di amministrazione, ai nodi di storage con servizi ADC, ai nodi gateway e a tutti i nodi di griglia che hanno indirizzi IP non statici. A tutti gli altri nodi della griglia viene assegnato il ruolo Client.

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

- **Tipo di archiviazione** (solo nodi di archiviazione): Specificare che un nuovo nodo di archiviazione deve essere utilizzato esclusivamente per i metadati. Le opzioni sono **oggetti e metadati** e **solo metadati**. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

  Quando si installa un grid con nodi solo metadati, il grid deve anche contenere un numero minimo di nodi per lo storage a oggetti. Per un grid a sito singolo, vengono configurati almeno due nodi storage per oggetti e metadati. Per un grid multisito, per gli oggetti e i metadati viene configurato almeno un nodo di storage per sito.

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

5. In Grid Network, modificare le impostazioni per le seguenti proprietà secondo necessità:

   - **IPv4 Address (CIDR)**: L'indirizzo di rete CIDR per l'interfaccia Grid Network (eth0 all'interno del container). Ad esempio: 192.168.1.234/21
   - **Gateway**: Il gateway Grid Network. Ad esempio: 192.168.0.1

     Il gateway è necessario se sono presenti più subnet di rete.

   Se si seleziona DHCP per la configurazione Grid Network e si modifica il valore, il nuovo valore verrà configurato come indirizzo statico sul nodo. Assicurarsi che l'indirizzo IP risultante non si trovi all'interno di un pool di indirizzi DHCP.

6. Se si desidera configurare la rete amministrativa per il nodo della griglia, aggiungere o aggiornare le impostazioni nella sezione rete amministrativa secondo necessità.

   Inserire le subnet di destinazione dei percorsi fuori da questa interfaccia nella casella di testo **subnet (CIDR)**. Se sono presenti più subnet Admin, è necessario il gateway Admin.

   Se si seleziona DHCP per la configurazione Admin Network e si modifica il valore, il nuovo valore verrà configurato come indirizzo statico sul nodo. Assicurarsi che l'indirizzo IP risultante non si trovi all'interno di un pool di indirizzi DHCP.

   Appliance: per un'appliance StorageGRID, se la rete amministrativa non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione dell'appliance StorageGRID, non è possibile configurarla in questa finestra di dialogo. È invece necessario attenersi alla seguente procedura:

   a. Riavviare l'appliance: Nel programma di installazione dell'appliance, selezionare **Avanzate** > **Riavvia**.

      Il riavvio può richiedere alcuni minuti.

   b. Selezionare **Configure Networking** > **link Configuration** (Configura rete) e abilitare le reti appropriate.

c. Selezionare **Configura rete** > **Configurazione IP** e configurare le reti abilitate.
d. Tornare alla Home page e fare clic su **Avvia installazione**.
e. In Grid Manager: Se il nodo è elencato nella tabella Approved Nodes (nodi approvati), rimuoverlo.
f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).
g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).
h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP del programma di installazione dell'appliance.

   Per ulteriori informazioni, consultare le istruzioni di installazione relative al modello di appliance in uso.

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

   > Se si seleziona DHCP per la configurazione di rete client e si modifica il valore, il nuovo valore verrà configurato come indirizzo statico sul nodo. Assicurarsi che l'indirizzo IP risultante non si trovi all'interno di un pool di indirizzi DHCP.

   Appliance: per un'appliance StorageGRID, se la rete client non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione dell'appliance StorageGRID, non è possibile configurarla in questa finestra di dialogo. È invece necessario attenersi alla seguente procedura:

   a. Riavviare l'appliance: Nel programma di installazione dell'appliance, selezionare **Avanzate** > **Riavvia**.

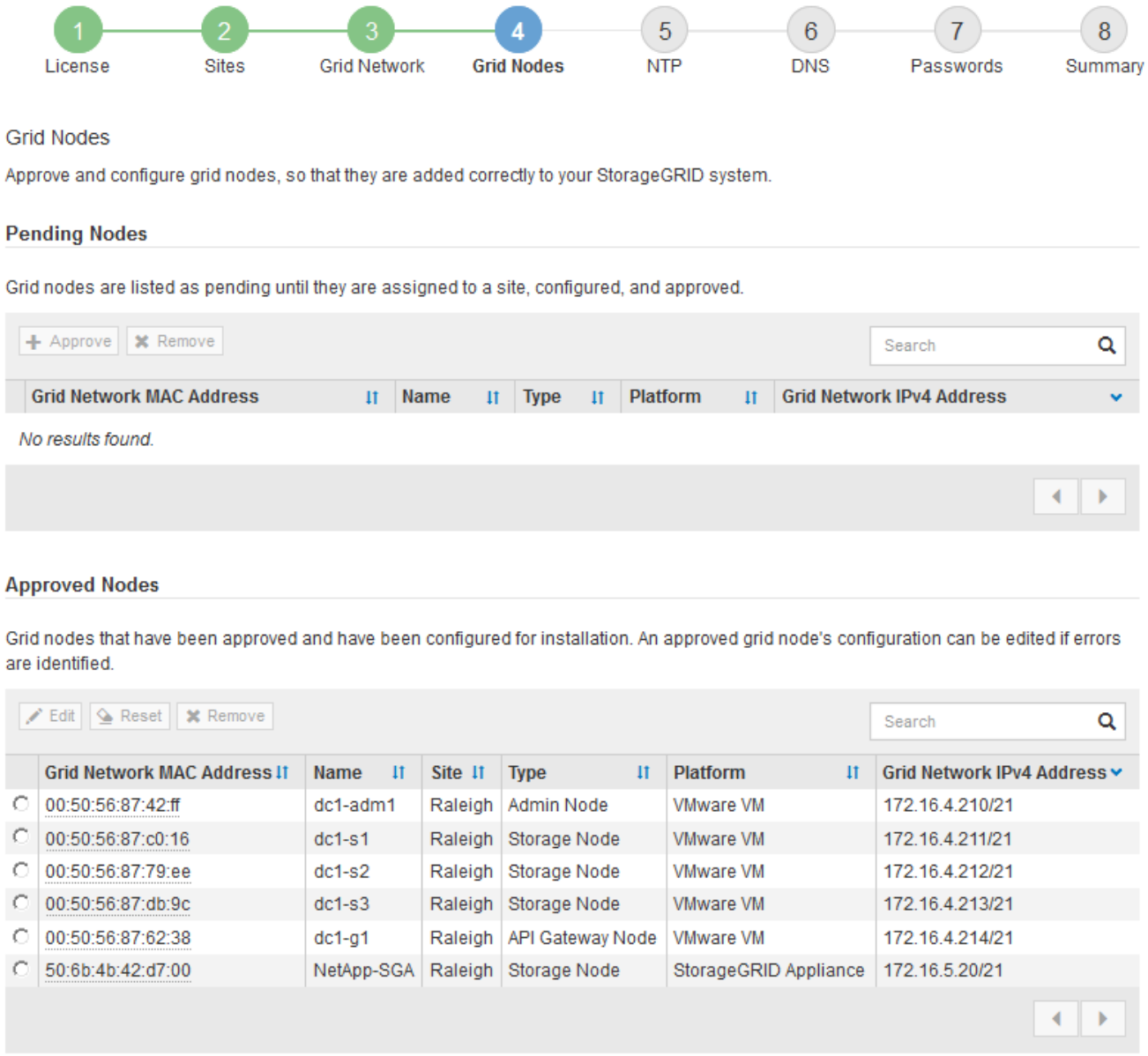
      Il riavvio può richiedere alcuni minuti.

   b. Selezionare **Configure Networking** > **link Configuration** (Configura rete) e abilitare le reti appropriate.
   c. Selezionare **Configura rete** > **Configurazione IP** e configurare le reti abilitate.
   d. Tornare alla Home page e fare clic su **Avvia installazione**.
   e. In Grid Manager: Se il nodo è elencato nella tabella Approved Nodes (nodi approvati), rimuoverlo.
   f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).
   g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).
   h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP del programma di installazione dell'appliance.

      Per ulteriori informazioni, consultare le istruzioni di installazione dell'apparecchio.

8. Fare clic su **Save** (Salva).

   La voce del nodo della griglia viene spostata nell'elenco dei nodi approvati.



9. Ripetere questi passaggi per ogni nodo griglia in sospeso che si desidera approvare.

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

10. Una volta completata l'approvazione dei nodi griglia, fare clic su **Avanti**.

Specificare le informazioni sul server Network Time Protocol

È necessario specificare le informazioni di configurazione del protocollo NTP (Network Time Protocol) per il sistema StorageGRID, in modo che le operazioni eseguite su server separati possano essere mantenute sincronizzate.

A proposito di questa attività

Specificare gli indirizzi IPv4 per i server NTP.

Specificare server NTP esterni. I server NTP specificati devono utilizzare il protocollo NTP.

È necessario specificare quattro riferimenti al server NTP di strato 3 o superiore per evitare problemi con la deriva del tempo.

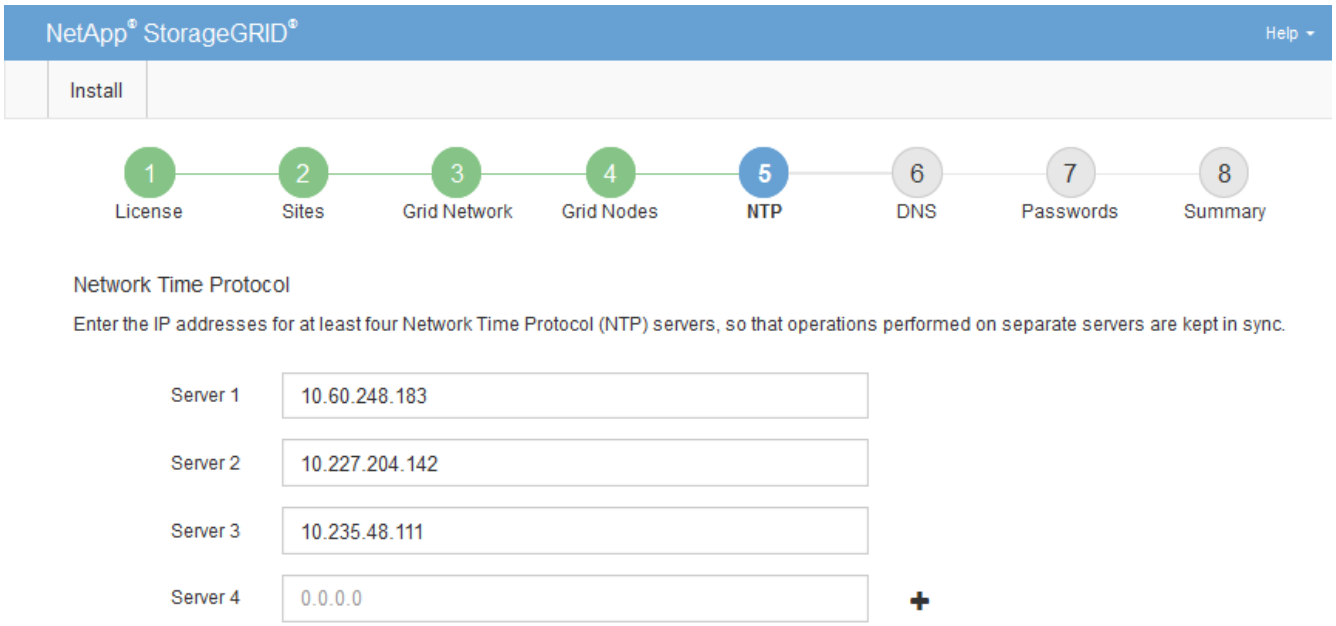
> Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Windows Time (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Time sulle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'utilizzo in ambienti ad alta precisione, come StorageGRID.
>
> "Supportare il limite per configurare il servizio Time di Windows per ambienti ad alta precisione"

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

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

Fasi

1. Specificare gli indirizzi IPv4 per almeno quattro server NTP nelle caselle di testo da **Server 1** a **Server 4**.
2. Se necessario, selezionare il segno più accanto all'ultima voce per aggiungere altre voci del server.



3. Selezionare **Avanti**.

Specificare le informazioni sul server DNS

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

A proposito di questa attività

Specificare "Informazioni sul server DNS" Consente di utilizzare nomi host FQDN (Fully Qualified Domain Name) piuttosto che indirizzi IP per le notifiche e-mail e AutoSupport.

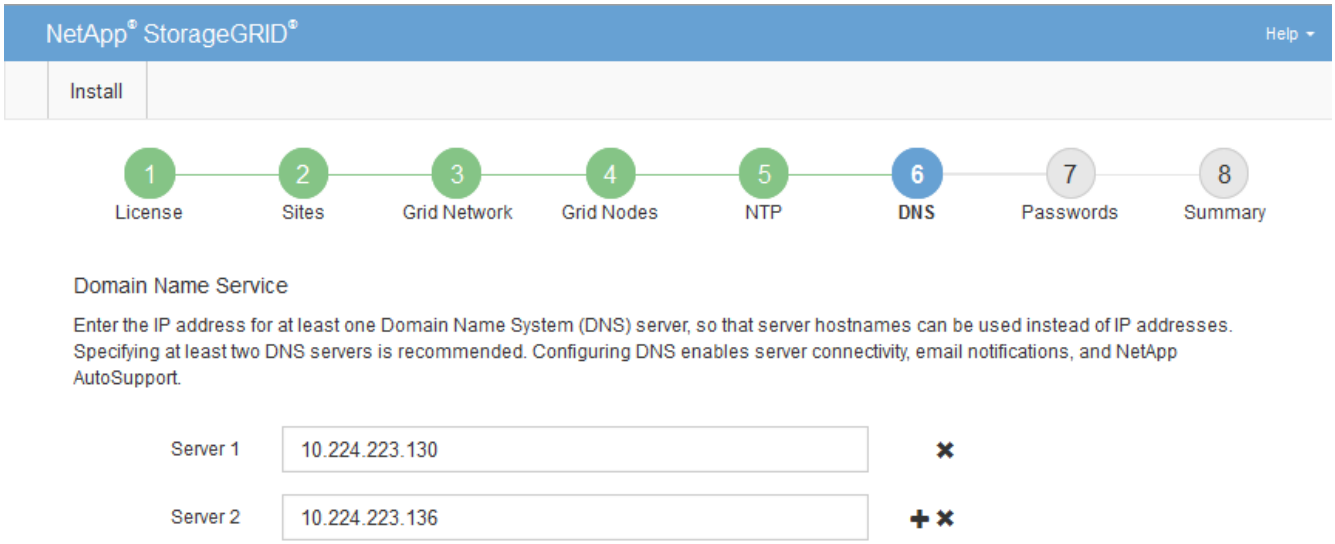
Per garantire il corretto funzionamento, specificare due o tre server DNS. Se si specificano più di tre, è possibile che ne vengano utilizzati solo tre a causa delle limitazioni del sistema operativo note su alcune piattaforme. Se nel proprio ambiente sono presenti restrizioni di routing, è possibile "Personalizzare l'elenco dei server DNS" Per i singoli nodi (in genere tutti i nodi di un sito) di utilizzare un set diverso di un massimo di tre server DNS.

Se possibile, utilizzare i server DNS a cui ciascun sito può accedere localmente per garantire che un sito islanded possa risolvere i FQDN per le destinazioni esterne.

Se le informazioni del server DNS vengono omesse o configurate in modo errato, viene attivato un allarme DNST sul servizio SSM di ciascun nodo della rete. L'allarme viene cancellato quando il DNS è configurato correttamente e le nuove informazioni sul server hanno raggiunto tutti i nodi della griglia.

Fasi

1. Specificare l'indirizzo IPv4 per almeno un server DNS nella casella di testo **Server 1**.
2. Se necessario, selezionare il segno più accanto all'ultima voce per aggiungere altre voci del server.



Si consiglia di specificare almeno due server DNS. È possibile specificare fino a sei server DNS.

3. Selezionare **Avanti**.

Specificare le password di sistema di StorageGRID

Durante l'installazione del sistema StorageGRID, è necessario inserire le password da utilizzare per proteggere il sistema ed eseguire attività di manutenzione.

A proposito di questa attività

Utilizzare la pagina Installa password per specificare la passphrase di provisioning e la password utente root di gestione della griglia.

- La passphrase di provisioning viene utilizzata come chiave di crittografia e non viene memorizzata dal sistema StorageGRID.
- È necessario disporre della passphrase di provisioning per le procedure di installazione, espansione e

manutenzione, incluso il download del pacchetto di ripristino. Pertanto, è importante memorizzare la passphrase di provisioning in una posizione sicura.

- È possibile modificare la passphrase di provisioning da Grid Manager, se si dispone di quella corrente.
- La password utente root della gestione della griglia può essere modificata utilizzando Grid Manager.
- Le password SSH e la console della riga di comando generate in modo casuale vengono memorizzate in `Passwords.txt` Nel pacchetto di ripristino.

Fasi

1. In **Provisioning Passphrase**, immettere la passphase di provisioning necessaria per apportare modifiche alla topologia grid del sistema StorageGRID.

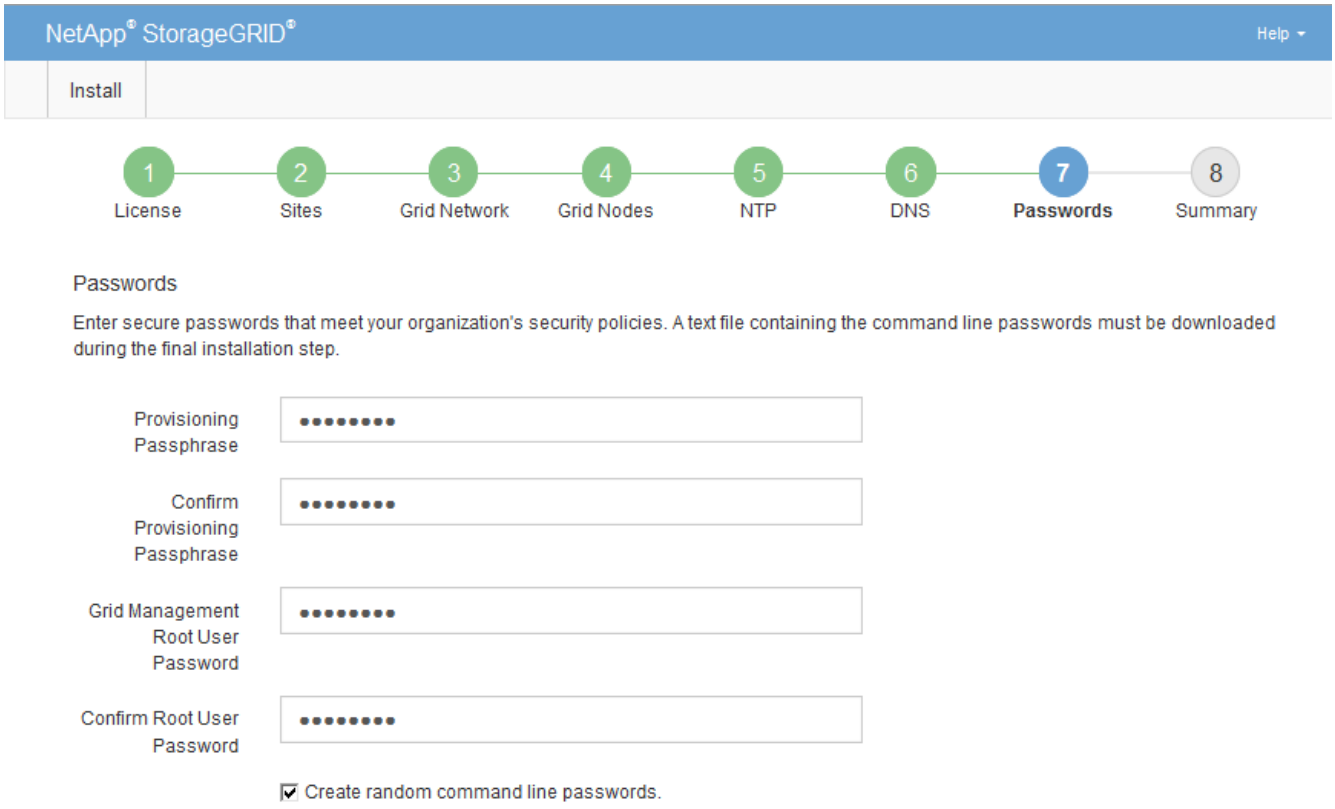
   Memorizzare la passphrase di provisioning in un luogo sicuro.

   > Se, al termine dell'installazione, si desidera modificare la passphrase di provisioning in un secondo momento, è possibile utilizzare Grid Manager. Selezionare **CONFIGURATION** > **Access control**> **Grid passwords**.

2. In **Confirm Provisioning Passphrase** (Conferma password di provisioning), immettere nuovamente la passphrase di provisioning per confermarla.
3. In **Grid Management Root User Password**, immettere la password da utilizzare per accedere al Grid Manager come utente "root".

   Memorizzare la password in un luogo sicuro.

4. In **Confirm Root User Password** (Conferma password utente root), immettere nuovamente la password di Grid Manager per confermarla.



5. Se si sta installando una griglia a scopo dimostrativo o dimostrativo, deselezionare la casella di controllo **Create random command line passwords** (Crea password della riga di comando casuale).

   Per le implementazioni in produzione, le password casuali devono essere sempre utilizzate per motivi di sicurezza. Cancella **Crea password casuali della riga di comando** solo per le griglie demo se desideri utilizzare password predefinite per accedere ai nodi della griglia dalla riga di comando utilizzando l'account "root" o "admin".

   > Viene richiesto di scaricare il file del pacchetto di ripristino (`sgws-recovery-package-id-revision.zip`) Dopo aver fatto clic su **Install** (Installa) nella pagina Summary (Riepilogo). È necessario "scarica questo file" per completare l'installazione. Le password richieste per accedere al sistema vengono memorizzate in `Passwords.txt` File, contenuto nel file del pacchetto di ripristino.

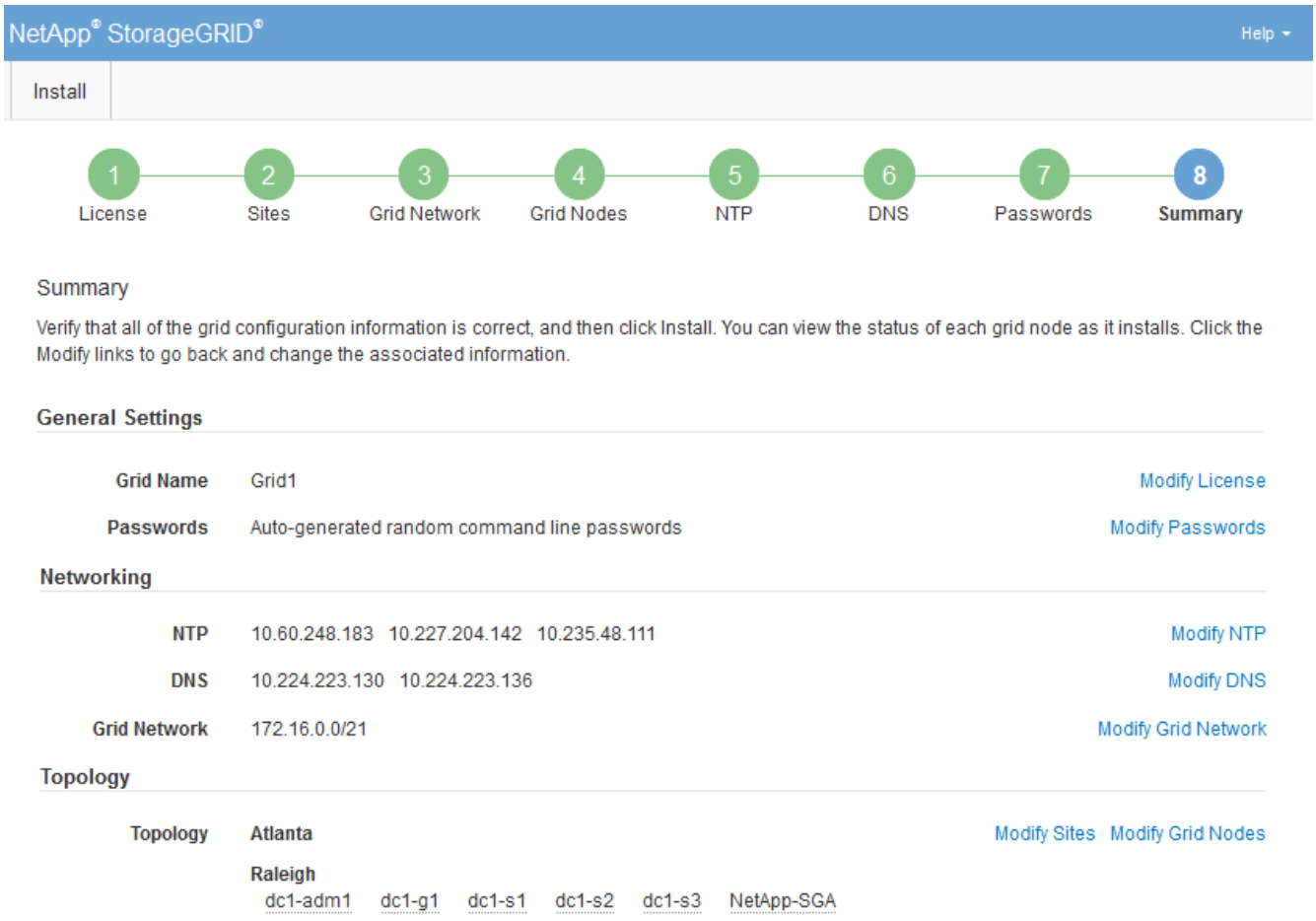
6. Fare clic su **Avanti**.

Esaminare la configurazione e completare l'installazione

È necessario esaminare attentamente le informazioni di configurazione inserite per assicurarsi che l'installazione venga completata correttamente.

Fasi

1. Visualizza la pagina **Riepilogo**.



2. Verificare che tutte le informazioni di configurazione della griglia siano corrette. Utilizzare i link Modify

(Modifica) nella pagina Summary (Riepilogo) per tornare indietro e correggere eventuali errori.

3. Fare clic su **Installa**.

> Se un nodo è configurato per utilizzare la rete client, il gateway predefinito per quel nodo passa dalla rete griglia alla rete client quando si fa clic su **Installa**. In caso di perdita della connettività, assicurarsi di accedere al nodo di amministrazione primario tramite una subnet accessibile. Vedere "Linee guida per il networking" per ulteriori informazioni.

4. Fare clic su **Download Recovery Package**.

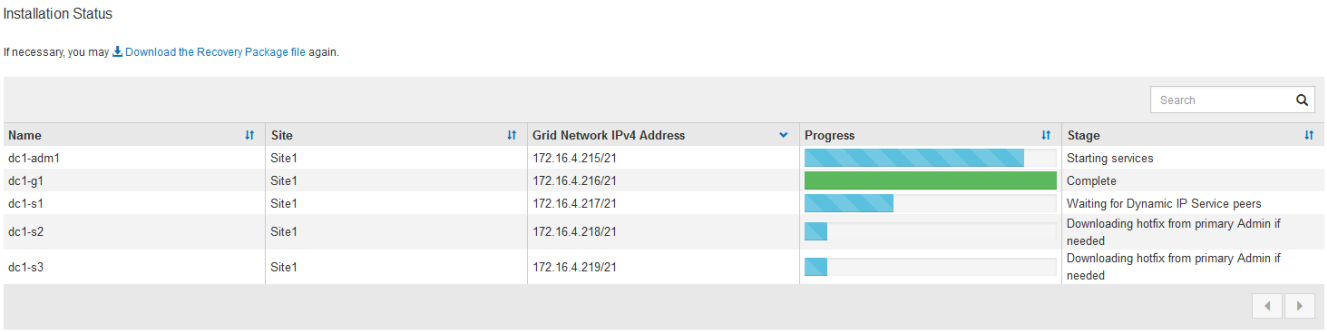
   Quando l'installazione prosegue fino al punto in cui è definita la topologia della griglia, viene richiesto di scaricare il file del pacchetto di ripristino (`.zip`) e confermare che sia possibile accedere al contenuto del file. È necessario scaricare il file del pacchetto di ripristino in modo da poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi griglia. L'installazione continua in background, ma non è possibile completare l'installazione e accedere al sistema StorageGRID fino a quando non si scarica e si verifica questo file.

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

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

6. Selezionare la casella di controllo **ho scaricato e verificato il file del pacchetto di ripristino** e fare clic su **Avanti**.

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



   Una volta raggiunta la fase completa per tutti i nodi della griglia, viene visualizzata la pagina di accesso per Grid Manager.

7. Accedere a Grid Manager utilizzando l'utente "root" e la password specificata durante l'installazione.

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. Impossibile 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.

Panoramica dell'API REST per l'installazione

StorageGRID fornisce l'API di installazione di StorageGRID per eseguire le attività di installazione.

L'API utilizza la piattaforma API open source Swagger per fornire la documentazione API. Swagger consente agli sviluppatori e ai non sviluppatori di interagire con l'API in un'interfaccia utente che illustra il modo in cui l'API risponde a parametri e opzioni. La presente documentazione presuppone che l'utente abbia familiarità con le tecnologie Web standard e il formato dati JSON.

> Tutte le operazioni API eseguite utilizzando la pagina web API Docs sono operazioni live. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Ogni comando REST API include l'URL dell'API, un'azione HTTP, qualsiasi parametro URL richiesto o opzionale e una risposta API prevista.

API di installazione StorageGRID

L'API di installazione di StorageGRID è disponibile solo quando si configura inizialmente il sistema StorageGRID e se è necessario eseguire un ripristino primario del nodo di amministrazione. È possibile accedere all'API di installazione tramite HTTPS da Grid Manager.

Per accedere alla documentazione API, accedere alla pagina Web di installazione nel nodo di amministrazione principale e selezionare **Guida** > **documentazione API** dalla barra dei menu.

L'API di installazione di StorageGRID include le seguenti sezioni:

- **Config** — operazioni relative alla release del prodotto e alle versioni dell'API. È possibile elencare la versione di release del prodotto e le principali versioni dell'API supportate da tale release.
- **Grid** — operazioni di configurazione a livello di griglia. È possibile ottenere e aggiornare le impostazioni della griglia, inclusi i dettagli della griglia, le subnet Grid Network, le password della griglia e gli indirizzi IP dei server NTP e DNS.
- **Nodi** — operazioni di configurazione a livello di nodo. È possibile recuperare un elenco di nodi griglia, eliminare un nodo griglia, configurare un nodo griglia, visualizzare un nodo griglia e ripristinare la configurazione di un nodo griglia.
- **Provision** — operazioni di provisioning. È possibile avviare l'operazione di provisioning e visualizzare lo stato dell'operazione di provisioning.
- **Recovery** — operazioni di recovery del nodo di amministrazione principale. È possibile ripristinare le

informazioni, caricare il pacchetto di ripristino, avviare il ripristino e visualizzare lo stato dell'operazione di ripristino.

- **Recovery-package** — operazioni per scaricare il pacchetto di ripristino.
- **Schemi** — schemi API per implementazioni avanzate
- **Siti** — operazioni di configurazione a livello di sito. È possibile creare, visualizzare, eliminare e modificare un sito.

Dove andare

Dopo aver completato un'installazione, eseguire le attività di integrazione e configurazione richieste. È possibile eseguire le attività opzionali in base alle necessità.

Attività richieste

- "Creare un account tenant" Per ogni protocollo client (Swift o S3) che verrà utilizzato per memorizzare gli oggetti nel sistema StorageGRID.
- "Controllare l'accesso al sistema" configurando gruppi e account utente. Se lo si desidera, è possibile "configurare un'origine di identità federata" (Ad esempio Active Directory o OpenLDAP), in modo da poter importare utenti e gruppi di amministrazione. In alternativa, è possibile "creare utenti e gruppi locali".
- Integrare e testare "API S3" oppure "API Swift" Applicazioni client che verranno utilizzate per caricare oggetti nel sistema StorageGRID.
- "Configurare le regole ILM (Information Lifecycle Management) e i criteri ILM" da utilizzare per proteggere i dati degli oggetti.
- Se l'installazione include nodi di storage dell'appliance, utilizzare SANtricity OS per completare le seguenti operazioni:
  - Connessione a ogni appliance StorageGRID.
  - Verificare la ricezione dei dati AutoSupport.

  Vedere "Configurare l'hardware".
- Esaminare e seguire "Linee guida per la protezione avanzata del sistema StorageGRID" eliminare i rischi per la sicurezza.
- "Configurare le notifiche e-mail per gli avvisi di sistema".
- Se il sistema StorageGRID include nodi di archiviazione (non più presenti), configurare la connessione del nodo di archiviazione al sistema di archiviazione esterno di destinazione.

Attività facoltative

- "Aggiornare gli indirizzi IP del nodo griglia" Se sono state modificate dopo la pianificazione dell'implementazione e la generazione del pacchetto di ripristino.
- "Configurare la crittografia dello storage", se necessario.
- "Configurare la compressione dello storage" ridurre le dimensioni degli oggetti memorizzati, se necessario.

Risolvere i problemi di installazione

Se si verificano problemi durante l'installazione del sistema StorageGRID, è possibile accedere ai file di log dell'installazione. Per risolvere i problemi, potrebbe essere

necessario utilizzare anche i file di log dell'installazione.

I seguenti file di log per l'installazione sono disponibili dal container che esegue ciascun nodo:

- `/var/local/log/install.log` (trovato su tutti i nodi della griglia)
- `/var/local/log/gdu-server.log` (Trovato sul nodo di amministrazione primario)

I seguenti file di log per l'installazione sono disponibili dall'host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

Per informazioni su come accedere ai file di registro, vedere "Raccogliere i file di log e i dati di sistema".

Informazioni correlate

"Risolvere i problemi di un sistema StorageGRID"

Esempio di /etc/sysconfig/network-scripts

È possibile utilizzare i file di esempio per aggregare quattro interfacce fisiche Linux in un unico collegamento LACP e quindi stabilire tre interfacce VLAN che sottendere il collegamento per l'utilizzo come interfacce di rete StorageGRID, amministratore e client.

Interfacce fisiche

Si noti che gli switch alle altre estremità dei collegamenti devono anche considerare le quattro porte come un singolo trunk LACP o canale di porta e devono passare almeno le tre VLAN a cui si fa riferimento con tag.

`/etc/sysconfig/network-scripts/ifcfg-ens160`

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

`/etc/sysconfig/network-scripts/ifcfg-ens192`

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Interfaccia bond

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

Interfacce VLAN

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Installare StorageGRID su Ubuntu o Debian

Avvio rapido per l'installazione di StorageGRID su Ubuntu o Debian

Seguire questi passaggi di alto livello per installare un nodo Ubuntu o Debian StorageGRID.

1 Preparazione

- Scopri di più "Architettura StorageGRID e topologia di rete".
- Scopri le specifiche di "Networking StorageGRID".
- Raccogliere e preparare il "Informazioni e materiali richiesti".
- Preparare il necessario "CPU e RAM".
- Prevedere "requisiti di storage e performance".
- "Preparare i server Linux" Che ospiterà i nodi StorageGRID.

2 Implementazione

Implementare i nodi grid. Quando si implementano nodi grid, questi vengono creati come parte del sistema StorageGRID e connessi a una o più reti.

- Per distribuire i nodi grid basati su software sugli host preparati nel passaggio 1, utilizzare la riga di comando di Linux e. "file di configurazione dei nodi".
- Per implementare i nodi di appliance StorageGRID, segui la procedura "Avvio rapido per l'installazione dell'hardware".

3 Configurazione

Una volta distribuiti tutti i nodi, utilizzare il Grid Manager per "configurare la griglia e completare l'installazione".

Automatizzare l'installazione

Per risparmiare tempo e garantire coerenza, è possibile automatizzare l'installazione del servizio host StorageGRID e la configurazione dei nodi grid.

- Utilizza un framework di orchestrazione standard come Ansible, Puppet o Chef per automatizzare:
  - Installazione di Ubuntu o Debian
  - Configurazione di rete e storage
  - Installazione del motore del container e del servizio host StorageGRID
  - Implementazione di nodi grid virtuali

  Vedere "Automatizzare l'installazione e la configurazione del servizio host StorageGRID".
- Dopo aver distribuito i nodi grid, "Automatizzare la configurazione del sistema StorageGRID" Utilizzo dello script di configurazione Python fornito nell'archivio di installazione.
- "Automatizzare l'installazione e la configurazione dei nodi grid delle appliance"
- Se si è uno sviluppatore avanzato di implementazioni StorageGRID, automatizzare l'installazione dei nodi grid utilizzando "API REST di installazione".

Pianificare e preparare l'installazione su Ubuntu o Debian

Informazioni e materiali richiesti

Prima di installare StorageGRID, raccogliere e preparare le informazioni e il materiale necessari.

Informazioni richieste

Piano di rete

Quali reti intendi collegare a ogni nodo StorageGRID? StorageGRID supporta più reti per la separazione del traffico, la sicurezza e la convenienza amministrativa.

Vedere StorageGRID "Linee guida per il networking".

Informazioni di rete

A meno che non si utilizzi DHCP, gli indirizzi IP da assegnare a ciascun nodo della griglia e gli indirizzi IP dei server DNS e NTP.

Server per i nodi grid

Identificare un insieme di server (fisici, virtuali o entrambi) che, in aggregato, forniscono risorse sufficienti per supportare il numero e il tipo di nodi StorageGRID che si intende implementare.

> Se l'installazione di StorageGRID non utilizza nodi di storage (hardware) dell'appliance StorageGRID, è necessario utilizzare lo storage RAID hardware con cache di scrittura supportata dalla batteria (BBWC). StorageGRID non supporta l'utilizzo di reti VSAN (Virtual Storage Area Network), RAID software o nessuna protezione RAID.

Migrazione dei nodi (se necessaria)

Comprendere "requisiti per la migrazione dei nodi", se si desidera eseguire la manutenzione pianificata sugli host fisici senza alcuna interruzione del servizio.

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Materiali richiesti

Licenza NetApp StorageGRID

È necessario disporre di una licenza NetApp valida con firma digitale.

> Nell'archivio di installazione di StorageGRID è inclusa una licenza non di produzione, che può essere utilizzata per test e griglie di prova.

Archivio di installazione di StorageGRID

"Scaricare l'archivio di installazione di StorageGRID ed estrarre i file".

Laptop di assistenza

Il sistema StorageGRID viene installato tramite un laptop di assistenza.

Il laptop di assistenza deve disporre di:

- Porta di rete
- Client SSH (ad esempio, putty)

- "Browser Web supportato"

Documentazione StorageGRID

- "Note di rilascio"
- "Istruzioni per l'amministrazione di StorageGRID"

Scaricare ed estrarre i file di installazione di StorageGRID

È necessario scaricare l'archivio di installazione di StorageGRID ed estrarre i file richiesti.

Fasi

1. Accedere alla "Pagina dei download NetApp per StorageGRID".
2. Selezionare il pulsante per scaricare l'ultima versione oppure selezionare un'altra versione dal menu a discesa e selezionare **Go**.
3. Accedi con il nome utente e la password del tuo account NetApp.
4. Se viene visualizzata un'istruzione Caution/MustRead, leggerla e selezionare la casella di controllo.

   Dopo aver installato la release di StorageGRID, è necessario applicare le correzioni rapide richieste. Per ulteriori informazioni, consultare "procedura di hotfix nelle istruzioni di ripristino e manutenzione"

5. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).

   Viene visualizzata la pagina dei download per la versione selezionata. La pagina contiene tre colonne:

6. Nella colonna **Installa StorageGRID**, selezionare il file .tgz o .zip per Ubuntu o Debian.

   Selezionare `.zip` File se si esegue Windows sul laptop di assistenza.

7. Salvare ed estrarre il file di archivio.
8. Scegliere i file desiderati dal seguente elenco.

   La serie di file necessari dipende dalla topologia della griglia pianificata e dal modo in cui verrà implementato il grid StorageGRID.

   I percorsi elencati nella tabella sono relativi alla directory di primo livello installata dall'archivio di installazione estratto.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Un file di licenza NetApp non in produzione che è possibile utilizzare per le implementazioni di test e proof of concept.

Percorso e nome del file	Descrizione
	PACCHETTO DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.
	Checksum MD5 per il file `/debs/storagegrid-webscale-images-version-SHA.deb`.
	PACCHETTO DEB per l'installazione del servizio host StorageGRID su host Ubuntu o Debian.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per il ping federate.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di manuale e ruolo Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Script di supporto chiamato dal compagno `storagegrid-ssoauth-azure.py` Script Python per eseguire interazioni SSO con Azure.

Percorso e nome del file	Descrizione
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

Requisiti software per Ubuntu e Debian

È possibile utilizzare una macchina virtuale per ospitare qualsiasi tipo di nodo StorageGRID. È necessaria una macchina virtuale per ogni nodo di griglia.

Per installare StorageGRID su Ubuntu o Debian, è necessario installare alcuni pacchetti software di terze parti. Alcune distribuzioni Linux supportate non contengono questi pacchetti per impostazione predefinita. Le versioni dei pacchetti software su cui vengono testate le installazioni di StorageGRID includono quelle elencate in questa pagina.

> Se si seleziona un'opzione di installazione runtime di distribuzione Linux e contenitore che richiede uno qualsiasi di questi pacchetti e questi non vengono installati automaticamente dalla distribuzione Linux, installare una delle versioni elencate qui se disponibile presso il provider o il fornitore di supporto per la distribuzione Linux. In caso contrario, utilizzare le versioni predefinite dei pacchetti disponibili presso il fornitore.

> Tutte le opzioni di installazione richiedono Podman o Docker. Non installare entrambi i pacchetti. Installare solo il pacchetto richiesto dall'opzione di installazione.

Versioni Python testate

- 3,5.2-2
- 3,6.8-2
- 3,6.8-38
- 3,6.9-1
- 3,7.3-1
- 3,8.10-0
- 3,9.2-1
- 3,9.10-2
- 3,9.16-1
- 3.10.6-1
- 3.11.2-6

Versioni di Podman testate

- 3,2.3-0
- 3,4.4+ds1
- 4,1.1-7
- 4,2.0-11
- 4,3.1+ds1-8+b1
- 4,4.1-8
- 4,4.1-12

Versioni di Docker testate

Il supporto di Docker è obsoleto e verrà rimosso in una release futura.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1
- Docker-CE 24,0.2-1
- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1.5-2

Requisiti di CPU e RAM

Prima di installare il software StorageGRID, verificare e configurare l'hardware in modo che sia pronto per il supporto del sistema StorageGRID.

Ogni nodo StorageGRID richiede le seguenti risorse minime:

- Core CPU: 8 per nodo
- RAM: Almeno 24 GB per nodo e da 2 a 16 GB in meno rispetto alla RAM totale del sistema, a seconda della RAM totale disponibile e della quantità di software non StorageGRID in esecuzione nel sistema

Le risorse dei nodi di solo metadati basate su software devono corrispondere alle risorse dei nodi di storage esistenti. Ad esempio:

- Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:
  - 128 GB DI RAM
  - CPU a 8 core
  - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)
- Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuale con 24 GB di RAM, 8 core CPU e 3 TB o 4TB di memorizzazione di metadati, i nodi basati solo sui metadati del software devono utilizzare risorse simili (24 GB di RAM, 8 core CPU e 4TB di memorizzazione di metadati (rangedb/0).

Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve almeno StorageGRID corrispondere ai nodi storage dei siti StorageGRID esistenti e alle nuove risorse del sito.

Assicurarsi che il numero di nodi StorageGRID che si intende eseguire su ciascun host fisico o virtuale non superi il numero di core CPU o la RAM fisica disponibile. Se gli host non sono dedicati all'esecuzione di StorageGRID (non consigliato), assicurarsi di prendere in considerazione i requisiti di risorse delle altre applicazioni.

> Monitorate regolarmente l'utilizzo di CPU e memoria per garantire che queste risorse continuino a soddisfare il vostro carico di lavoro. Ad esempio, raddoppiando l'allocazione di RAM e CPU per i nodi di storage virtuali si fornirebbero risorse simili a quelle fornite per i nodi di appliance StorageGRID. Inoltre, se la quantità di metadati per nodo supera i 500 GB, considerare l'aumento della RAM per nodo a 48 GB o più. Per informazioni sulla gestione dello storage dei metadati degli oggetti, sull'aumento dell'impostazione Metadata Reserved Space e sul monitoraggio dell'utilizzo di CPU e memoria, vedere le istruzioni per "amministrazione", "monitoraggio", e. "aggiornamento in corso" StorageGRID.

Se l'hyperthreading è attivato sugli host fisici sottostanti, è possibile fornire 8 core virtuali (4 core fisici) per nodo. Se l'hyperthreading non è attivato sugli host fisici sottostanti, è necessario fornire 8 core fisici per nodo.

Se si utilizzano macchine virtuali come host e si ha il controllo sulle dimensioni e sul numero di macchine virtuali, è necessario utilizzare una singola macchina virtuale per ciascun nodo StorageGRID e dimensionare di conseguenza la macchina virtuale.

Per le implementazioni in produzione, non è necessario eseguire più nodi di storage sullo stesso hardware di storage fisico o host virtuale. Ciascun nodo di storage in una singola implementazione StorageGRID deve trovarsi nel proprio dominio di errore isolato. È possibile massimizzare la durata e la disponibilità dei dati degli oggetti se si garantisce che un singolo guasto hardware possa avere un impatto solo su un singolo nodo di storage.

Vedere anche "Requisiti di storage e performance".

Requisiti di storage e performance

È necessario comprendere i requisiti di storage per i nodi StorageGRID, in modo da poter fornire spazio sufficiente per supportare la configurazione iniziale e l'espansione dello storage futura.

I nodi StorageGRID richiedono tre categorie logiche di storage:

- **Pool di container** — storage a Tier di performance (10.000 SAS o SSD) per i container di nodi, che verrà assegnato al driver di storage Docker quando si installa e configura Docker sugli host che supporteranno i nodi StorageGRID.
- **Dati di sistema** — storage a Tier di performance (10.000 SAS o SSD) per lo storage persistente per nodo dei dati di sistema e dei log delle transazioni, che i servizi host StorageGRID utilizzeranno e mapperanno in singoli nodi.
- **Dati oggetto** — storage di livello Performance (10.000 SAS o SSD) e storage bulk di livello capacità (NL-SAS/SATA) per lo storage persistente di dati oggetto e metadati oggetto.

È necessario utilizzare i dispositivi a blocchi supportati da RAID per tutte le categorie di storage. I dischi non ridondanti, gli SSD o i JBOD non sono supportati. È possibile utilizzare lo storage RAID condiviso o locale per qualsiasi categoria di storage; tuttavia, se si desidera utilizzare la funzionalità di migrazione dei nodi in StorageGRID, è necessario memorizzare i dati di sistema e i dati degli oggetti sullo storage condiviso. Per

ulteriori informazioni, vedere "Requisiti per la migrazione dei container di nodi".

Requisiti relativi alle performance

Le performance dei volumi utilizzati per il pool di container, i dati di sistema e i metadati degli oggetti influiscono in modo significativo sulle performance complessive del sistema. Per questi volumi, è necessario utilizzare storage di livello performance (10.000 SAS o SSD) per garantire prestazioni disco adeguate in termini di latenza, operazioni di input/output al secondo (IOPS) e throughput. È possibile utilizzare lo storage a Tier di capacità (NL-SAS/SATA) per lo storage persistente dei dati a oggetti.

I volumi utilizzati per il pool di container, i dati di sistema e i dati degli oggetti devono avere il caching write-back abilitato. La cache deve essere su un supporto protetto o persistente.

Requisiti degli host che utilizzano lo storage NetApp ONTAP

Se il nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verifica che il volume non disponga di una policy di tiering FabricPool abilitata. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

> Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

Numero di host richiesti

Ogni sito StorageGRID richiede almeno tre nodi di storage.

> In un'implementazione in produzione, non eseguire più di un nodo di storage su un singolo host fisico o virtuale. L'utilizzo di un host dedicato per ciascun nodo di storage fornisce un dominio di errore isolato.

È possibile implementare altri tipi di nodi, come ad esempio nodi di amministrazione o nodi gateway, sugli stessi host oppure implementarli sui propri host dedicati in base alle necessità.

Numero di volumi di storage per ciascun host

La seguente tabella mostra il numero di volumi di storage (LUN) richiesti per ciascun host e le dimensioni minime richieste per ogni LUN, in base ai nodi che verranno implementati su tale host.

La dimensione massima del LUN testato è di 39 TB.

> Questi numeri si riferiscono a ciascun host e non all'intera griglia.

Scopo del LUN	Categoria di storage	Numero di LUN	Dimensione minima/LUN
Pool di storage del motore di container	Pool di container	1	Numero totale di nodi × 100 GB
`/var/local` volume	Dati di sistema	1 per ogni nodo su questo host	90 GB

Scopo del LUN	Categoria di storage	Numero di LUN	Dimensione minima/LUN
Nodo di storage	Dati dell'oggetto	3 per ciascun nodo di storage su questo host **Nota:** Un nodo di storage basato su software può avere da 1 a 16 volumi di storage; si consigliano almeno 3 volumi di storage.	12 TB (4 TB/LUN) VEDERE Requisiti di storage per i nodi di storage per ulteriori informazioni.
Nodo di storage (solo metadati)	Metadati dell'oggetto	1	4 TB vedere Requisiti di storage per i nodi di storage per ulteriori informazioni. **Nota**: È richiesto un solo rangedb per i nodi di archiviazione di solo metadati.
Registri di audit del nodo di amministrazione	Dati di sistema	1 per ogni nodo Admin su questo host	200 GB
Tabelle del nodo di amministrazione	Dati di sistema	1 per ogni nodo Admin su questo host	200 GB

A seconda del livello di audit configurato, la dimensione degli input dell'utente, come il nome della chiave a oggetti S3, Inoltre, la quantità di dati del registro di controllo da conservare potrebbe essere necessaria per aumentare la dimensione del LUN del registro di controllo su ciascun nodo di amministrazione.in genere, una griglia genera circa 1 KB di dati di controllo per ogni operazione S3, Ciò significa che un LUN da 200 GB supporterà 70 milioni di operazioni al giorno o 800 operazioni al secondo per due o tre giorni.

Spazio di storage minimo per un host

La seguente tabella mostra lo spazio di storage minimo richiesto per ciascun tipo di nodo. È possibile utilizzare questa tabella per determinare la quantità minima di storage da fornire all'host in ciascuna categoria di storage, in base ai nodi che verranno implementati su tale host.

Non è possibile utilizzare le snapshot dei dischi per ripristinare i nodi della griglia. Fare riferimento invece alla "recovery del nodo grid" procedure per ogni tipo di nodo.

Tipo di nodo	Pool di container	Dati di sistema	Dati dell'oggetto
Nodo di storage	100 GB	90 GB	4.000 GB
Nodo Admin	100 GB	490 GB (3 LUN)	*non applicabile*

Tipo di nodo	Pool di container	Dati di sistema	Dati dell'oggetto
Nodo gateway	100 GB	90 GB	*non applicabile*
Nodo di archiviazione	100 GB	90 GB	*non applicabile*

Esempio: Calcolo dei requisiti di storage per un host

Si supponga di voler implementare tre nodi sullo stesso host: Un nodo di storage, un nodo di amministrazione e un nodo gateway. È necessario fornire un minimo di nove volumi di storage all'host. Sono necessari almeno 300 GB di storage a Tier di performance per i container di nodi, 670 GB di storage a Tier di performance per i dati di sistema e i log delle transazioni e 12 TB di storage a Tier di capacità per i dati a oggetti.

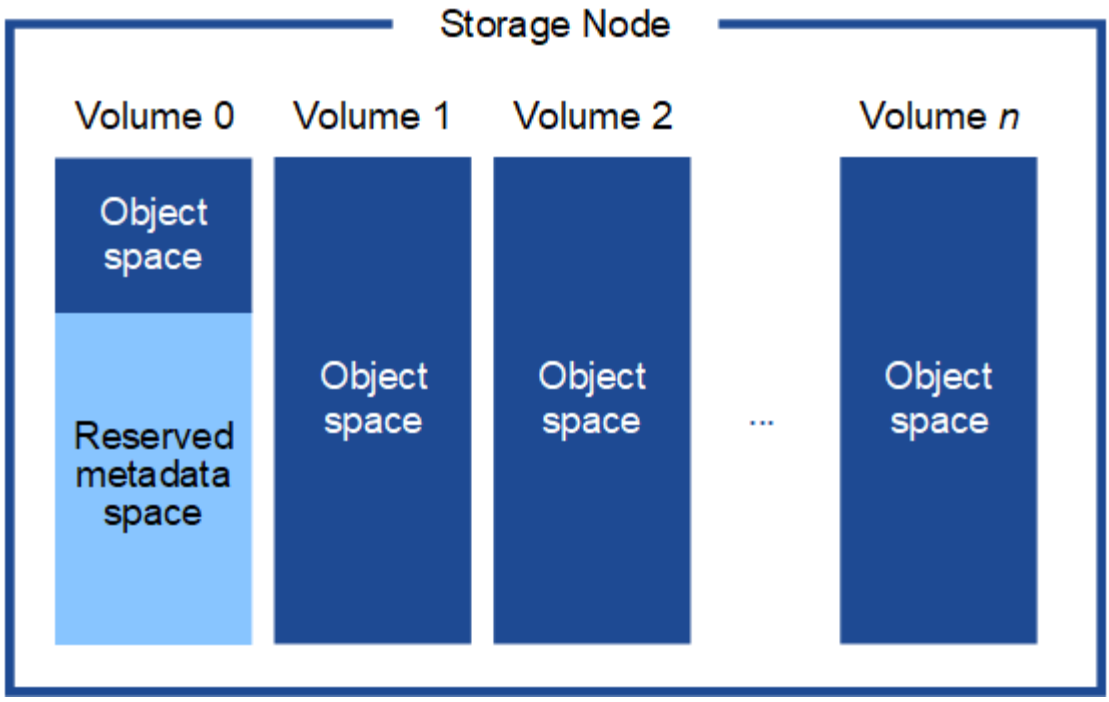
Tipo di nodo	Scopo del LUN	Numero di LUN	Dimensione del LUN
Nodo di storage	Pool di storage Docker	1	300 GB (100 GB/nodo)
Nodo di storage	`/var/local` volume	1	90 GB
Nodo di storage	Dati dell'oggetto	3	12 TB (4 TB/LUN)
Nodo Admin	`/var/local` volume	1	90 GB
Nodo Admin	Registri di audit del nodo di amministrazione	1	200 GB
Nodo Admin	Tabelle del nodo di amministrazione	1	200 GB
Nodo gateway	`/var/local` volume	1	90 GB
Totale		**9**	**Pool di container:** 300 GB **Dati di sistema:** 670 GB **Dati oggetto:** 12,000 GB

Requisiti di storage per i nodi di storage

Un nodo di storage basato su software può avere da 1 a 16 volumi di storage: Si consiglia di utilizzare almeno -3 volumi di storage. Ogni volume di storage deve essere pari o superiore a 4 TB.

> Un nodo di storage dell'appliance può avere fino a 48 volumi di storage.

Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di storage 0 di ciascun nodo di storage. Qualsiasi spazio rimanente sul volume di storage 0 e qualsiasi altro volume di storage nel nodo di storage viene utilizzato esclusivamente per i dati a oggetti.



Per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti del sistema in ogni sito. Le tre copie dei metadati degli oggetti sono distribuite in modo uniforme in tutti i nodi di storage di ciascun sito.

Quando si installa un grid con nodi di storage solo metadati, il grid deve anche contenere un numero minimo di nodi per lo storage a oggetti. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

- Per un grid a sito singolo, vengono configurati almeno due nodi storage per oggetti e metadati.
- Per un grid multisito, per gli oggetti e i metadati viene configurato almeno un nodo di storage per sito.

Quando si assegna spazio al volume 0 di un nuovo nodo di storage, è necessario assicurarsi che vi sia spazio sufficiente per la porzione di tale nodo di tutti i metadati dell'oggetto.

- È necessario assegnare almeno 4 TB al volume 0.

> Se si utilizza un solo volume di storage per un nodo di storage e si assegnano 4 TB o meno al volume, il nodo di storage potrebbe entrare nello stato di sola lettura dello storage all'avvio e memorizzare solo i metadati degli oggetti.

> Se si assegnano meno di 500 GB al volume 0 (solo per uso non in produzione), il 10% della capacità del volume di storage viene riservato ai metadati.

- Le risorse dei nodi di solo metadati basate su software devono corrispondere alle risorse dei nodi di storage esistenti. Ad esempio:
  - Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:
    - 128 GB DI RAM
    - CPU a 8 core
    - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)

- Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuale con 24 GB di RAM, 8 core CPU e 3 TB o 4TB di memorizzazione di metadati, i nodi basati solo sui metadati del software devono utilizzare risorse simili (24 GB di RAM, 8 core CPU e 4TB di memorizzazione di metadati (rangedb/0).

  Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve almeno StorageGRID corrispondere ai nodi storage dei siti StorageGRID esistenti e alle nuove risorse del sito.

- Se si sta installando un nuovo sistema (StorageGRID 11.6 o superiore) e ciascun nodo di storage dispone di almeno 128 GB di RAM, assegnare 8 TB o più al volume 0. L'utilizzo di un valore maggiore per il volume 0 può aumentare lo spazio consentito per i metadati su ciascun nodo di storage.
- Quando si configurano diversi nodi di storage per un sito, utilizzare la stessa impostazione per il volume 0, se possibile. Se un sito contiene nodi di storage di dimensioni diverse, il nodo di storage con il volume più piccolo 0 determinerà la capacità dei metadati di quel sito.

Per ulteriori informazioni, visitare il sito Web all'indirizzo "Gestire lo storage dei metadati degli oggetti".

Requisiti per la migrazione dei container di nodi

La funzione di migrazione dei nodi consente di spostare manualmente un nodo da un host all'altro. In genere, entrambi gli host si trovano nello stesso data center fisico.

La migrazione dei nodi consente di eseguire la manutenzione fisica degli host senza interrompere le operazioni di grid. Tutti i nodi StorageGRID vengono spostati uno alla volta su un altro host prima di portare l'host fisico offline. La migrazione dei nodi richiede solo un breve downtime per ciascun nodo e non deve influire sul funzionamento o sulla disponibilità dei servizi grid.

Se si desidera utilizzare la funzionalità di migrazione dei nodi StorageGRID, l'implementazione deve soddisfare requisiti aggiuntivi:

- Nomi di interfaccia di rete coerenti tra gli host di un singolo data center fisico
- Storage condiviso per i metadati StorageGRID e i volumi di repository di oggetti accessibili da tutti gli host in un singolo data center fisico. Ad esempio, è possibile utilizzare gli storage array NetApp e-Series.

Se si utilizzano host virtuali e il layer hypervisor sottostante supporta la migrazione delle macchine virtuali, è possibile utilizzare questa funzionalità invece della funzionalità di migrazione dei nodi in StorageGRID. In questo caso, è possibile ignorare questi requisiti aggiuntivi.

Prima di eseguire la migrazione o la manutenzione dell'hypervisor, arrestare correttamente i nodi. Consultare le istruzioni per "chiusura di un nodo di rete".

VMware Live Migration non supportato

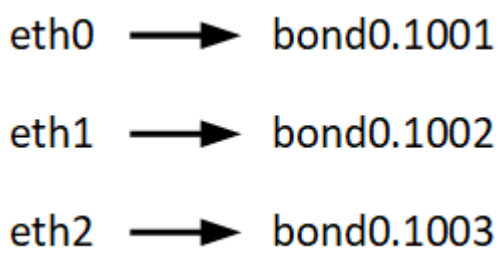
Quando si esegue l'installazione bare-metal su macchine virtuali VMware, OpenStack Live Migration e VMware Live vMotion causano l'aumento del tempo di clock della macchina virtuale e non sono supportati per nodi grid di qualsiasi tipo. Anche se rari, tempi di clock errati possono causare la perdita di dati o aggiornamenti della configurazione.

La migrazione a freddo è supportata. Durante la migrazione a freddo, i nodi StorageGRID vengono arrestati prima della migrazione tra host. Consultare le istruzioni per "chiusura di un nodo di rete".

Nomi di interfaccia di rete coerenti

Per spostare un nodo da un host a un altro, il servizio host StorageGRID deve avere una certa certezza che la connettività di rete esterna del nodo nella sua posizione corrente possa essere duplicata nella nuova posizione. Questa sicurezza viene ottenuta grazie all'utilizzo di nomi di interfaccia di rete coerenti negli host.

Si supponga, ad esempio, che StorageGRID NodeA in esecuzione sull'host 1 sia stato configurato con le seguenti mappature di interfaccia:



Il lato sinistro delle frecce corrisponde alle interfacce tradizionali visualizzate all'interno di un container StorageGRID (ovvero le interfacce griglia, Amministratore e rete client, rispettivamente). Il lato destro delle frecce corrisponde alle interfacce host effettive che forniscono queste reti, che sono tre interfacce VLAN subordinate allo stesso legame di interfaccia fisico.

Supponiamo ora di voler migrare NodeA in Host2. Se l'host 2 ha anche interfacce denominate bond0.1001, bond0.1002 e bond0.1003, il sistema consentirà lo spostamento, supponendo che le interfacce con nome simile forniscano la stessa connettività sull'host 2 di quella sull'host 1. Se l'host 2 non dispone di interfacce con gli stessi nomi, lo spostamento non sarà consentito.

Esistono diversi modi per ottenere un nome coerente dell'interfaccia di rete tra più host; vedere "Configurare la rete host" per alcuni esempi.

Storage condiviso

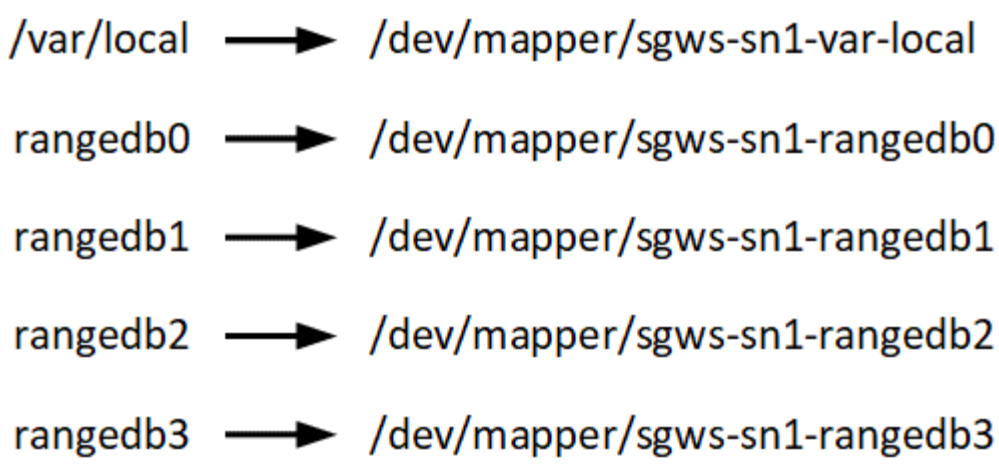
Per ottenere migrazioni dei nodi rapide e a basso overhead, la funzionalità di migrazione dei nodi StorageGRID non sposta fisicamente i dati dei nodi. La migrazione dei nodi viene invece eseguita come coppia di operazioni di esportazione e importazione, come segue:

Fasi

1. Durante l'operazione di "esportazione dei nodi", una piccola quantità di dati di stato persistenti viene estratta dal contenitore di nodi in esecuzione sull'host e memorizzata nella cache sul volume di dati di sistema di quel nodo. Quindi, il contenitore di nodi su Hosta viene decreato.
2. Durante l'operazione di "importazione nodo", viene creata un'istanza del contenitore di nodo sull'HostB che utilizza la stessa interfaccia di rete e le mappature di archiviazione di blocco in vigore sull'Hosta. Quindi, i dati dello stato persistente memorizzati nella cache vengono inseriti nella nuova istanza.

Data questa modalità operativa, tutti i dati di sistema e i volumi di storage a oggetti del nodo devono essere accessibili sia da host che da host B affinché la migrazione sia consentita e funzioni. Inoltre, devono essere stati mappati nel nodo utilizzando nomi che sono garantiti per fare riferimento alle stesse LUN su Hosta e HostB.

Nell'esempio riportato di seguito viene illustrata una soluzione per il mapping dei dispositivi a blocchi per un nodo di storage StorageGRID, in cui il multipathing DM è in uso sugli host e il campo alias è stato utilizzato in `/etc/multipath.conf` fornire nomi di dispositivi a blocchi coerenti e intuitivi disponibili su tutti gli host.



Preparare gli host (Ubuntu o Debian)

Come cambiano le impostazioni dell'intero host durante l'installazione

Nei sistemi bare metal, StorageGRID apporta alcune modifiche all'intero host `sysctl` impostazioni.

Vengono apportate le seguenti modifiche:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
```

```
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
```

```
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Installare Linux

È necessario installare StorageGRID su tutti i grid host Ubuntu o Debian. Per un elenco delle versioni supportate, utilizza lo strumento matrice di interoperabilità NetApp.

Assicurarsi che il sistema operativo sia aggiornato al kernel Linux 4.15 o superiore.

Fasi

1. Installare Linux su tutti gli host grid fisici o virtuali in base alle istruzioni del distributore o alla procedura standard.

   Non installare ambienti desktop grafici. Quando si installa Ubuntu, è necessario selezionare **utility di sistema standard**. Si consiglia di selezionare **OpenSSH server** per abilitare l'accesso ssh agli host Ubuntu. Tutte le altre opzioni possono rimanere deselezionate.

2. Assicurarsi che tutti gli host abbiano accesso ai repository dei pacchetti di Ubuntu o Debian.
3. Se lo swap è attivato:
   a. Eseguire il seguente comando: `$ sudo swapoff --all`
   b. Rimuovere tutte le voci di swap da `/etc/fstab` per mantenere le impostazioni.

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

Comprendere l'installazione del profilo AppArmor

Se si opera in un ambiente Ubuntu autodistribuito e si utilizza il sistema di controllo degli accessi obbligatorio AppArmor, i profili AppArmor associati ai pacchetti installati sul sistema di base potrebbero essere bloccati dai pacchetti corrispondenti installati con StorageGRID.

Per impostazione predefinita, i profili AppArmor vengono installati per i pacchetti installati sul sistema operativo di base. Quando si eseguono questi pacchetti dal container di sistema StorageGRID, i profili AppArmor vengono bloccati. Anche i pacchetti di base DHCP, MySQL, NTP e tcdump sono in conflitto con AppArmor e altri pacchetti di base potrebbero entrare in conflitto.

Esistono due opzioni per la gestione dei profili AppArmor:

- Disattivare i singoli profili per i pacchetti installati sul sistema di base che si sovrappongono ai pacchetti nel container di sistema StorageGRID. Quando si disattivano singoli profili, nei file di log di StorageGRID viene visualizzata una voce che indica che AppArmor è abilitato.

  Utilizzare i seguenti comandi:

```
sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
```

Esempio:

```
sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/bin.ping
```

- Disattiva AppArmor del tutto. Per Ubuntu 9.10 o versioni successive, seguire le istruzioni della community online di Ubuntu: "Disattiva AppArmor". La disattivazione totale di AppArmor potrebbe non essere possibile sulle versioni più recenti di Ubuntu.

  Dopo aver disattivato AppArmor, nei file di registro di StorageGRID non verrà visualizzata alcuna voce che indichi che AppArmor è attivato.

Configurare la rete host (Ubuntu o Debian)

Dopo aver completato l'installazione di Linux sugli host, potrebbe essere necessario eseguire alcune configurazioni aggiuntive per preparare un set di interfacce di rete su ciascun host adatte per il mapping nei nodi StorageGRID che verranno implementati in seguito.

Prima di iniziare

- Hai esaminato il "Linee guida per il networking StorageGRID".
- Sono state esaminate le informazioni su "requisiti per la migrazione dei container di nodi".
- Se si utilizzano host virtuali, è stato letto il Considerazioni e consigli per la clonazione degli indirizzi MAC prima di configurare la rete host.

> Se si utilizzano macchine virtuali come host, selezionare VMXNET 3 come scheda di rete virtuale. L'adattatore di rete VMware E1000 ha causato problemi di connettività con i container StorageGRID implementati su determinate distribuzioni di Linux.

A proposito di questa attività

I nodi Grid devono essere in grado di accedere alla rete Grid e, facoltativamente, alle reti Admin e Client. È possibile fornire questo accesso creando mappature che associano l'interfaccia fisica dell'host alle interfacce virtuali per ciascun nodo della griglia. Quando si creano interfacce host, utilizzare nomi descrittivi per facilitare l'implementazione su tutti gli host e per abilitare la migrazione.

La stessa interfaccia può essere condivisa tra l'host e uno o più nodi. Ad esempio, è possibile utilizzare la stessa interfaccia per l'accesso all'host e l'accesso alla rete di amministrazione del nodo, per facilitare la manutenzione di host e nodi. Sebbene sia possibile condividere la stessa interfaccia tra l'host e i singoli nodi, tutti devono avere indirizzi IP diversi. Gli indirizzi IP non possono essere condivisi tra nodi o tra l'host e qualsiasi nodo.

È possibile utilizzare la stessa interfaccia di rete host per fornire l'interfaccia di rete griglia per tutti i nodi StorageGRID sull'host; è possibile utilizzare un'interfaccia di rete host diversa per ciascun nodo oppure eseguire operazioni intermedie. Tuttavia, in genere, non è possibile fornire la stessa interfaccia di rete host

delle interfacce Grid e Admin Network per un singolo nodo o Grid Network per un nodo e Client Network per un altro.

Puoi completare questa attività in molti modi. Ad esempio, se gli host sono macchine virtuali e si stanno implementando uno o due nodi StorageGRID per ciascun host, è possibile creare il numero corretto di interfacce di rete nell'hypervisor e utilizzare un mapping 1-to-1. Se si implementano più nodi su host bare metal per uso in produzione, è possibile sfruttare il supporto dello stack di rete Linux per VLAN e LACP per la fault tolerance e la condivisione della larghezza di banda. Le sezioni seguenti forniscono approcci dettagliati per entrambi questi esempi. Non è necessario utilizzare nessuno di questi esempi: È possibile utilizzare qualsiasi approccio che soddisfi le proprie esigenze.

> Non utilizzare dispositivi bond o bridge direttamente come interfaccia di rete container. In questo modo si potrebbe impedire l'avvio del nodo causato da un problema del kernel con l'utilizzo di MACVLAN con dispositivi bond e bridge nello spazio dei nomi container. Utilizzare invece un dispositivo non-bond, ad esempio una coppia VLAN o Virtual Ethernet (veth). Specificare questo dispositivo come interfaccia di rete nel file di configurazione del nodo.

Considerazioni e consigli per la clonazione degli indirizzi MAC

La clonazione dell'indirizzo MAC fa in modo che il container utilizzi l'indirizzo MAC dell'host e l'host utilizzi l'indirizzo MAC di un indirizzo specificato o generato in modo casuale. È necessario utilizzare la clonazione dell'indirizzo MAC per evitare l'utilizzo di configurazioni di rete in modalità promiscua.

Abilitazione della clonazione MAC

In alcuni ambienti, la sicurezza può essere migliorata mediante la clonazione dell'indirizzo MAC, in quanto consente di utilizzare una NIC virtuale dedicata per Admin Network, Grid Network e Client Network. Il fatto che il container utilizzi l'indirizzo MAC della scheda NIC dedicata sull'host consente di evitare l'utilizzo di configurazioni di rete promiscue mode.

> La clonazione dell'indirizzo MAC è destinata all'utilizzo con le installazioni di server virtuali e potrebbe non funzionare correttamente con tutte le configurazioni fisiche delle appliance.

> Se un nodo non si avvia a causa di un'interfaccia di destinazione per la clonazione MAC occupata, potrebbe essere necessario impostare il collegamento su "inattivo" prima di avviare il nodo. Inoltre, è possibile che l'ambiente virtuale impedisca la clonazione MAC su un'interfaccia di rete mentre il collegamento è attivo. Se un nodo non riesce a impostare l'indirizzo MAC e si avvia a causa di un'interfaccia occupata, impostare il collegamento su "inattivo" prima di avviare il nodo potrebbe risolvere il problema.

La clonazione dell'indirizzo MAC è disattivata per impostazione predefinita e deve essere impostata mediante le chiavi di configurazione del nodo. È necessario attivarlo quando si installa StorageGRID.

Per ogni rete è disponibile una chiave:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Impostando la chiave su "true", il container utilizza l'indirizzo MAC della NIC dell'host. Inoltre, l'host utilizzerà l'indirizzo MAC della rete container specificata. Per impostazione predefinita, l'indirizzo del contenitore è un

indirizzo generato in modo casuale, ma se ne è stato impostato uno utilizzando `_NETWORK_MAC` chiave di configurazione del nodo, viene utilizzato l'indirizzo. L'host e il container avranno sempre indirizzi MAC diversi.

> L'attivazione della clonazione MAC su un host virtuale senza attivare anche la modalità promiscua sull'hypervisor potrebbe causare l'interruzione del funzionamento della rete host Linux che utilizza l'interfaccia dell'host.

Casi di utilizzo della clonazione MAC

Esistono due casi di utilizzo da considerare con la clonazione MAC:

- CLONAZIONE MAC non abilitata: Quando `_CLONE_MAC` La chiave nel file di configurazione del nodo non è impostata, o impostata su "false", l'host utilizzerà il MAC NIC host e il container avrà un MAC generato da StorageGRID, a meno che non sia specificato un MAC in `_NETWORK_MAC` chiave. Se un indirizzo è impostato in `_NETWORK_MAC` il contenitore avrà l'indirizzo specificato in `_NETWORK_MAC` chiave. Questa configurazione delle chiavi richiede l'utilizzo della modalità promiscua.
- CLONAZIONE MAC abilitata: Quando `_CLONE_MAC` La chiave nel file di configurazione del nodo è impostata su "true", il container utilizza il MAC NIC host e l'host utilizza un MAC generato da StorageGRID, a meno che non sia specificato un MAC in `_NETWORK_MAC` chiave. Se un indirizzo è impostato in `_NETWORK_MAC` l'host utilizza l'indirizzo specificato invece di quello generato. In questa configurazione di chiavi, non si dovrebbe utilizzare la modalità promiscua.

> Se non si desidera utilizzare la clonazione dell'indirizzo MAC e si desidera consentire a tutte le interfacce di ricevere e trasmettere dati per indirizzi MAC diversi da quelli assegnati dall'hypervisor, Assicurarsi che le proprietà di sicurezza a livello di switch virtuale e gruppo di porte siano impostate su **Accept** per modalità promiscuous, modifiche indirizzo MAC e trasmissione forgiata. I valori impostati sullo switch virtuale possono essere sovrascritti dai valori a livello di gruppo di porte, quindi assicurarsi che le impostazioni siano le stesse in entrambe le posizioni.

Per attivare la clonazione MAC, consultare "istruzioni per la creazione dei file di configurazione del nodo".

Esempio di clonazione MAC

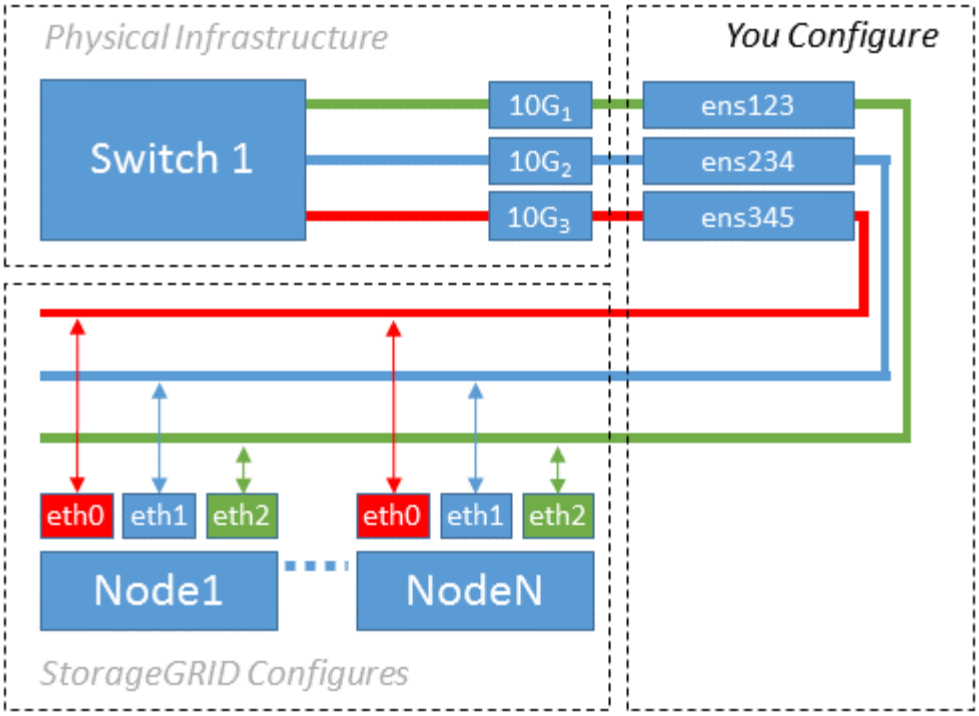
Esempio di clonazione MAC abilitata con un host con indirizzo MAC 11:22:33:44:55:66 per l'interfaccia ens256 e le seguenti chiavi nel file di configurazione del nodo:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Risultato: Il MAC host per ens256 è b2:9c:02:c2:27:10 e il MAC Admin Network è 11:22:33:44:55:66

Esempio 1: Mappatura 1 a 1 su NIC fisiche o virtuali

L'esempio 1 descrive una semplice mappatura dell'interfaccia fisica che richiede una configurazione minima o nulla sul lato host.



Il sistema operativo Linux crea automaticamente le interfacce ensXYZ durante l'installazione, l'avvio o quando le interfacce vengono aggiunte a caldo. Non è richiesta alcuna configurazione se non quella di garantire che le interfacce siano impostate in modo che si avviino automaticamente dopo l'avvio. È necessario determinare quale ensXYZ corrisponde a quale rete StorageGRID (griglia, amministratore o client) in modo da poter fornire le mappature corrette in un secondo momento del processo di configurazione.

Si noti che la figura mostra più nodi StorageGRID; tuttavia, normalmente si utilizza questa configurazione per macchine virtuali a nodo singolo.

Se lo switch 1 è uno switch fisico, configurare le porte collegate alle interfacce da $10G_1$ a $10G_3$ per la modalità di accesso e posizionarle sulle VLAN appropriate.

Esempio 2: Collegamento LACP con VLAN

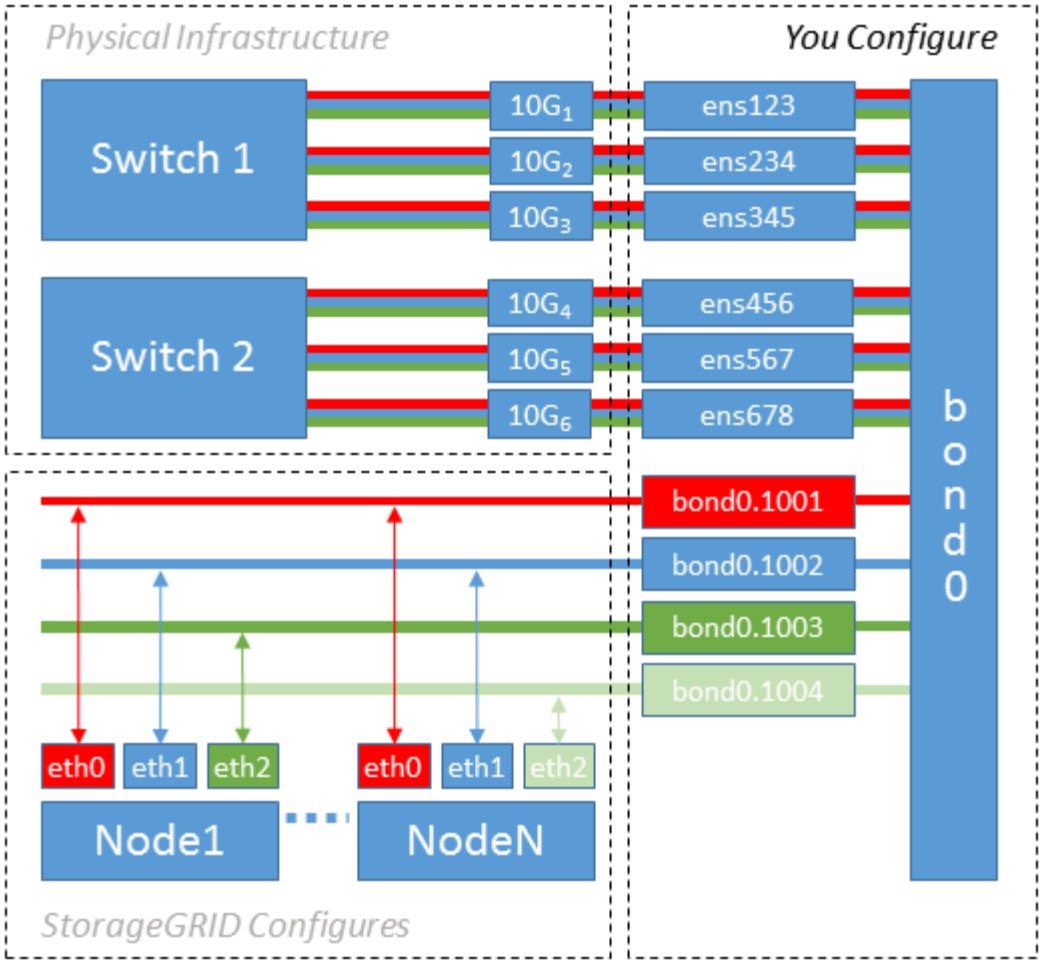
L'esempio 2 presuppone che si abbia familiarità con il bonding delle interfacce di rete e con la creazione di interfacce VLAN sulla distribuzione Linux in uso.

A proposito di questa attività

L'esempio 2 descrive uno schema generico, flessibile e basato su VLAN che facilita la condivisione di tutta la larghezza di banda di rete disponibile in tutti i nodi su un singolo host. Questo esempio è particolarmente applicabile agli host bare metal.

Per comprendere questo esempio, si supponga di disporre di tre subnet separate per le reti Grid, Admin e Client in ogni data center. Le sottoreti si trovano su VLAN separate (1001, 1002 e 1003) e vengono presentate all'host su una porta di trunk collegata LACP (bond0). Configurare tre interfacce VLAN sul bond: Bond0.1001, bond0.1002 e bond0.1003.

Se si richiedono VLAN e subnet separate per le reti di nodi sullo stesso host, è possibile aggiungere interfacce VLAN sul collegamento e mapparle nell'host (come illustrato nella figura come bond0.1004).



Fasi

1. Aggregare tutte le interfacce di rete fisiche che verranno utilizzate per la connettività di rete StorageGRID in un unico collegamento LACP.

   Utilizzare lo stesso nome per il bond su ogni host, ad esempio bond0.

2. Creare interfacce VLAN che utilizzano questo collegamento come "dispositivo fisico" associato utilizzando la convenzione di denominazione dell'interfaccia VLAN standard `physdev-name.VLAN ID`.

   I passi 1 e 2 richiedono una configurazione appropriata sugli edge switch che terminano le altre estremità dei collegamenti di rete. Le porte degli edge switch devono anche essere aggregate in un canale di porta LACP, configurate come trunk e in grado di passare tutte le VLAN richieste.

   Vengono forniti file di configurazione di interfaccia di esempio per questo schema di configurazione di rete per host.

Informazioni correlate

"Esempio di /etc/network/interfaces"

Configurare lo storage host

È necessario allocare volumi di storage a blocchi a ciascun host.

Prima di iniziare

Sono stati esaminati i seguenti argomenti, che forniscono le informazioni necessarie per eseguire questa attività:

"Requisiti di storage e performance"

"Requisiti per la migrazione dei container di nodi"

A proposito di questa attività

Quando si allocano i volumi di storage a blocchi (LUN) agli host, utilizzare le tabelle in "requisiti di archiviazione" per determinare quanto segue:

- Numero di volumi richiesti per ciascun host (in base al numero e ai tipi di nodi che verranno implementati su tale host)
- Categoria di storage per ciascun volume (ovvero dati di sistema o dati oggetto)
- Dimensione di ciascun volume

Quando si distribuiscono i nodi StorageGRID sull'host, verranno utilizzate queste informazioni e il nome persistente assegnato da Linux a ciascun volume fisico.

Non è necessario partizionare, formattare o montare nessuno di questi volumi; è sufficiente assicurarsi che siano visibili agli host.

È necessaria una sola LUN per i dati degli oggetti per i nodi di storage basati solo sui metadati.

Evitare di utilizzare file speciali "RAW" del dispositivo (`/dev/sdb`, ad esempio) mentre si compone l'elenco dei nomi dei volumi. Questi file possono cambiare durante i riavvii dell'host, il che avrà un impatto sul corretto funzionamento del sistema. Se si utilizzano LUN iSCSI e multipathing di Device Mapper, considerare l'utilizzo di alias multipath in `/dev/mapper` Directory, soprattutto se la topologia SAN include percorsi di rete ridondanti per lo storage condiviso. In alternativa, è possibile utilizzare i softlink creati dal sistema in `/dev/disk/by-path/` per i nomi persistenti dei dispositivi.

Ad esempio:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

I risultati saranno diversi per ogni installazione.

Assegnare nomi descrittivi a ciascuno di questi volumi di storage a blocchi per semplificare l'installazione iniziale di StorageGRID e le future procedure di manutenzione. Se si utilizza il driver multipath del device mapper per l'accesso ridondante ai volumi di storage condivisi, è possibile utilizzare `alias` nel campo `/etc/multipath.conf` file.

Ad esempio:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

In questo modo, gli alias verranno visualizzati come dispositivi a blocchi in `/dev/mapper` directory sull'host, che consente di specificare un nome semplice e facilmente validato ogni volta che un'operazione di configurazione o manutenzione richiede la specifica di un volume di storage a blocchi.

> Se si imposta lo storage condiviso per supportare la migrazione dei nodi StorageGRID e si utilizza il multipathing di Device Mapper, è possibile creare e installare un file comune `/etc/multipath.conf` su tutti gli host co-locati. Assicurati di utilizzare un volume di storage Docker diverso su ciascun host. L'utilizzo di alias e l'inclusione del nome host di destinazione nell'alias per ogni LUN del volume di storage Docker renderà questa operazione facile da ricordare ed è consigliabile.

Informazioni correlate

"Requisiti di storage e performance"

"Requisiti per la migrazione dei container di nodi"

Configurare il volume di storage Docker

Prima di installare Docker, potrebbe essere necessario formattare il volume di storage Docker e montarlo `/var/lib/docker`.

A proposito di questa attività

È possibile saltare questi passaggi se si intende utilizzare lo storage locale per il volume di storage Docker e si dispone di spazio sufficiente sulla partizione host contenente `/var/lib`.

Fasi

1. Creare un file system sul volume di storage Docker:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Montare il volume di storage Docker:

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. Aggiungere una voce per docker-storage-volume-device a /etc/fstab.

   Questo passaggio garantisce che il volume di storage venga rimontato automaticamente dopo il riavvio dell'host.

Installare Docker

Il sistema StorageGRID viene eseguito su Linux come una raccolta di container Docker. Prima di poter installare StorageGRID, è necessario installare Docker.

Fasi

1. Installare Docker seguendo le istruzioni per la distribuzione Linux.

   > Se Docker non è incluso nella distribuzione Linux, è possibile scaricarlo dal sito Web di Docker.

2. Assicurarsi che Docker sia stato attivato e avviato eseguendo i seguenti due comandi:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Verificare di aver installato la versione prevista di Docker inserendo quanto segue:

```
sudo docker version
```

Le versioni del client e del server devono essere 1.11.0 o successive.

Informazioni correlate

"Configurare lo storage host"

Installare i servizi host StorageGRID

Il pacchetto DEB di StorageGRID viene utilizzato per installare i servizi host di StorageGRID.

A proposito di questa attività

Queste istruzioni descrivono come installare i servizi host dai pacchetti DEB. In alternativa, è possibile utilizzare i metadati del repository APT inclusi nell'archivio di installazione per installare i pacchetti DEB in remoto. Consultare le istruzioni del repository APT per il sistema operativo Linux in uso.

Fasi

1. Copiare i pacchetti DEB di StorageGRID su ciascuno degli host o renderli disponibili sullo storage condiviso.

   Ad esempio, inserirli in `/tmp` directory, in modo da poter utilizzare il comando di esempio nel passaggio successivo.

2. Accedere a ciascun host come root o utilizzando un account con autorizzazione sudo ed eseguire i seguenti comandi.

   È necessario installare `images` prima il pacchetto e il `service` pacchetto secondo. Se i pacchetti sono inseriti in una directory diversa da `/tmp`, modificare il comando in modo che rifletta il percorso utilizzato.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```

> Python 2.7 deve essere già installato prima di poter installare i pacchetti StorageGRID. Il `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` il comando non riuscirà fino a quando non sarà stato fatto.

Automatizzare l'installazione (Ubuntu o Debian)

È possibile automatizzare l'installazione del servizio host StorageGRID e la configurazione dei nodi di rete.

A proposito di questa attività

L'automazione della distribuzione può essere utile in uno dei seguenti casi:

- Si utilizza già un framework di orchestrazione standard, ad esempio Ansible, Puppet o Chef, per implementare e configurare host fisici o virtuali.
- Si intende implementare più istanze di StorageGRID.
- Si sta implementando un'istanza di StorageGRID grande e complessa.

Il servizio host di StorageGRID viene installato da un pacchetto e gestito da file di configurazione che possono essere creati in modo interattivo durante un'installazione manuale o preparati in anticipo (o a livello di programmazione) per consentire l'installazione automatica utilizzando framework di orchestrazione standard. StorageGRID fornisce script Python opzionali per automatizzare la configurazione delle appliance StorageGRID e dell'intero sistema StorageGRID (il "grid"). È possibile utilizzare questi script direttamente o ispezionarli per scoprire come utilizzare l'API REST per l'installazione di StorageGRID nei tool di configurazione e distribuzione grid sviluppati da soli.

Automatizzare l'installazione e la configurazione del servizio host StorageGRID

È possibile automatizzare l'installazione del servizio host StorageGRID utilizzando framework di orchestrazione standard come Ansible, Puppet, Chef, Fabric o SaltStack.

Il servizio host di StorageGRID è confezionato in un DEB ed è gestito da file di configurazione che possono essere preparati in anticipo (o a livello di programmazione) per consentire l'installazione automatica. Se si utilizza già un framework di orchestrazione standard per installare e configurare Ubuntu o Debian, aggiungere StorageGRID ai propri playbook o alle proprie ricette dovrebbe essere semplice.

È possibile automatizzare queste attività:

1. Installazione di Linux
2. Configurazione di Linux
3. Configurazione delle interfacce di rete host per soddisfare i requisiti StorageGRID
4. Configurazione dello storage host per soddisfare i requisiti StorageGRID
5. Installazione di Docker
6. Installazione del servizio host StorageGRID
7. Creazione dei file di configurazione del nodo StorageGRID in `/etc/storagegrid/nodes`
8. Convalida dei file di configurazione del nodo StorageGRID
9. Avvio del servizio host StorageGRID

Esempio di Ansible role and playbook

Ad esempio, il ruolo e il playbook Ansible vengono forniti con l'archivio di installazione nel `/extras` cartella. Il playbook Ansible mostra come `storagegrid` Il ruolo prepara gli host e installa StorageGRID sui server di destinazione. È possibile personalizzare il ruolo o il manuale in base alle esigenze.

Automatizzare la configurazione di StorageGRID

Una volta implementati i nodi grid, è possibile automatizzare la configurazione del sistema StorageGRID.

Prima di iniziare

- Si conosce la posizione dei seguenti file dall'archivio di installazione.

Nome file	Descrizione
configure-storagegrid.py	Script Python utilizzato per automatizzare la configurazione
configure-storagegrid.sample.json	File di configurazione di esempio da utilizzare con lo script
configure-storagegrid.blank.json	File di configurazione vuoto da utilizzare con lo script

- È stato creato un `configure-storagegrid.json` file di configurazione. Per creare questo file, è possibile modificare il file di configurazione di esempio (`configure-storagegrid.sample.json`) o il file di configurazione vuoto (`configure-storagegrid.blank.json`).

A proposito di questa attività

È possibile utilizzare `configure-storagegrid.py` Script Python e il `configure-storagegrid.json` File di configurazione per automatizzare la configurazione del sistema StorageGRID.

È inoltre possibile configurare il sistema utilizzando Grid Manager o l'API di installazione.

Fasi

1. Accedere alla macchina Linux in uso per eseguire lo script Python.
2. Passare alla directory in cui è stato estratto l'archivio di installazione.

   Ad esempio:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   dove `platform` è `debs`, `rpms`, o. `vsphere`.

3. Eseguire lo script Python e utilizzare il file di configurazione creato.

   Ad esempio:

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Risultato

Un pacchetto di ripristino `.zip` il file viene generato durante il processo di configurazione e scaricato nella directory in cui si esegue il processo di installazione e configurazione. È necessario eseguire il backup del file del pacchetto di ripristino in modo da poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi della griglia. Ad esempio, copiarla in una posizione di rete sicura e di backup e in una posizione di cloud storage sicura.

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.

Se si specifica che devono essere generate password casuali, aprire `Passwords.txt` E cercare le password necessarie per accedere al sistema StorageGRID.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Il sistema StorageGRID viene installato e configurato quando viene visualizzato un messaggio di conferma.

```
StorageGRID has been configured and installed.
```

Informazioni correlate

"Panoramica dell'API REST per l'installazione"

Implementare nodi virtual grid (Ubuntu o Debian)

Creare file di configurazione del nodo per le distribuzioni Ubuntu o Debian

I file di configurazione dei nodi sono piccoli file di testo che forniscono le informazioni necessarie al servizio host StorageGRID per avviare un nodo e collegarlo alla rete appropriata e bloccare le risorse di storage. I file di configurazione dei nodi vengono utilizzati per i nodi virtuali e non per i nodi appliance.

Posizione dei file di configurazione dei nodi

Posizionare il file di configurazione per ogni nodo StorageGRID in `/etc/storagegrid/nodes` directory sull'host in cui verrà eseguito il nodo. Ad esempio, se si intende eseguire un nodo Admin, un nodo Gateway e un nodo Storage sull'host, è necessario inserire tre file di configurazione del nodo `/etc/storagegrid/nodes` Su host.

È possibile creare i file di configurazione direttamente su ciascun host utilizzando un editor di testo, ad esempio vim o nano, oppure crearli altrove e spostarli su ciascun host.

Denominazione dei file di configurazione dei nodi

I nomi dei file di configurazione sono significativi. Il formato è `node-name.conf`, dove `node-name` è un nome assegnato al nodo. Questo nome viene visualizzato nel programma di installazione di StorageGRID e viene utilizzato per le operazioni di manutenzione dei nodi, ad esempio la migrazione dei nodi.

I nomi dei nodi devono seguire queste regole:

- Deve essere unico
- Deve iniziare con una lettera
- Può contenere i caratteri Da A a Z e da a a z

- Può contenere i numeri da 0 a 9
- Può contenere uno o più trattini (-)
- Non deve contenere più di 32 caratteri, ad eccezione di `.conf` interno

Qualsiasi file in `/etc/storagegrid/nodes` che non seguono queste convenzioni di denominazione non verranno analizzata dal servizio host.

Se è stata pianificata una topologia multi-sito per il proprio grid, uno schema di denominazione tipico dei nodi potrebbe essere:

```
site-nodetype-nodenumber.conf
```

Ad esempio, è possibile utilizzare `dc1-adm1.conf` Per il primo nodo Admin nel data center 1, e. `dc2-sn3.conf` Per il terzo nodo di storage nel data center 2. Tuttavia, è possibile utilizzare qualsiasi schema desiderato, purché tutti i nomi dei nodi seguano le regole di denominazione.

Contenuto di un file di configurazione del nodo

Un file di configurazione contiene coppie chiave/valore, con una chiave e un valore per riga. Per ogni coppia chiave/valore, attenersi alle seguenti regole:

- La chiave e il valore devono essere separati da un segno di uguale (=) e spazio vuoto opzionale.
- Le chiavi non possono contenere spazi.
- I valori possono contenere spazi incorporati.
- Qualsiasi spazio iniziale o finale viene ignorato.

La tabella seguente definisce i valori per tutte le chiavi supportate. Ogni chiave ha una delle seguenti designazioni:

- **Obbligatorio**: Richiesto per ogni nodo o per i tipi di nodo specificati
- **Best practice**: Facoltativo, anche se consigliato
- **Opzionale**: Opzionale per tutti i nodi

Chiavi di rete Admin

ADMIN_IP

Valore	Designazione
Grid Network IPv4 address del nodo di amministrazione principale per la griglia a cui appartiene questo nodo. Utilizzare lo stesso valore specificato per GRID_NETWORK_IP per il nodo Grid con NODE_TYPE = VM_Admin_Node e ADMIN_ROLE = Primary. Se si omette questo parametro, il nodo tenta di rilevare un nodo Admin primario utilizzando mDNS. "In che modo i nodi della griglia rilevano il nodo di amministrazione primario" **Nota**: Questo valore viene ignorato e potrebbe essere proibito sul nodo di amministrazione primario.	Best practice

ADMIN_NETWORK_CONFIG

Valore	Designazione
DHCP, STATICO O DISATTIVATO	Opzionale

ADMIN_NETWORK_ESL

Valore	Designazione
Elenco separato da virgole delle subnet nella notazione CIDR a cui il nodo deve comunicare utilizzando il gateway Admin Network. Esempio: `172.16.0.0/21,172.17.0.0/21`	Opzionale

ADMIN_NETWORK_GATEWAY

Valore	Designazione

Indirizzo IPv4 del gateway Admin Network locale per questo nodo. Deve trovarsi nella subnet definita da ADMIN_NETWORK_IP e ADMIN_NETWORK_MASK. Questo valore viene ignorato per le reti configurate con DHCP.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessario se `ADMIN_NETWORK_ESL` viene specificato. Facoltativo altrimenti.

ADMIN_NETWORK_IP

Valore	Designazione

Indirizzo IPv4 di questo nodo nella rete di amministrazione. Questa chiave è necessaria solo quando ADMIN_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessario quando ADMIN_NETWORK_CONFIG = STATICO.
	
	Facoltativo altrimenti.

ADMIN_NETWORK_MAC

Valore	Designazione
L'indirizzo MAC dell'interfaccia Admin Network nel contenitore. Questo campo è facoltativo. Se omesso, viene generato automaticamente un indirizzo MAC. Devono essere 6 coppie di cifre esadecimali separate da due punti. Esempio: `b2:9c:02:c2:27:10`	Opzionale

ADMIN_NETWORK_MASK

Valore	Designazione

Netmask IPv4 per questo nodo, sulla rete di amministrazione. Specificare questa chiave quando ADMIN_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessario se viene specificato ADMIN_NETWORK_IP e ADMIN_NETWORK_CONFIG = STATICO.
	
	Facoltativo altrimenti.

ADMIN_NETWORK_MTU

Valore	Designazione

MTU (Maximum Transmission Unit) per questo nodo nella rete di amministrazione. Non specificare se ADMIN_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omesso, viene utilizzato 1500.
 	
Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito.
 	
IMPORTANTE: Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.
 	
Esempi:
 	
`1500`
 	
`8192`
	Opzionale

ADMIN_NETWORK_TARGET

Valore	Designazione

Nome del dispositivo host che verrà utilizzato per l'accesso alla rete amministrativa dal nodo StorageGRID. Sono supportati solo i nomi delle interfacce di rete. In genere, si utilizza un nome di interfaccia diverso da quello specificato per GRID_NETWORK_TARGET o CLIENT_NETWORK_TARGET.
 	
Nota: Non utilizzare dispositivi bond o bridge come destinazione di rete. Configurare una VLAN (o un'altra interfaccia virtuale) sulla parte superiore del dispositivo bond oppure utilizzare una coppia di bridge e Virtual Ethernet (veth).
 	
Best practice:specificare un valore anche se questo nodo inizialmente non dispone di un indirizzo IP Admin Network. Quindi, è possibile aggiungere un indirizzo IP Admin Network in un secondo momento, senza dover riconfigurare il nodo sull'host.
 	
Esempi:
 	
`bond0.1002`
 	
`ens256`
	Best practice

ADMIN_NETWORK_TARGET_TYPE

Valore	Designazione

Interfaccia (questo è l'unico valore supportato).	Opzionale

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o Falso Impostare la chiave su "true" per fare in modo che il container StorageGRID utilizzi l'indirizzo MAC dell'interfaccia host di destinazione sulla rete di amministrazione. **Best practice:** nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare la chiave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per ulteriori informazioni sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Ubuntu o Debian)"	Best practice

RUOLO_AMMINISTRATORE

Valore	Designazione
Primario o non primario Questa chiave è necessaria solo quando NODE_TYPE = VM_Admin_Node; non specificarla per altri tipi di nodo.	Necessario quando NODE_TYPE = VM_Admin_Node Facoltativo altrimenti.

Bloccare le chiavi del dispositivo

BLOCK_DEVICE_AUDIT_LOGS

Valore	Designazione

Percorso e nome del file speciale del dispositivo a blocchi utilizzato da questo nodo per la memorizzazione persistente dei registri di controllo.
 	
Esempi:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	Richiesto per i nodi con NODE_TYPE = VM_Admin_NODE. Non specificarlo per altri tipi di nodi.

BLOCK_DEVICE_RANGEDB_NNN

Valore	Designazione

Percorso e nome del file speciale del dispositivo a blocchi utilizzato da questo nodo per lo storage a oggetti persistente. Questa chiave è necessaria solo per i nodi con NODE_TYPE = VM_Storage_Node; non specificarla per altri tipi di nodo.
 	
È necessario solo BLOCK_DEVICE_RANGEDB_000; gli altri sono facoltativi. Il dispositivo a blocchi specificato per BLOCK_DEVICE_RANGEDB_000 deve essere di almeno 4 TB; gli altri possono essere più piccoli.
 	
Non lasciare lacune. Se si specifica BLOCK_DEVICE_RANGEDB_005, è necessario specificare ANCHE BLOCK_DEVICE_RANGEDB_004.
 	
Nota: Per la compatibilità con le implementazioni esistenti, sono supportate chiavi a due cifre per i nodi aggiornati.
 	
Esempi:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	Richiesti:
	
	BLOCK_DEVICE_RANGEDB_000
	
	Opzionale:
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002
	
	BLOCK_DEVICE_RANGEDB_003
	
	BLOCK_DEVICE_RANGEDB_004
	
	BLOCK_DEVICE_RANGEDB_005
	
	BLOCK_DEVICE_RANGEDB_006
	
	BLOCK_DEVICE_RANGEDB_007
	
	BLOCK_DEVICE_RANGEDB_008
	
	BLOCK_DEVICE_RANGEDB_009
	
	BLOCK_DEVICE_RANGEDB_010
	
	BLOCK_DEVICE_RANGEDB_011
	
	BLOCK_DEVICE_RANGEDB_012
	
	BLOCK_DEVICE_RANGEDB_013
	
	BLOCK_DEVICE_RANGEDB_014
	
	BLOCK_DEVICE_RANGEDB_015

BLOCK_DEVICE_TABLES

Valore	Designazione

Percorso e nome del file speciale del dispositivo a blocchi utilizzato da questo nodo per l'archiviazione persistente delle tabelle di database. Questa chiave è necessaria solo per i nodi con NODE_TYPE = VM_Admin_Node; non specificarla per altri tipi di nodo.
 	
Esempi:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	Obbligatorio

BLOCK_DEVICE_VAR_LOCAL

Valore	Designazione

Percorso e nome del file speciale del dispositivo di blocco utilizzato da questo nodo per ITS `/var/local` storage persistente.
 	
Esempi:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	Obbligatorio

Chiavi di rete client

CONFIGURAZIONE_RETE_CLIENT

Valore	Designazione
DHCP, STATICO O DISATTIVATO	Opzionale

GATEWAY_RETE_CLIENT

Valore	Designazione

Indirizzo IPv4 del gateway di rete client locale per questo nodo, che deve trovarsi sulla subnet definita da CLIENT_NETWORK_IP e CLIENT_NETWORK_MASK. Questo valore viene ignorato per le reti configurate con DHCP.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Opzionale

IP_RETE_CLIENT

Valore	Designazione

Indirizzo IPv4 di questo nodo sulla rete client.
 	
Questa chiave è necessaria solo quando CLIENT_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessario quando CLIENT_NETWORK_CONFIG = STATICO
	
	Facoltativo altrimenti.

CLIENT_NETWORK_MAC

Valore	Designazione
L'indirizzo MAC dell'interfaccia di rete client nel contenitore. Questo campo è facoltativo. Se omesso, viene generato automaticamente un indirizzo MAC. Devono essere 6 coppie di cifre esadecimali separate da due punti. Esempio: `b2:9c:02:c2:27:20`	Opzionale

CLIENT_NETWORK_MASK

Valore	Designazione

Netmask IPv4 per questo nodo sulla rete client.
 	
Specificare questa chiave quando CLIENT_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessario se viene specificato CLIENT_NETWORK_IP e CLIENT_NETWORK_CONFIG = STATICO
	
	Facoltativo altrimenti.

MTU_RETE_CLIENT

Valore	Designazione

MTU (Maximum Transmission Unit) per questo nodo sulla rete client. Non specificare se CLIENT_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omesso, viene utilizzato 1500.
 	
Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito.
 	
IMPORTANTE: Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.
 	
Esempi:
 	
`1500`
 	
`8192`
	Opzionale

DESTINAZIONE_RETE_CLIENT

Valore	Designazione

Nome del dispositivo host che verrà utilizzato per l'accesso alla rete client dal nodo StorageGRID. Sono supportati solo i nomi delle interfacce di rete. In genere, si utilizza un nome di interfaccia diverso da quello specificato per GRID_NETWORK_TARGET o ADMIN_NETWORK_TARGET.
 	
Nota: Non utilizzare dispositivi bond o bridge come destinazione di rete. Configurare una VLAN (o un'altra interfaccia virtuale) sulla parte superiore del dispositivo bond oppure utilizzare una coppia di bridge e Virtual Ethernet (veth).
 	
Best practice: specificare un valore anche se questo nodo inizialmente non avrà un indirizzo IP di rete client. Quindi, è possibile aggiungere un indirizzo IP di rete client in un secondo momento, senza dover riconfigurare il nodo sull'host.
 	
Esempi:
 	
`bond0.1003`
 	
`ens423`
	Best practice

TIPO_DESTINAZIONE_RETE_CLIENT

Valore	Designazione
Interfaccia (solo valore supportato).	Opzionale

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o Falso Impostare la chiave su "true" per fare in modo che il container StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete client. **Best practice:** nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per ulteriori informazioni sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Ubuntu o Debian)"	Best practice

Chiavi di rete della griglia

GRID_NETWORK_CONFIG

Valore	Designazione
STATICO o DHCP Se non specificato, il valore predefinito è STATICO.	Best practice

GRID_NETWORK_GATEWAY

Valore	Designazione
Indirizzo IPv4 del gateway Grid Network locale per questo nodo, che deve trovarsi sulla subnet definita da GRID_NETWORK_IP e GRID_NETWORK_MASK. Questo valore viene ignorato per le reti configurate con DHCP. Se Grid Network è una singola subnet senza gateway, utilizzare l'indirizzo del gateway standard per la subnet (X. YY.Z.1) o il valore GRID_NETWORK_IP di questo nodo; entrambi i valori semplificheranno le future espansioni Grid Network.	Obbligatorio

IP_RETE_GRIGLIA

Valore	Designazione

Indirizzo IPv4 di questo nodo sulla rete griglia. Questa chiave è necessaria solo quando GRID_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessario quando GRID_NETWORK_CONFIG = STATICO
	
	Facoltativo altrimenti.

GRID_NETWORK_MAC

Valore	Designazione
L'indirizzo MAC dell'interfaccia Grid Network nel contenitore. Devono essere 6 coppie di cifre esadecimali separate da due punti. Esempio: `b2:9c:02:c2:27:30`	Opzionale Se omesso, viene generato automaticamente un indirizzo MAC.

GRID_NETWORK_MASK

Valore	Designazione

Netmask IPv4 per questo nodo sulla rete griglia. Specificare questa chiave quando GRID_NETWORK_CONFIG = STATIC; non specificarla per altri valori.
 	
Esempi:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessario quando viene specificato GRID_NETWORK_IP e GRID_NETWORK_CONFIG = STATICO.
	
	Facoltativo altrimenti.

GRID_NETWORK_MTU

Valore	Designazione

MTU (Maximum Transmission Unit) per questo nodo sulla rete di rete. Non specificare se GRID_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omesso, viene utilizzato 1500.
 	
Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito.
 	
IMPORTANTE: Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.
 	
IMPORTANTE: Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete.
 	
Esempi:
 	
`1500`
 	
`8192`
	Opzionale

GRID_NETWORK_TARGET

Valore	Designazione

Nome del dispositivo host che verrà utilizzato per l'accesso alla rete griglia dal nodo StorageGRID. Sono supportati solo i nomi delle interfacce di rete. In genere, si utilizza un nome di interfaccia diverso da quello specificato per ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET.
 	
Nota: Non utilizzare dispositivi bond o bridge come destinazione di rete. Configurare una VLAN (o un'altra interfaccia virtuale) sulla parte superiore del dispositivo bond oppure utilizzare una coppia di bridge e Virtual Ethernet (veth).
 	
Esempi:
 	
`bond0.1001`
 	
`ens192`
	Obbligatorio

GRID_NETWORK_TARGET_TYPE

Valore	Designazione
Interfaccia (questo è l'unico valore supportato).	Opzionale

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o Falso Impostare il valore della chiave su "true" per fare in modo che il contenitore StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete di rete. **Best practice:** nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per ulteriori informazioni sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Ubuntu o Debian)"	Best practice

Interfaces key

INTERFACE_TARGET_nnnn

Valore	Designazione
Nome e descrizione opzionale per un'interfaccia aggiuntiva che si desidera aggiungere a questo nodo. È possibile aggiungere più interfacce aggiuntive a ciascun nodo. Per *nnnnn*, specificare un numero univoco per ogni voce di INTERFACCIA_TARGET che si sta aggiungendo. Per il valore, specificare il nome dell'interfaccia fisica sull'host bare-metal. Quindi, facoltativamente, aggiungere una virgola e fornire una descrizione dell'interfaccia, che viene visualizzata nella pagina delle interfacce VLAN e nella pagina dei gruppi ha. Esempio: `INTERFACE_TARGET_0001=ens256, Trunk` Se si aggiunge un'interfaccia di linea, è necessario configurare un'interfaccia VLAN in StorageGRID. Se si aggiunge un'interfaccia di accesso, è possibile aggiungerla direttamente a un gruppo ha; non è necessario configurare un'interfaccia VLAN.	Opzionale

Chiave RAM massima

MAXIMUM_RAM

Valore	Designazione

La quantità massima di RAM che questo nodo può consumare. Se questa chiave viene omessa, il nodo non presenta limitazioni di memoria. Quando si imposta questo campo per un nodo a livello di produzione, specificare un valore di almeno 24 GB e da 16 a 32 GB inferiore alla RAM totale di sistema.
 	
Nota: Il valore RAM influisce sullo spazio riservato ai metadati effettivi di un nodo. Vedere "Descrizione di Metadata Reserved Space".
 	
Il formato di questo campo è *`numberunit`*, dove *`unit`* può essere `b`, `k`, `m`, o. `g`.
 	
Esempi:
 	
`24g`
 	
`38654705664b`
 	
Nota: Se si desidera utilizzare questa opzione, è necessario abilitare il supporto del kernel per i gruppi di memoria.
	Opzionale

Chiave del tipo di nodo

NODE_TYPE

Valore	Designazione
Tipo di nodo: Nodo_amministrazione_VM Nodo_storage_VM Nodo_archivio_VM Gateway VM_API	Obbligatorio

Tasti di rimappatura delle porte

PORT_REMAP

Valore	Designazione
Consente di rimapare qualsiasi porta utilizzata da un nodo per comunicazioni interne al nodo di rete o comunicazioni esterne. Il rimapping delle porte è necessario se i criteri di rete aziendali limitano una o più porte utilizzate da StorageGRID, come descritto in "Comunicazioni interne al nodo di rete" oppure "Comunicazioni esterne". **IMPORTANTE**: Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico. **Nota**: Se è impostato solo PORT_REMAP, il mapping specificato viene utilizzato per le comunicazioni in entrata e in uscita. Se VIENE specificato anche PORT_REMAP_INBOUND, PORT_REMAP si applica solo alle comunicazioni in uscita. Il formato utilizzato è: *`network type/protocol/default port used by grid node/new port`*, dove *`network type`* è grid, admin o client, e. *`protocol`* è tcp o udp. Esempio: `PORT_REMAP = client/tcp/18082/443`	Opzionale

PORT_REMAP_INBOUND

Valore	Designazione

Consente di rimapare le comunicazioni in entrata alla porta specificata. Se si specifica PORT_REMAP_INBOUND ma non si specifica un valore per PORT_REMAP, le comunicazioni in uscita per la porta rimangono invariate. **IMPORTANTE**: Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico. Il formato utilizzato è: *`network type/protocol/remapped port /default port used by grid node`*, dove *`network type`* è grid, admin o client, e. *`protocol`* è tcp o udp. Esempio: `PORT_REMAP_INBOUND = grid/tcp/3022/22`	Opzionale

In che modo i nodi della griglia rilevano il nodo di amministrazione primario

I nodi Grid comunicano con il nodo Admin primario per la configurazione e la gestione. Ciascun nodo della griglia deve conoscere l'indirizzo IP del nodo di amministrazione primario sulla rete di griglia.

Per garantire che un nodo Grid possa accedere al nodo Admin primario, è possibile eseguire una delle seguenti operazioni durante l'implementazione del nodo:

- È possibile utilizzare IL parametro ADMIN_IP per inserire manualmente l'indirizzo IP del nodo di amministrazione primario.
- È possibile omettere il parametro ADMIN_IP per fare in modo che il nodo Grid rilevi automaticamente il valore. Il rilevamento automatico è particolarmente utile quando Grid Network utilizza DHCP per assegnare l'indirizzo IP al nodo di amministrazione primario.

Il rilevamento automatico del nodo di amministrazione primario viene eseguito utilizzando un sistema di nomi di dominio multicast (mDNS). Al primo avvio, il nodo di amministrazione primario pubblica il proprio indirizzo IP utilizzando mDNS. Gli altri nodi della stessa sottorete possono quindi ricercare l'indirizzo IP e acquisirlo automaticamente. Tuttavia, poiché il traffico IP multicast non è normalmente instradabile attraverso le sottoreti, i nodi su altre sottoreti non possono acquisire direttamente l'indirizzo IP del nodo di amministrazione primario.

Se si utilizza la ricerca automatica:

- È necessario includere l'impostazione ADMIN_IP per almeno un nodo Grid su qualsiasi subnet a cui non è collegato direttamente il nodo Admin primario. Questo nodo della griglia pubblicherà quindi l'indirizzo IP del nodo di amministrazione primario per gli altri nodi della subnet da rilevare con mDNS.
- Assicurarsi che l'infrastruttura di rete supporti il passaggio del traffico IP multi-cast all'interno di una subnet.

File di configurazione del nodo di esempio

È possibile utilizzare i file di configurazione dei nodi di esempio per configurare i file di configurazione dei nodi per il sistema StorageGRID. Gli esempi mostrano i file di configurazione dei nodi per tutti i tipi di nodi griglia.

Per la maggior parte dei nodi, è possibile aggiungere le informazioni di indirizzamento di Admin e Client Network (IP, mask, gateway e così via) quando si configura la griglia utilizzando Grid Manager o l'API di installazione. L'eccezione è il nodo di amministrazione principale. Se si desidera accedere all'indirizzo IP Admin Network del nodo di amministrazione principale per completare la configurazione della griglia (ad esempio perché la rete di griglia non viene instradata), è necessario configurare la connessione Admin Network per il nodo di amministrazione primario nel relativo file di configurazione del nodo. Questo è illustrato nell'esempio.

> Negli esempi, la destinazione di rete client è stata configurata come Best practice, anche se la rete client è disattivata per impostazione predefinita.

Esempio per nodo amministratore primario

Nome file di esempio: `/etc/storagegrid/nodes/dc1-adm1.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Esempio per nodo di storage

Esempio di nome del file: `/etc/storagegrid/nodes/dc1-sn1.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Esempio per nodo di archivio

Esempio di nome del file: `/etc/storagegrid/nodes/dc1-arc1.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Esempio per Gateway Node

Esempio di nome del file: `/etc/storagegrid/nodes/dc1-gw1.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Esempio di nodo amministrativo non primario

Esempio di nome del file: `/etc/storagegrid/nodes/dc1-adm2.conf`

Esempio di contenuto del file:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Convalidare la configurazione StorageGRID

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

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

```
sudo storagegrid node validate all
```

Se i file sono corretti, l'output mostra **PASSED** per ciascun file di configurazione, come mostrato nell'esempio.

> Quando si utilizza un solo LUN sui nodi solo metadati, è possibile che venga visualizzato un messaggio di avviso che può essere ignorato.

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

Per un'installazione automatica, è possibile eliminare questo output utilizzando `-q` oppure `--quiet` in `storagegrid` command (ad esempio, `storagegrid --quiet…`). Se si elimina l'output, il comando avrà un valore di uscita diverso da zero se vengono rilevati avvisi o errori di configurazione.

Se i file di configurazione non sono corretti, i problemi vengono visualizzati come **WARNING** e **ERROR**, come mostrato nell'esempio. Se vengono rilevati errori di configurazione, è necessario correggerli prima di procedere con l'installazione.

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

Avviare il servizio host StorageGRID

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

Fasi

1. Eseguire i seguenti comandi su ciascun host:

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

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

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

3. Se un nodo restituisce lo stato "Not Running" (non in esecuzione) o "Stopped" (arrestato), eseguire il comando seguente:

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

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

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

Configurare la griglia e completare l'installazione (Ubuntu o Debian)

Accedere a Grid Manager

Il Gestore griglia consente di definire tutte le informazioni necessarie per configurare il sistema StorageGRID.

Prima di iniziare

Il nodo di amministrazione primario deve essere implementato e aver completato la sequenza di avvio iniziale.

Fasi

1. Aprire il browser Web e accedere a uno dei seguenti indirizzi:

   `https://primary_admin_node_ip`

   `client_network_ip`

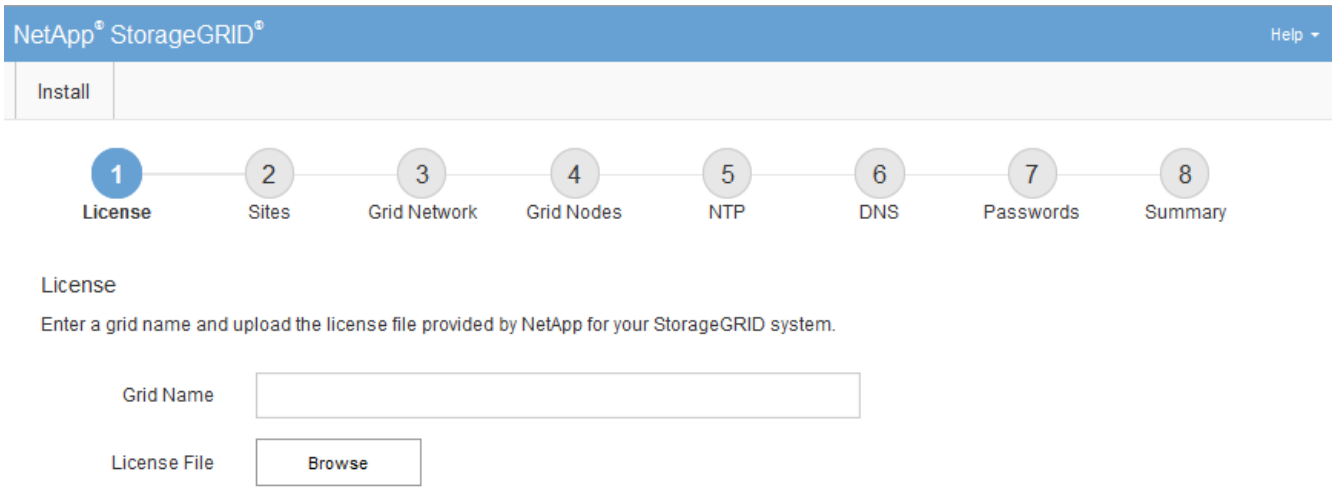
   In alternativa, è possibile accedere a Grid Manager dalla porta 8443:

   `https://primary_admin_node_ip:8443`

   > È possibile utilizzare l'indirizzo IP per l'indirizzo IP del nodo di amministrazione primario sulla rete griglia o sulla rete di amministrazione, a seconda della configurazione di rete.

2. Selezionare **Installa un sistema StorageGRID**.

   Viene visualizzata la pagina utilizzata per configurare un sistema StorageGRID.



Specificare le informazioni sulla licenza StorageGRID

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

Fasi

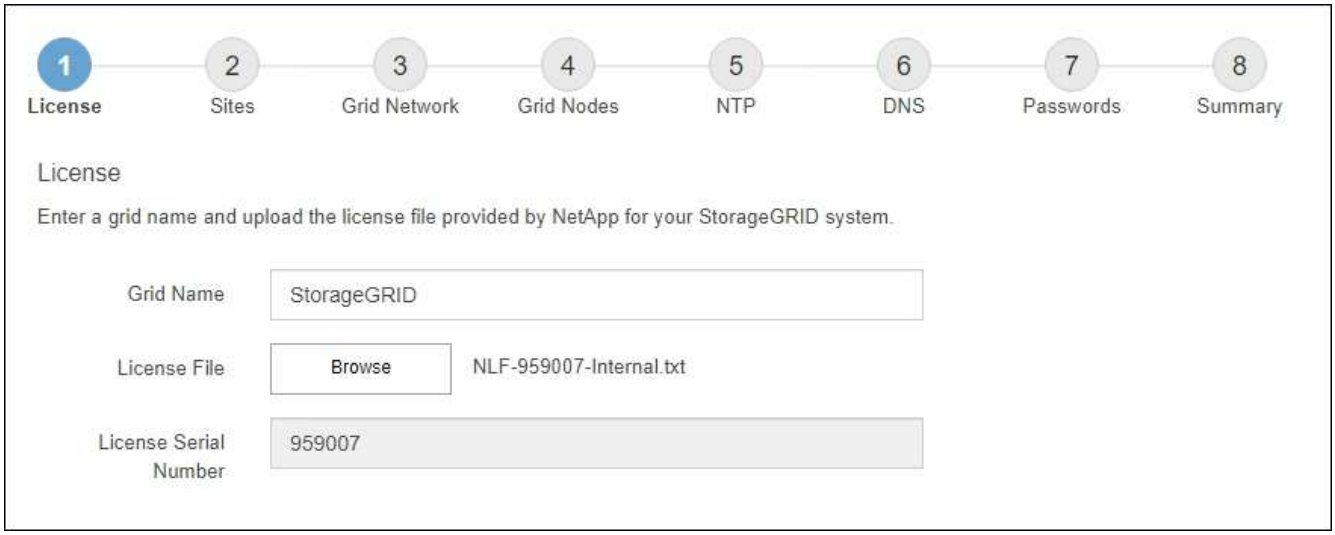
1. Nella pagina licenza, immettere un nome significativo per il sistema StorageGRID nel campo **Nome griglia**.

   Dopo l'installazione, il nome viene visualizzato nella parte superiore del menu Nodes (nodi).

2. Selezionare **Sfoglia**, individuare il file di licenza NetApp (`NLF-unique-id.txt`), quindi selezionare **Apri**.

   Il file di licenza viene validato e viene visualizzato il numero di serie.

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



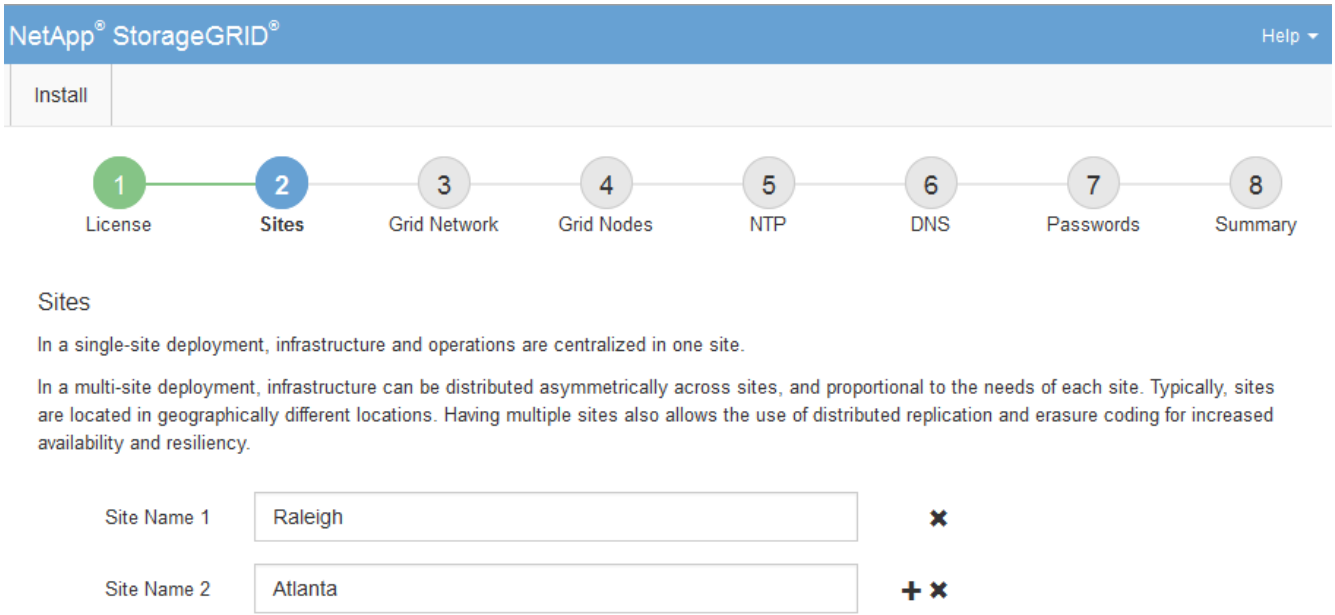
3. Selezionare **Avanti**.

Aggiungere siti

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

1. Nella pagina Siti, immettere il nome del sito *.
2. Per aggiungere altri siti, fare clic sul segno più accanto all'ultima voce del sito e inserire il nome nella nuova casella di testo **Nome sito**.

   Aggiungi tutti i siti aggiuntivi necessari per la topologia della griglia. È possibile aggiungere fino a 16 siti.



3. Fare clic su **Avanti**.

Specificare le subnet Grid Network

È necessario specificare le subnet utilizzate nella rete Grid.

A proposito di questa attività

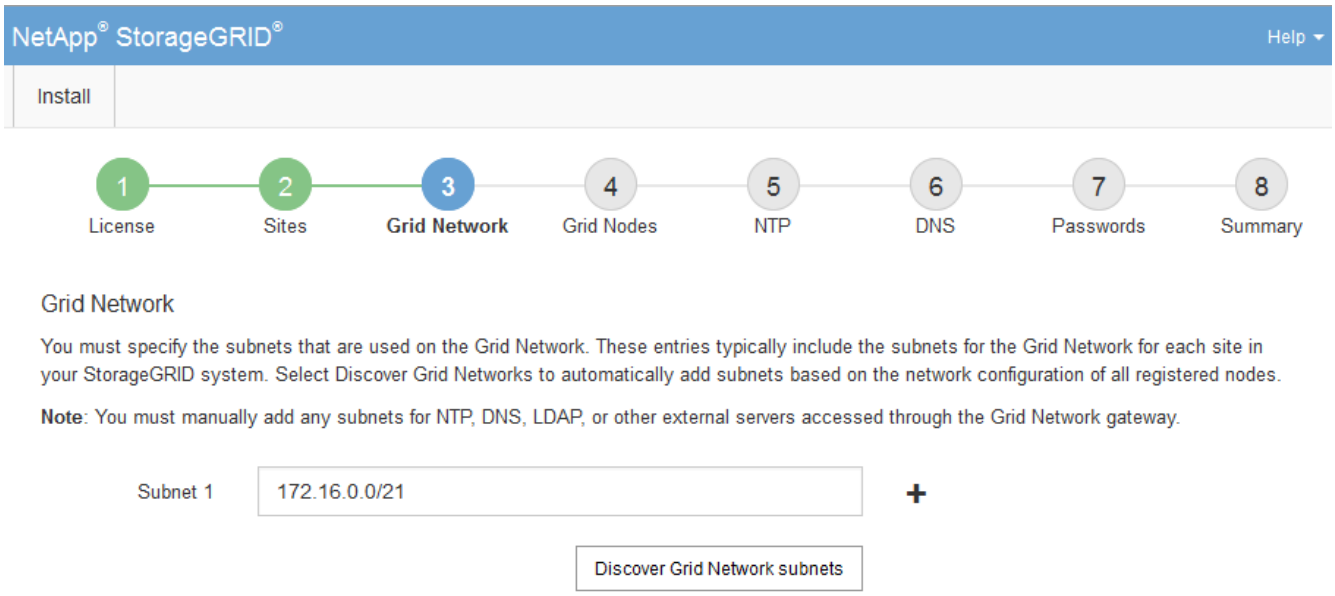
Le voci della subnet includono le subnet della rete di rete per ciascun sito del sistema StorageGRID, nonché le subnet che devono essere raggiungibili tramite la rete di rete.

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

Fasi

1. Specificare l'indirizzo di rete CIDR per almeno una rete griglia nella casella di testo **Subnet 1**.
2. Fare clic sul segno più accanto all'ultima voce per aggiungere una voce di rete aggiuntiva.

   Se è già stato implementato almeno un nodo, fare clic su **Discover Grid Networks Subnet** (rileva subnet Grid Network) per compilare automaticamente Grid Network Subnet List (elenco subnet Grid Network) con le subnet segnalate dai nodi Grid registrati con Grid Manager.



3. Fare clic su **Avanti**.

Approvare i nodi griglia in sospeso

È necessario approvare ciascun nodo della griglia prima che possa unirsi al sistema StorageGRID.

Prima di iniziare

Hai implementato tutti i nodi grid delle appliance virtuali e StorageGRID.

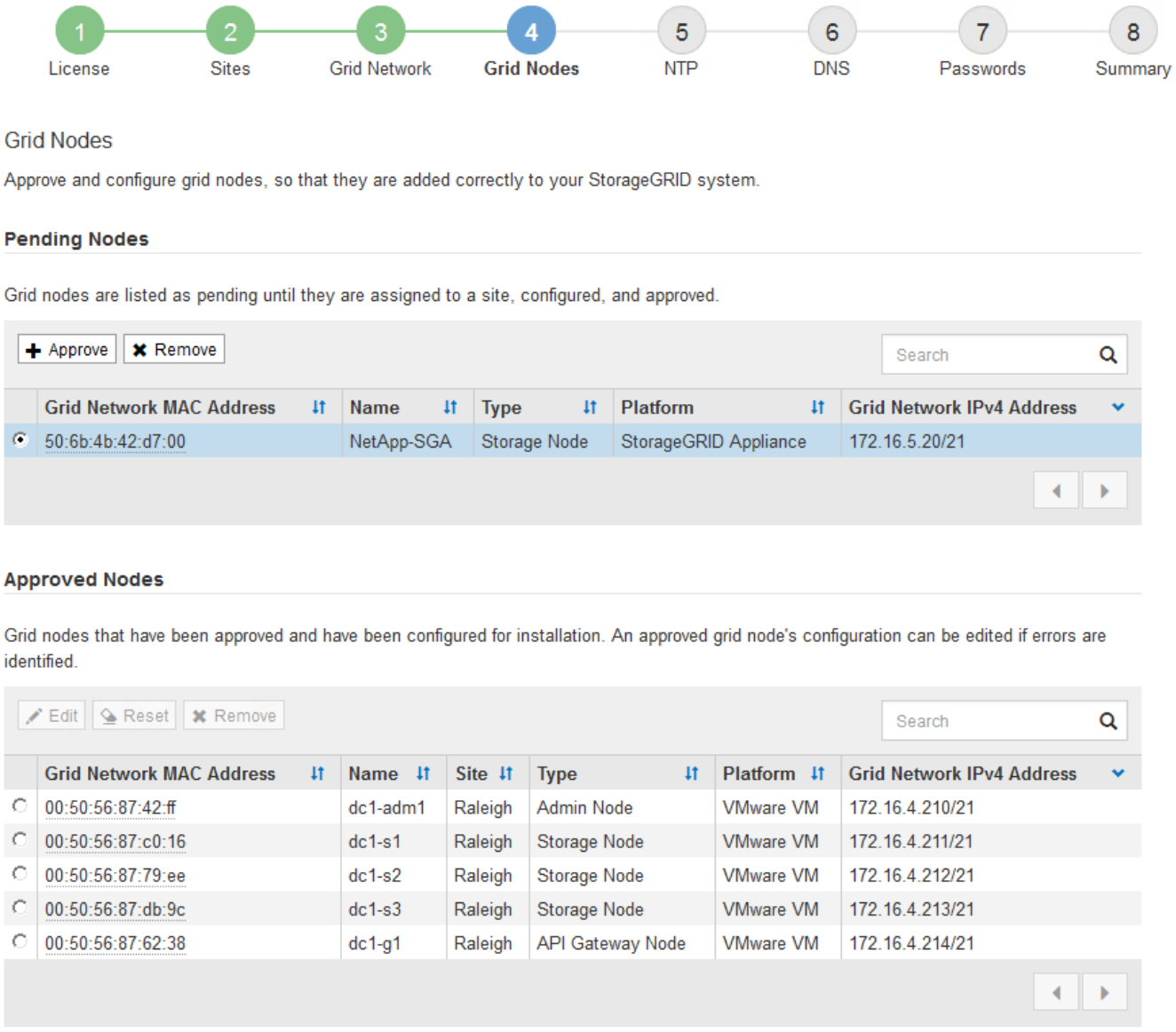
> È più efficiente eseguire una singola installazione di tutti i nodi, piuttosto che installare alcuni nodi ora e alcuni nodi successivamente.

Fasi

1. Esaminare l'elenco Pending Nodes (nodi in sospeso) e confermare che mostra tutti i nodi della griglia implementati.

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

2. Selezionare il pulsante di opzione accanto al nodo in sospeso che si desidera approvare.



3. Fare clic su **approva**.
4. In General Settings (Impostazioni generali), modificare le impostazioni per le seguenti proprietà, in base alle necessità:
   - **Sito**: Il nome di sistema del sito per questo nodo della griglia.
   - **Name**: Il nome del sistema per il nodo. Il nome predefinito corrisponde al nome specificato al momento della configurazione del nodo.

     I nomi di sistema sono necessari per le operazioni StorageGRID interne e non possono essere modificati dopo aver completato l'installazione. Tuttavia, durante questa fase del processo di installazione, è possibile modificare i nomi di sistema in base alle esigenze.

   - **Ruolo NTP**: Ruolo NTP (Network Time Protocol) del nodo Grid. Le opzioni disponibili sono **automatico**, **primario** e **Client**. Selezionando **automatico**, il ruolo primario viene assegnato ai nodi di amministrazione, ai nodi di storage con servizi ADC, ai nodi gateway e a tutti i nodi di griglia che hanno indirizzi IP non statici. A tutti gli altri nodi della griglia viene assegnato il ruolo Client.

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

- **Tipo di archiviazione** (solo nodi di archiviazione): Specificare che un nuovo nodo di archiviazione deve essere utilizzato esclusivamente per i metadati. Le opzioni sono **oggetti e metadati** e **solo metadati**. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

  Quando si installa un grid con nodi solo metadati, il grid deve anche contenere un numero minimo di nodi per lo storage a oggetti. Per un grid a sito singolo, vengono configurati almeno due nodi storage per oggetti e metadati. Per un grid multisito, per gli oggetti e i metadati viene configurato almeno un nodo di storage per sito.

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

5. In Grid Network, modificare le impostazioni per le seguenti proprietà secondo necessità:

   - **IPv4 Address (CIDR)**: L'indirizzo di rete CIDR per l'interfaccia Grid Network (eth0 all'interno del container). Ad esempio: 192.168.1.234/21
   - **Gateway**: Il gateway Grid Network. Ad esempio: 192.168.0.1

     Il gateway è necessario se sono presenti più subnet di rete.

   Se si seleziona DHCP per la configurazione Grid Network e si modifica il valore, il nuovo valore verrà configurato come indirizzo statico sul nodo. Assicurarsi che l'indirizzo IP risultante non si trovi all'interno di un pool di indirizzi DHCP.

6. Se si desidera configurare la rete amministrativa per il nodo della griglia, aggiungere o aggiornare le impostazioni nella sezione rete amministrativa secondo necessità.

   Inserire le subnet di destinazione dei percorsi fuori da questa interfaccia nella casella di testo **subnet (CIDR)**. Se sono presenti più subnet Admin, è necessario il gateway Admin.

   Se si seleziona DHCP per la configurazione Admin Network e si modifica il valore, il nuovo valore verrà configurato come indirizzo statico sul nodo. Assicurarsi che l'indirizzo IP risultante non si trovi all'interno di un pool di indirizzi DHCP.

   Appliance: per un'appliance StorageGRID, se la rete amministrativa non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione dell'appliance StorageGRID, non è possibile configurarla in questa finestra di dialogo. È invece necessario attenersi alla seguente procedura:

   a. Riavviare l'appliance: Nel programma di installazione dell'appliance, selezionare **Avanzate** > **Riavvia**.

      Il riavvio può richiedere alcuni minuti.

   b. Selezionare **Configure Networking** > **link Configuration** (Configura rete) e abilitare le reti appropriate.

c. Selezionare **Configura rete** > **Configurazione IP** e configurare le reti abilitate.

d. Tornare alla Home page e fare clic su **Avvia installazione**.

e. In Grid Manager: Se il nodo è elencato nella tabella Approved Nodes (nodi approvati), rimuoverlo.

f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).

g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).

h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP del programma di installazione dell'appliance.

   Per ulteriori informazioni, consultare "Avvio rapido per l'installazione dell'hardware" per individuare le istruzioni relative all'apparecchio.

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

   > Se si seleziona DHCP per la configurazione di rete client e si modifica il valore, il nuovo valore verrà configurato come indirizzo statico sul nodo. Assicurarsi che l'indirizzo IP risultante non si trovi all'interno di un pool di indirizzi DHCP.

   Appliance: per un'appliance StorageGRID, se la rete client non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione dell'appliance StorageGRID, non è possibile configurarla in questa finestra di dialogo. È invece necessario attenersi alla seguente procedura:

   a. Riavviare l'appliance: Nel programma di installazione dell'appliance, selezionare **Avanzate** > **Riavvia**.

      Il riavvio può richiedere alcuni minuti.

   b. Selezionare **Configure Networking** > **link Configuration** (Configura rete) e abilitare le reti appropriate.

   c. Selezionare **Configura rete** > **Configurazione IP** e configurare le reti abilitate.

   d. Tornare alla Home page e fare clic su **Avvia installazione**.

   e. In Grid Manager: Se il nodo è elencato nella tabella Approved Nodes (nodi approvati), rimuoverlo.

   f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).

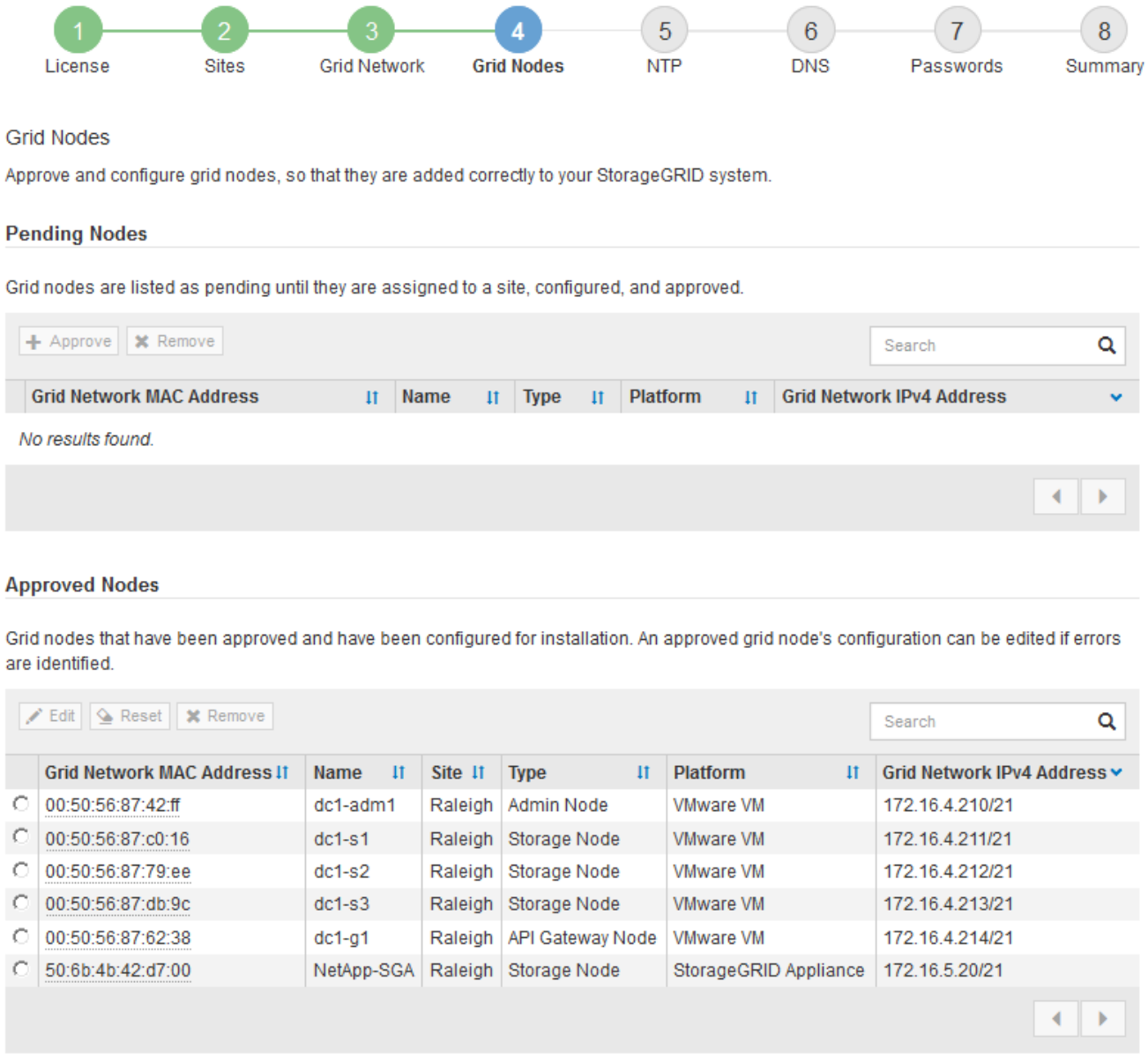
   g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).

   h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP del programma di installazione dell'appliance.

      Per informazioni su come installare le appliance StorageGRID, consultare "Avvio rapido per l'installazione dell'hardware" per individuare le istruzioni relative all'apparecchio.

8. Fare clic su **Save** (Salva).

   La voce del nodo della griglia viene spostata nell'elenco dei nodi approvati.



9. Ripetere questi passaggi per ogni nodo griglia in sospeso che si desidera approvare.

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

10. Una volta completata l'approvazione dei nodi griglia, fare clic su **Avanti**.

Specificare le informazioni sul server Network Time Protocol

È necessario specificare le informazioni di configurazione del protocollo NTP (Network Time Protocol) per il sistema StorageGRID, in modo che le operazioni eseguite su server separati possano essere mantenute sincronizzate.

A proposito di questa attività

Specificare gli indirizzi IPv4 per i server NTP.

Specificare server NTP esterni. I server NTP specificati devono utilizzare il protocollo NTP.

È necessario specificare quattro riferimenti al server NTP di strato 3 o superiore per evitare problemi con la deriva del tempo.

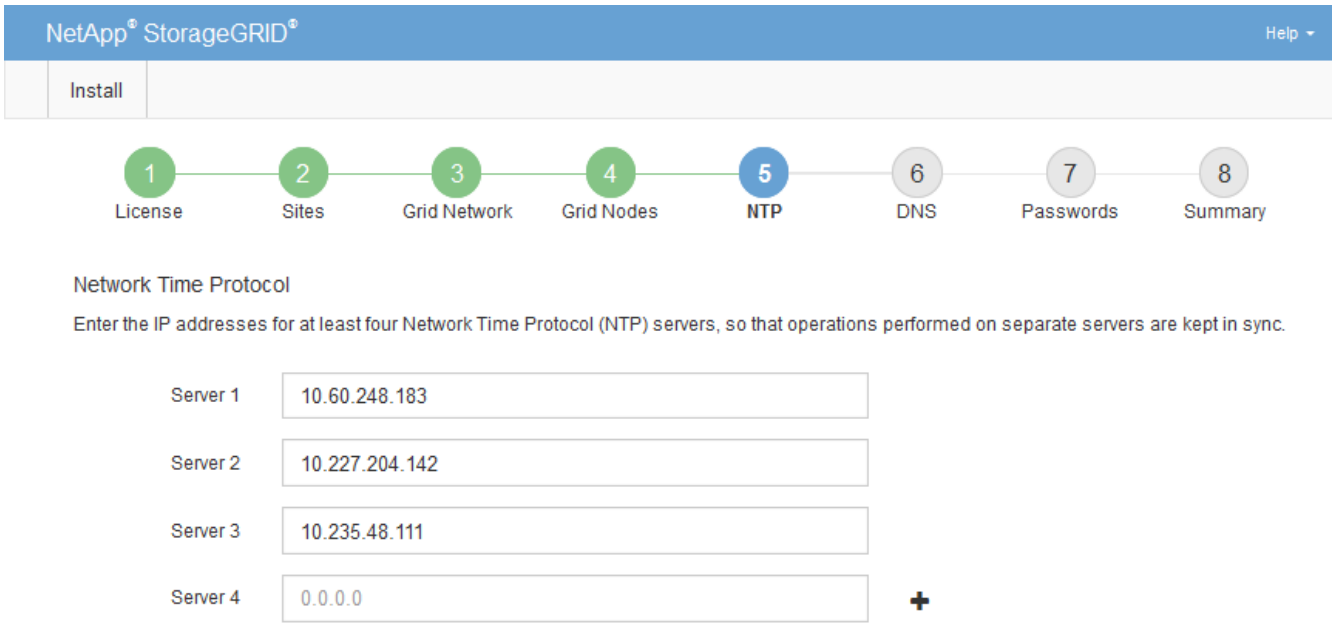
> Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Windows Time (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Time sulle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'utilizzo in ambienti ad alta precisione, come StorageGRID.
>
> "Supportare il limite per configurare il servizio Time di Windows per ambienti ad alta precisione"

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

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

Fasi

1. Specificare gli indirizzi IPv4 per almeno quattro server NTP nelle caselle di testo da **Server 1** a **Server 4**.
2. Se necessario, selezionare il segno più accanto all'ultima voce per aggiungere altre voci del server.



3. Selezionare **Avanti**.

Informazioni correlate

"Linee guida per il networking"

Specificare le informazioni sul server DNS

È necessario specificare le informazioni DNS per il sistema StorageGRID, in modo da

poter accedere ai server esterni utilizzando i nomi host anziché gli indirizzi IP.

A proposito di questa attività

Specificare "Informazioni sul server DNS" Consente di utilizzare nomi host FQDN (Fully Qualified Domain Name) piuttosto che indirizzi IP per le notifiche e-mail e AutoSupport.

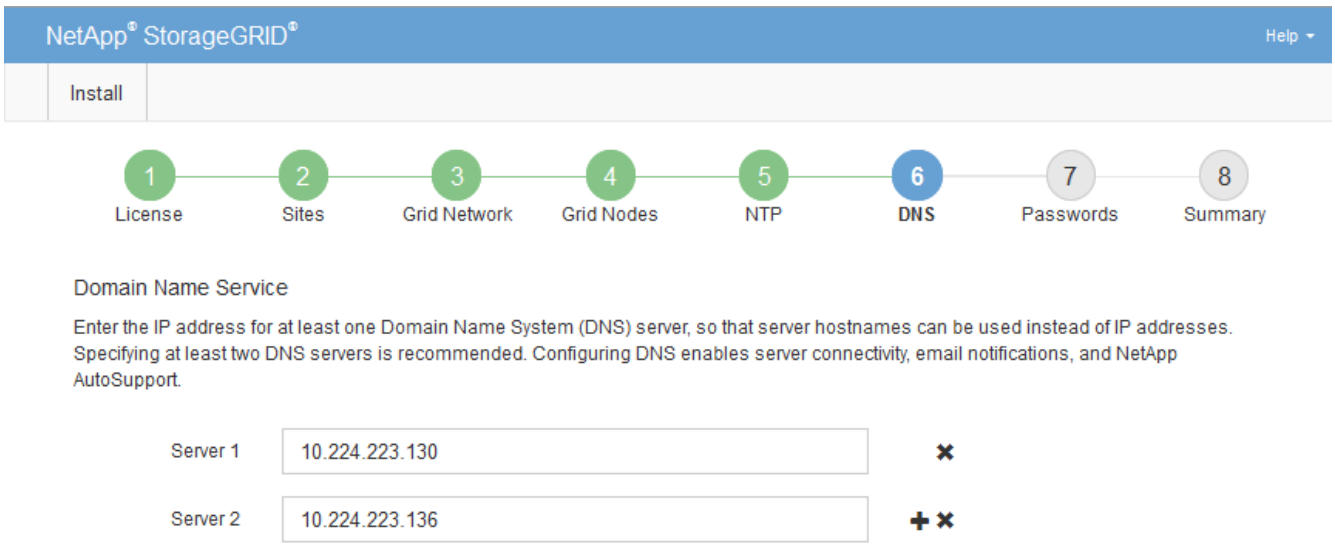
Per garantire il corretto funzionamento, specificare due o tre server DNS. Se si specificano più di tre, è possibile che ne vengano utilizzati solo tre a causa delle limitazioni del sistema operativo note su alcune piattaforme. Se nel proprio ambiente sono presenti restrizioni di routing, è possibile "Personalizzare l'elenco dei server DNS" Per i singoli nodi (in genere tutti i nodi di un sito) di utilizzare un set diverso di un massimo di tre server DNS.

Se possibile, utilizzare i server DNS a cui ciascun sito può accedere localmente per garantire che un sito islanded possa risolvere i FQDN per le destinazioni esterne.

Se le informazioni del server DNS vengono omesse o configurate in modo errato, viene attivato un allarme DNST sul servizio SSM di ciascun nodo della rete. L'allarme viene cancellato quando il DNS è configurato correttamente e le nuove informazioni sul server hanno raggiunto tutti i nodi della griglia.

Fasi

1. Specificare l'indirizzo IPv4 per almeno un server DNS nella casella di testo **Server 1**.
2. Se necessario, selezionare il segno più accanto all'ultima voce per aggiungere altre voci del server.



   Si consiglia di specificare almeno due server DNS. È possibile specificare fino a sei server DNS.

3. Selezionare **Avanti**.

Specificare le password di sistema di StorageGRID

Durante l'installazione del sistema StorageGRID, è necessario inserire le password da utilizzare per proteggere il sistema ed eseguire attività di manutenzione.

A proposito di questa attività

Utilizzare la pagina Installa password per specificare la passphrase di provisioning e la password utente root di gestione della griglia.

- La passphrase di provisioning viene utilizzata come chiave di crittografia e non viene memorizzata dal sistema StorageGRID.
- È necessario disporre della passphrase di provisioning per le procedure di installazione, espansione e manutenzione, incluso il download del pacchetto di ripristino. Pertanto, è importante memorizzare la passphrase di provisioning in una posizione sicura.
- È possibile modificare la passphrase di provisioning da Grid Manager, se si dispone di quella corrente.
- La password utente root della gestione della griglia può essere modificata utilizzando Grid Manager.
- Le password SSH e la console della riga di comando generate in modo casuale vengono memorizzate in `Passwords.txt` Nel pacchetto di ripristino.

Fasi

1. In **Provisioning Passphrase**, immettere la passphase di provisioning necessaria per apportare modifiche alla topologia grid del sistema StorageGRID.

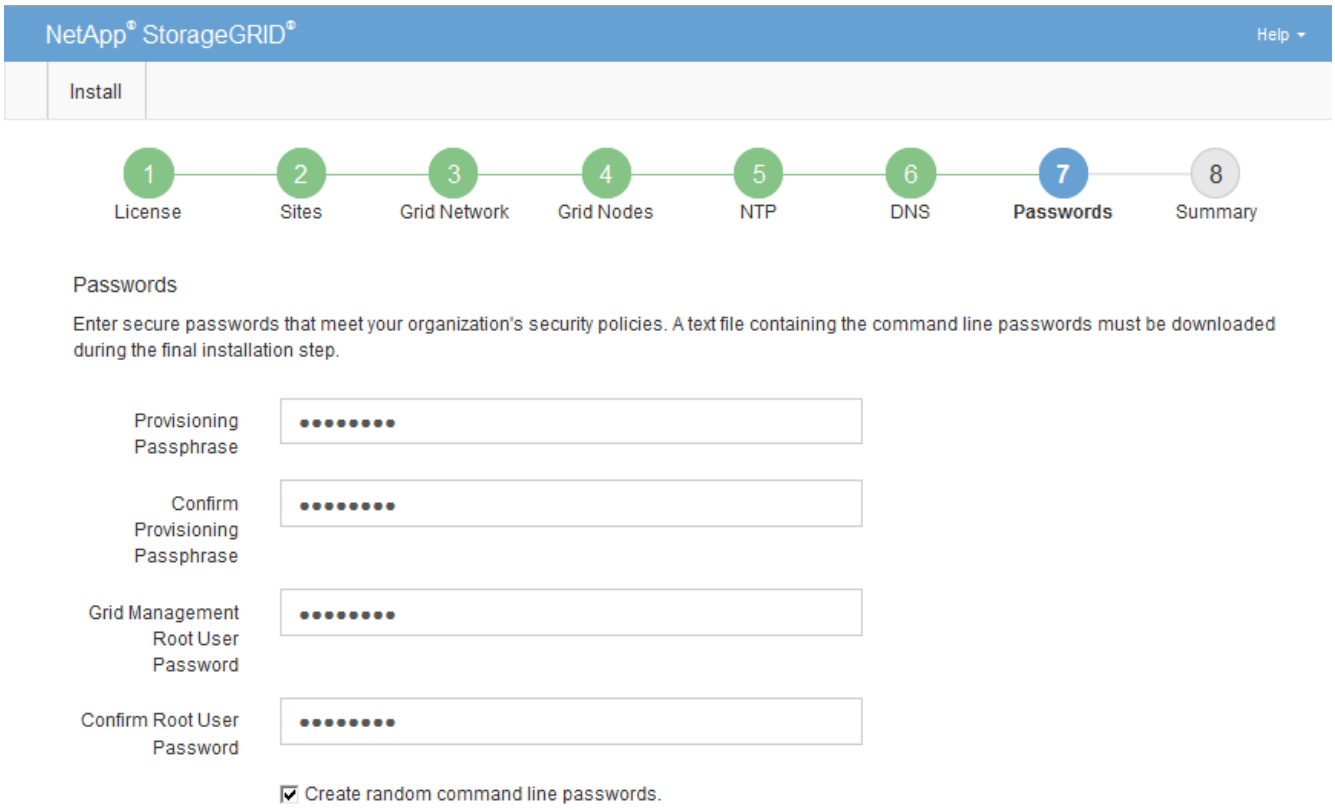
   Memorizzare la passphrase di provisioning in un luogo sicuro.

   > Se, al termine dell'installazione, si desidera modificare la passphrase di provisioning in un secondo momento, è possibile utilizzare Grid Manager. Selezionare **CONFIGURATION** > **Access control**> **Grid passwords**.

2. In **Confirm Provisioning Passphrase** (Conferma password di provisioning), immettere nuovamente la passphrase di provisioning per confermarla.
3. In **Grid Management Root User Password**, immettere la password da utilizzare per accedere al Grid Manager come utente "root".

   Memorizzare la password in un luogo sicuro.

4. In **Confirm Root User Password** (Conferma password utente root), immettere nuovamente la password di Grid Manager per confermarla.



5. Se si sta installando una griglia a scopo dimostrativo o dimostrativo, deselezionare la casella di controllo **Create random command line passwords** (Crea password della riga di comando casuale).

   Per le implementazioni in produzione, le password casuali devono essere sempre utilizzate per motivi di sicurezza. Cancella **Crea password casuali della riga di comando** solo per le griglie demo se desideri utilizzare password predefinite per accedere ai nodi della griglia dalla riga di comando utilizzando l'account "root" o "admin".

   > Viene richiesto di scaricare il file del pacchetto di ripristino (`sgws-recovery-package-id-revision.zip`) Dopo aver fatto clic su **Install** (Installa) nella pagina Summary (Riepilogo). È necessario "scarica questo file" per completare l'installazione. Le password richieste per accedere al sistema vengono memorizzate in `Passwords.txt` File, contenuto nel file del pacchetto di ripristino.

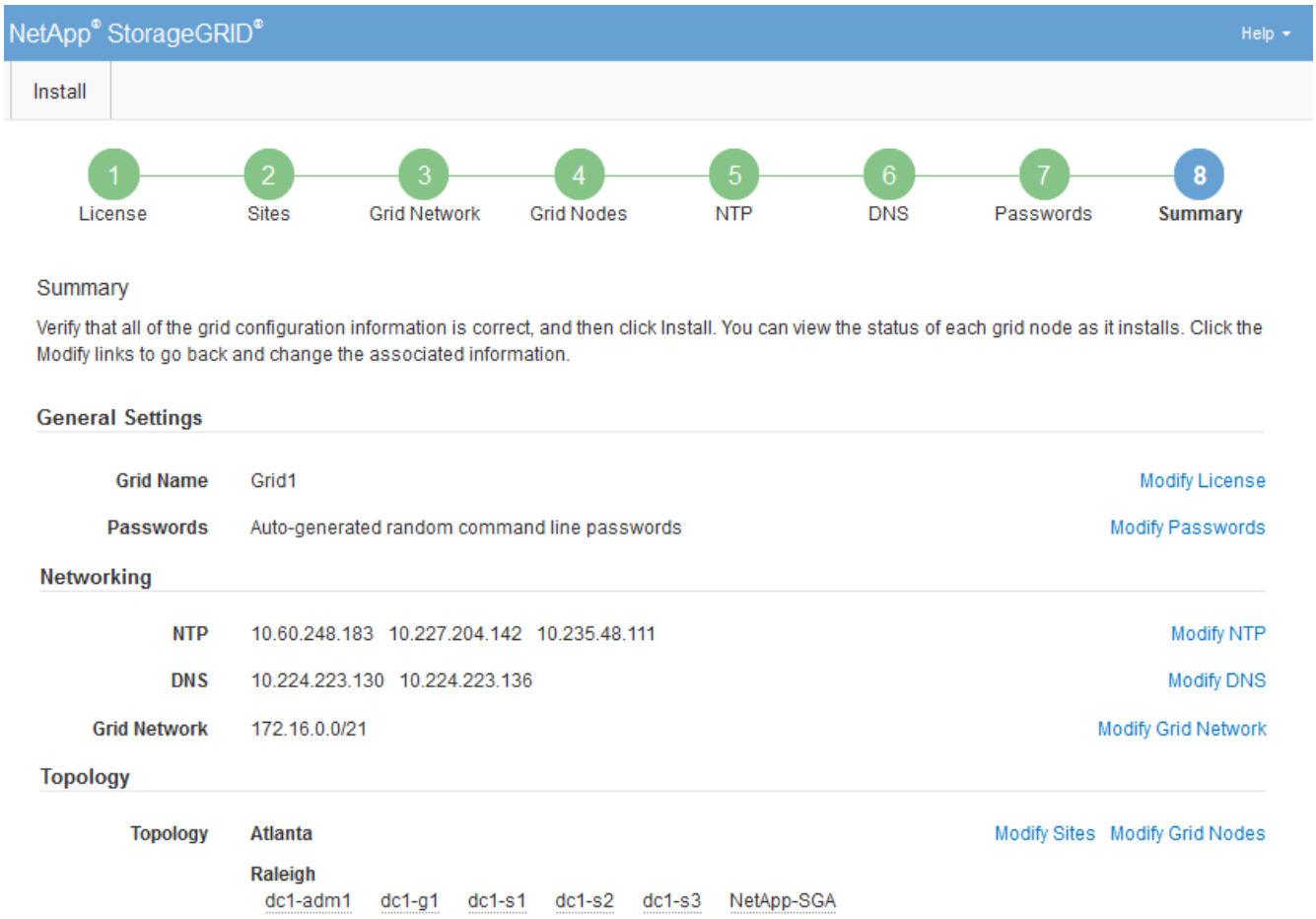
6. Fare clic su **Avanti**.

Esaminare la configurazione e completare l'installazione

È necessario esaminare attentamente le informazioni di configurazione inserite per assicurarsi che l'installazione venga completata correttamente.

Fasi

1. Visualizza la pagina **Riepilogo**.



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

> Se un nodo è configurato per utilizzare la rete client, il gateway predefinito per quel nodo passa dalla rete griglia alla rete client quando si fa clic su **Installa**. In caso di perdita della connettività, assicurarsi di accedere al nodo di amministrazione primario tramite una subnet accessibile. Vedere "Linee guida per il networking" per ulteriori informazioni.

4. Fare clic su **Download Recovery Package**.

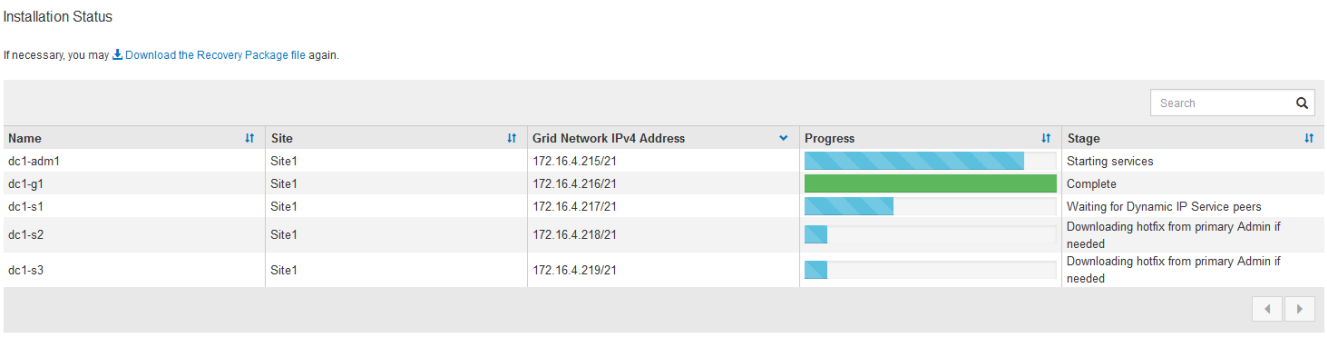
   Quando l'installazione prosegue fino al punto in cui è definita la topologia della griglia, viene richiesto di scaricare il file del pacchetto di ripristino (`.zip`) e confermare che sia possibile accedere al contenuto del file. È necessario scaricare il file del pacchetto di ripristino in modo da poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi griglia. L'installazione continua in background, ma non è possibile completare l'installazione e accedere al sistema StorageGRID fino a quando non si scarica e si verifica questo file.

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

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

6. Selezionare la casella di controllo **ho scaricato e verificato il file del pacchetto di ripristino** e fare clic su **Avanti**.

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



   Una volta raggiunta la fase completa per tutti i nodi della griglia, viene visualizzata la pagina di accesso per Grid Manager.

7. Accedere a Grid Manager utilizzando l'utente "root" e la password specificata durante l'installazione.

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. Impossibile 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.

Panoramica dell'API REST per l'installazione

StorageGRID fornisce l'API di installazione di StorageGRID per eseguire le attività di installazione.

L'API utilizza la piattaforma API open source Swagger per fornire la documentazione API. Swagger consente agli sviluppatori e ai non sviluppatori di interagire con l'API in un'interfaccia utente che illustra il modo in cui l'API risponde a parametri e opzioni. La presente documentazione presuppone che l'utente abbia familiarità con le tecnologie Web standard e il formato dati JSON.

Tutte le operazioni API eseguite utilizzando la pagina web API Docs sono operazioni live. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Ogni comando REST API include l'URL dell'API, un'azione HTTP, qualsiasi parametro URL richiesto o opzionale e una risposta API prevista.

API di installazione StorageGRID

L'API di installazione di StorageGRID è disponibile solo quando si configura inizialmente il sistema StorageGRID e se è necessario eseguire un ripristino primario del nodo di amministrazione. È possibile accedere all'API di installazione tramite HTTPS da Grid Manager.

Per accedere alla documentazione API, accedere alla pagina Web di installazione nel nodo di amministrazione principale e selezionare **Guida** > **documentazione API** dalla barra dei menu.

L'API di installazione di StorageGRID include le seguenti sezioni:

- **Config** — operazioni relative alla release del prodotto e alle versioni dell'API. È possibile elencare la versione di release del prodotto e le principali versioni dell'API supportate da tale release.
- **Grid** — operazioni di configurazione a livello di griglia. È possibile ottenere e aggiornare le impostazioni della griglia, inclusi i dettagli della griglia, le subnet Grid Network, le password della griglia e gli indirizzi IP dei server NTP e DNS.
- **Nodi** — operazioni di configurazione a livello di nodo. È possibile recuperare un elenco di nodi griglia, eliminare un nodo griglia, configurare un nodo griglia, visualizzare un nodo griglia e ripristinare la configurazione di un nodo griglia.
- **Provision** — operazioni di provisioning. È possibile avviare l'operazione di provisioning e visualizzare lo stato dell'operazione di provisioning.
- **Recovery** — operazioni di recovery del nodo di amministrazione principale. È possibile ripristinare le informazioni, caricare il pacchetto di ripristino, avviare il ripristino e visualizzare lo stato dell'operazione di ripristino.
- **Recovery-package** — operazioni per scaricare il pacchetto di ripristino.
- **Schemi** — schemi API per implementazioni avanzate
- **Siti** — operazioni di configurazione a livello di sito. È possibile creare, visualizzare, eliminare e modificare un sito.

Informazioni correlate

"Automazione dell'installazione"

Dove andare

Dopo aver completato un'installazione, eseguire le attività di integrazione e configurazione richieste. È possibile eseguire le attività opzionali in base alle necessità.

Attività richieste

- "Creare un account tenant" Per ogni protocollo client (Swift o S3) che verrà utilizzato per memorizzare gli oggetti nel sistema StorageGRID.
- "Controllare l'accesso al sistema" configurando gruppi e account utente. Se lo si desidera, è possibile "configurare un'origine di identità federata" (Ad esempio Active Directory o OpenLDAP), in modo da poter

importare utenti e gruppi di amministrazione. In alternativa, è possibile "creare utenti e gruppi locali".

- Integrare e testare "API S3" oppure "API Swift" Applicazioni client che verranno utilizzate per caricare oggetti nel sistema StorageGRID.
- "Configurare le regole ILM (Information Lifecycle Management) e i criteri ILM" da utilizzare per proteggere i dati degli oggetti.
- Se l'installazione include nodi di storage dell'appliance, utilizzare SANtricity OS per completare le seguenti operazioni:
  - Connessione a ogni appliance StorageGRID.
  - Verificare la ricezione dei dati AutoSupport.

  Vedere "Configurare l'hardware".
- Esaminare e seguire "Linee guida per la protezione avanzata del sistema StorageGRID" eliminare i rischi per la sicurezza.
- "Configurare le notifiche e-mail per gli avvisi di sistema".
- Se il sistema StorageGRID include nodi di archiviazione (non più presenti), configurare la connessione del nodo di archiviazione al sistema di archiviazione esterno di destinazione.

Attività facoltative

- "Aggiornare gli indirizzi IP del nodo griglia" Se sono state modificate dopo la pianificazione dell'implementazione e la generazione del pacchetto di ripristino.
- "Configurare la crittografia dello storage", se necessario.
- "Configurare la compressione dello storage" ridurre le dimensioni degli oggetti memorizzati, se necessario.

Risolvere i problemi di installazione

Se si verificano problemi durante l'installazione del sistema StorageGRID, è possibile accedere ai file di log dell'installazione. Per risolvere i problemi, potrebbe essere necessario utilizzare anche i file di log dell'installazione.

I seguenti file di log per l'installazione sono disponibili dal container che esegue ciascun nodo:

- `/var/local/log/install.log` (trovato su tutti i nodi della griglia)
- `/var/local/log/gdu-server.log` (Trovato sul nodo di amministrazione primario)

I seguenti file di log per l'installazione sono disponibili dall'host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/<node-name>.log`

Per informazioni su come accedere ai file di registro, vedere "Raccogliere i file di log e i dati di sistema".

Informazioni correlate

"Risolvere i problemi di un sistema StorageGRID"

Esempio di /etc/network/interfaces

Il `/etc/network/interfaces` Il file include tre sezioni, che definiscono le interfacce fisiche, l'interfaccia bond e le interfacce VLAN. È possibile combinare le tre sezioni di esempio in un singolo file, che aggrega quattro interfacce fisiche Linux in un singolo collegamento LACP e quindi stabilisce tre interfacce VLAN che sottintende il collegamento per l'utilizzo come interfacce di rete StorageGRID, amministratore e client.

Interfacce fisiche

Si noti che gli switch alle altre estremità dei collegamenti devono anche considerare le quattro porte come un singolo trunk LACP o canale di porta e devono passare almeno le tre VLAN a cui si fa riferimento con tag.

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Interfaccia bond

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

Interfacce VLAN

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

Installare StorageGRID su VMware

Guida rapida per l'installazione di StorageGRID su VMware

Seguire questi passaggi di alto livello per installare un nodo VMware StorageGRID.

1 **Preparazione**

- Scopri di più "Architettura StorageGRID e topologia di rete".
- Scopri le specifiche di "Networking StorageGRID".
- Raccogliere e preparare il "Informazioni e materiali richiesti".
- Installare e configurare "Hypervisor di VMware vSphere, vCenter e host ESX".
- Preparare il necessario "CPU e RAM".
- Prevedere "requisiti di storage e performance".

2 **Implementazione**

Implementare i nodi grid. Quando si implementano nodi grid, questi vengono creati come parte del sistema

StorageGRID e connessi a una o più reti.

- Utilizzare il client Web VMware vSphere, un file .vmdk e un set di modelli di file .ovf su "Implementa i nodi basati su software come macchine virtuali (VM)" sui server preparati nel passaggio 1.
- Per implementare i nodi di appliance StorageGRID, segui la procedura "Avvio rapido per l'installazione dell'hardware".

3 **Configurazione**

Una volta distribuiti tutti i nodi, utilizzare il Grid Manager per "configurare la griglia e completare l'installazione".

Automatizzare l'installazione

Per risparmiare tempo e garantire coerenza, è possibile automatizzare l'implementazione e la configurazione dei nodi grid e la configurazione del sistema StorageGRID.

- "Automatizza l'implementazione dei nodi con VMware vSphere".
- Dopo aver distribuito i nodi grid, "Automatizzare la configurazione del sistema StorageGRID" Utilizzo dello script di configurazione Python fornito nell'archivio di installazione.
- "Automatizzare l'installazione e la configurazione dei nodi grid delle appliance"
- Se si è uno sviluppatore avanzato di implementazioni StorageGRID, automatizzare l'installazione dei nodi grid utilizzando "API REST di installazione".

Pianificare e preparare l'installazione su VMware

Informazioni e materiali richiesti

Prima di installare StorageGRID, raccogliere e preparare le informazioni e il materiale necessari.

Informazioni richieste

Piano di rete

Quali reti intendi collegare a ogni nodo StorageGRID? StorageGRID supporta più reti per la separazione del traffico, la sicurezza e la convenienza amministrativa.

Vedere StorageGRID "Linee guida per il networking".

Informazioni di rete

A meno che non si utilizzi DHCP, gli indirizzi IP da assegnare a ciascun nodo della griglia e gli indirizzi IP dei server DNS e NTP.

Server per i nodi grid

Identificare un insieme di server (fisici, virtuali o entrambi) che, in aggregato, forniscono risorse sufficienti per supportare il numero e il tipo di nodi StorageGRID che si intende implementare.

> Se l'installazione di StorageGRID non utilizza nodi di storage (hardware) dell'appliance StorageGRID, è necessario utilizzare lo storage RAID hardware con cache di scrittura supportata dalla batteria (BBWC). StorageGRID non supporta l'utilizzo di reti VSAN (Virtual Storage Area Network), RAID software o nessuna protezione RAID.

Migrazione dei nodi (se necessaria)

Comprendere "requisiti per la migrazione dei nodi", se si desidera eseguire la manutenzione pianificata sugli host fisici senza alcuna interruzione del servizio.

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Materiali richiesti

Licenza NetApp StorageGRID

È necessario disporre di una licenza NetApp valida con firma digitale.

> Nell'archivio di installazione di StorageGRID è inclusa una licenza non di produzione, che può essere utilizzata per test e griglie di prova.

Archivio di installazione di StorageGRID

"Scaricare l'archivio di installazione di StorageGRID ed estrarre i file".

Laptop di assistenza

Il sistema StorageGRID viene installato tramite un laptop di assistenza.

Il laptop di assistenza deve disporre di:

- Porta di rete
- Client SSH (ad esempio, putty)
- "Browser Web supportato"

Documentazione StorageGRID

- "Note di rilascio"
- "Istruzioni per l'amministrazione di StorageGRID"

Scaricare ed estrarre i file di installazione di StorageGRID

È necessario scaricare gli archivi di installazione di StorageGRID ed estrarre i file.

Fasi

1. Accedere alla "Pagina dei download NetApp per StorageGRID".
2. Selezionare il pulsante per scaricare l'ultima versione oppure selezionare un'altra versione dal menu a discesa e selezionare **Go**.
3. Accedi con il nome utente e la password del tuo account NetApp.
4. Se viene visualizzata un'istruzione Caution/MustRead, leggerla e selezionare la casella di controllo.

> Dopo aver installato la release di StorageGRID, è necessario applicare le correzioni rapide richieste. Per ulteriori informazioni, consultare "procedura di hotfix nelle istruzioni di ripristino e manutenzione"

5. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).

6. Nella colonna **Installa StorageGRID**, selezionare il file .tgz o .zip per VMware.

   Utilizzare `.zip` File se si esegue Windows sul laptop di assistenza.

7. Salvare ed estrarre il file di archivio.
8. Scegliere i file desiderati dal seguente elenco.

   I file necessari dipendono dalla topologia di griglia pianificata e dal modo in cui verrà implementato il sistema StorageGRID.

   I percorsi elencati nella tabella sono relativi alla directory di primo livello installata dall'archivio di installazione estratto.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid.
	Il file di modello Open Virtualization Format (`.ovf`) e il file manifest (`.mf`) Per l'implementazione del nodo di amministrazione primario.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi amministrativi non primari.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi di archiviazione.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi gateway.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi di storage basati su macchine virtuali.
Tool di scripting per la distribuzione	Descrizione
	Uno script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.

Percorso e nome del file	Descrizione
	Un file di configurazione di esempio da utilizzare con `deploy-vsphere-ovftool.sh` script.
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando è attivato il Single Sign-on (SSO). È anche possibile utilizzare questo script per il ping federate.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Script di supporto chiamato dal compagno `storagegrid-ssoauth-azure.py` Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

Requisiti software per VMware

È possibile utilizzare una macchina virtuale per ospitare qualsiasi tipo di nodo StorageGRID. È necessaria una macchina virtuale per ogni nodo di griglia.

Hypervisor VMware vSphere

È necessario installare VMware vSphere Hypervisor su un server fisico preparato. L'hardware deve essere configurato correttamente (incluse le versioni del firmware e le impostazioni del BIOS) prima di installare il

software VMware.

- Configurare il collegamento in rete nell'hypervisor in base alle esigenze per supportare il collegamento in rete per il sistema StorageGRID che si sta installando.

  "Linee guida per il networking"

- Assicurarsi che l'archivio dati sia sufficientemente grande per le macchine virtuali e i dischi virtuali necessari per ospitare i nodi della griglia.
- Se si crea più di un datastore, assegnare un nome a ciascun datastore in modo da identificare facilmente quale datastore utilizzare per ciascun nodo della griglia quando si creano macchine virtuali.

Requisiti di configurazione dell'host ESX

È necessario configurare correttamente il protocollo NTP (Network Time Protocol) su ciascun host ESX. Se il tempo dell'host non è corretto, potrebbero verificarsi effetti negativi, inclusa la perdita di dati.

Requisiti di configurazione di VMware

È necessario installare e configurare VMware vSphere e vCenter prima di implementare i nodi StorageGRID.

Per le versioni supportate del software VMware vSphere Hypervisor e VMware vCenter Server, consultare la "Tool di matrice di interoperabilità NetApp".

Per informazioni sui passaggi necessari per l'installazione di questi prodotti VMware, consultare la documentazione VMware.

Altro software richiesto

Per installare StorageGRID su VMware, è necessario installare alcuni pacchetti software di terze parti. Alcune distribuzioni Linux supportate non contengono questi pacchetti per impostazione predefinita. Le versioni dei pacchetti software su cui vengono testate le installazioni di StorageGRID includono quelle elencate in questa pagina.

Se si seleziona un'opzione di installazione runtime di distribuzione Linux e contenitore che richiede uno qualsiasi di questi pacchetti e questi non vengono installati automaticamente dalla distribuzione Linux, installare una delle versioni elencate qui se disponibile presso il provider o il fornitore di supporto per la distribuzione Linux. In caso contrario, utilizzare le versioni predefinite dei pacchetti disponibili presso il fornitore.

Tutte le opzioni di installazione richiedono Podman o Docker. Non installare entrambi i pacchetti. Installare solo il pacchetto richiesto dall'opzione di installazione.

Versioni Python testate

- 3,5.2-2
- 3,6.8-2
- 3,6.8-38
- 3,6.9-1
- 3,7.3-1

- 3,8.10-0
- 3,9.2-1
- 3,9.10-2
- 3,9.16-1
- 3.10.6-1
- 3.11.2-6

Versioni di Podman testate

- 3,2.3-0
- 3,4.4+ds1
- 4,1.1-7
- 4,2.0-11
- 4,3.1+ds1-8+b1
- 4,4.1-8
- 4,4.1-12

Versioni di Docker testate

Il supporto di Docker è obsoleto e verrà rimosso in una release futura.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1
- Docker-CE 24,0.2-1
- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1.5-2

Requisiti di CPU e RAM

Prima di installare il software StorageGRID, verificare e configurare l'hardware in modo che sia pronto per il supporto del sistema StorageGRID.

Ogni nodo StorageGRID richiede le seguenti risorse minime:

- Core CPU: 8 per nodo
- RAM: Almeno 24 GB per nodo e da 2 a 16 GB in meno rispetto alla RAM totale del sistema, a seconda della RAM totale disponibile e della quantità di software non StorageGRID in esecuzione nel sistema

Le risorse dei nodi di solo metadati basate su software devono corrispondere alle risorse dei nodi di storage esistenti. Ad esempio:

- Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:
  - 128 GB DI RAM
  - CPU a 8 core
  - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)
- Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuale con 24 GB di RAM, 8 core CPU e 3 TB o 4TB di memorizzazione di metadati, i nodi basati solo sui metadati del software devono utilizzare risorse simili (24 GB di RAM, 8 core CPU e 4TB di memorizzazione di metadati (rangedb/0).

Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve almeno StorageGRID corrispondere ai nodi storage dei siti StorageGRID esistenti e alle nuove risorse del sito.

Assicurarsi che il numero di nodi StorageGRID che si intende eseguire su ciascun host fisico o virtuale non superi il numero di core CPU o la RAM fisica disponibile. Se gli host non sono dedicati all'esecuzione di StorageGRID (non consigliato), assicurarsi di prendere in considerazione i requisiti di risorse delle altre applicazioni.

> Monitorate regolarmente l'utilizzo di CPU e memoria per garantire che queste risorse continuino a soddisfare il vostro carico di lavoro. Ad esempio, raddoppiando l'allocazione di RAM e CPU per i nodi di storage virtuali si fornirebbero risorse simili a quelle fornite per i nodi di appliance StorageGRID. Inoltre, se la quantità di metadati per nodo supera i 500 GB, considerare l'aumento della RAM per nodo a 48 GB o più. Per informazioni sulla gestione dello storage dei metadati degli oggetti, sull'aumento dell'impostazione Metadata Reserved Space e sul monitoraggio dell'utilizzo di CPU e memoria, vedere le istruzioni per "amministrazione", "monitoraggio", e. "aggiornamento in corso" StorageGRID.

Se l'hyperthreading è attivato sugli host fisici sottostanti, è possibile fornire 8 core virtuali (4 core fisici) per nodo. Se l'hyperthreading non è attivato sugli host fisici sottostanti, è necessario fornire 8 core fisici per nodo.

Se si utilizzano macchine virtuali come host e si ha il controllo sulle dimensioni e sul numero di macchine virtuali, è necessario utilizzare una singola macchina virtuale per ciascun nodo StorageGRID e dimensionare di conseguenza la macchina virtuale.

Per le implementazioni in produzione, non è necessario eseguire più nodi di storage sullo stesso hardware di storage fisico o host virtuale. Ciascun nodo di storage in una singola implementazione StorageGRID deve trovarsi nel proprio dominio di errore isolato. È possibile massimizzare la durata e la disponibilità dei dati degli oggetti se si garantisce che un singolo guasto hardware possa avere un impatto solo su un singolo nodo di storage.

Vedere anche "Requisiti di storage e performance".

Requisiti di storage e performance

È necessario comprendere i requisiti di storage e performance per i nodi StorageGRID ospitati dalle macchine virtuali, in modo da fornire spazio sufficiente per supportare la configurazione iniziale e l'espansione futura dello storage.

Requisiti relativi alle performance

Le performance del volume del sistema operativo e del primo volume di storage hanno un impatto significativo sulle performance complessive del sistema. Assicurarsi che queste offrano performance disco adeguate in termini di latenza, operazioni di input/output al secondo (IOPS) e throughput.

Tutti i nodi StorageGRID richiedono che il disco del sistema operativo e tutti i volumi di storage abbiano attivato il caching write-back. La cache deve essere su un supporto protetto o persistente.

Requisiti delle macchine virtuali che utilizzano lo storage NetApp ONTAP

Se stai implementando un nodo StorageGRID come macchina virtuale con lo storage assegnato da un sistema NetApp ONTAP, hai verificato che il volume non disponga di una policy di tiering FabricPool abilitata. Ad esempio, se un nodo StorageGRID viene eseguito come macchina virtuale su un host VMware, assicurati che il volume che supporta l'archivio dati del nodo non disponga di una policy di tiering FabricPool abilitata. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

> Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

Numero di macchine virtuali richieste

Ogni sito StorageGRID richiede almeno tre nodi di storage.

> In un'implementazione in produzione, non eseguire più di un nodo di storage su un singolo server di macchine virtuali. L'utilizzo di un host di macchina virtuale dedicato per ciascun nodo di storage fornisce un dominio di errore isolato.

È possibile implementare altri tipi di nodi, come ad esempio nodi di amministrazione o nodi gateway, sullo stesso host della macchina virtuale oppure su host di macchine virtuali dedicati, in base alle esigenze. Tuttavia, se si dispone di più nodi dello stesso tipo (ad esempio due nodi gateway), non installare tutte le istanze sullo stesso host della macchina virtuale.

Requisiti di storage per tipo di nodo

In un ambiente di produzione, le macchine virtuali per i nodi StorageGRID devono soddisfare requisiti diversi, a seconda dei tipi di nodi.

> Non è possibile utilizzare le snapshot dei dischi per ripristinare i nodi della griglia. Fare riferimento invece alla "recovery del nodo grid" procedure per ogni tipo di nodo.

Tipo di nodo	Storage
Nodo Admin	LUN DA 100 GB PER SISTEMA OPERATIVO LUN da 200 GB per le tabelle dei nodi di amministrazione 200 GB di LUN per il registro di controllo di Admin Node

Tipo di nodo	Storage
Nodo di storage	LUN DA 100 GB PER SISTEMA OPERATIVO 3 LUN per ciascun nodo di storage su questo host **Nota**: Un nodo di storage può avere da 1 a 16 LUN di storage; si consigliano almeno 3 LUN di storage. Dimensione minima per LUN: 4 TB Dimensione massima LUN testata: 39 TB.
Nodo di storage (solo metadati)	LUN DA 100 GB PER SISTEMA OPERATIVO 1 LUN Dimensione minima per LUN: 4 TB **Nota**: Non esiste una dimensione massima per il singolo LUN. La capacità in eccesso viene risparmiata per uso futuro. **Nota**: È richiesto un solo rangedb per i nodi di archiviazione di solo metadati.
Nodo gateway	LUN DA 100 GB PER SISTEMA OPERATIVO
Nodo di archiviazione	LUN DA 100 GB PER SISTEMA OPERATIVO

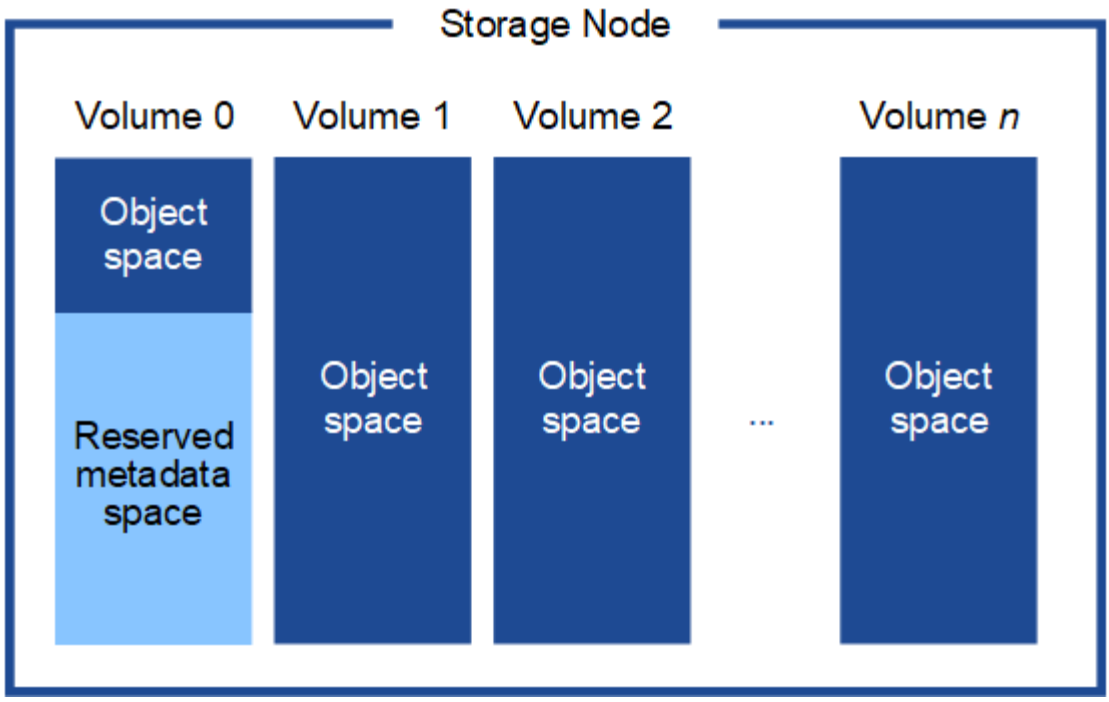
A seconda del livello di audit configurato, la dimensione degli input dell'utente, come il nome della chiave a oggetti S3, Inoltre, la quantità di dati del registro di controllo da conservare potrebbe essere necessaria per aumentare la dimensione del LUN del registro di controllo su ciascun nodo di amministrazione.in genere, una griglia genera circa 1 KB di dati di controllo per ogni operazione S3, Ciò significa che un LUN da 200 GB supporterà 70 milioni di operazioni al giorno o 800 operazioni al secondo per due o tre giorni.

Requisiti di storage per i nodi di storage

Un nodo di storage basato su software può avere da 1 a 16 volumi di storage: Si consiglia di utilizzare almeno -3 volumi di storage. Ogni volume di storage deve essere pari o superiore a 4 TB.

Un nodo di storage dell'appliance può avere fino a 48 volumi di storage.

Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di storage 0 di ciascun nodo di storage. Qualsiasi spazio rimanente sul volume di storage 0 e qualsiasi altro volume di storage nel nodo di storage viene utilizzato esclusivamente per i dati a oggetti.



Per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti del sistema in ogni sito. Le tre copie dei metadati degli oggetti sono distribuite in modo uniforme in tutti i nodi di storage di ciascun sito.

Quando si installa un grid con nodi di storage solo metadati, il grid deve anche contenere un numero minimo di nodi per lo storage a oggetti. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

- Per un grid a sito singolo, vengono configurati almeno due nodi storage per oggetti e metadati.
- Per un grid multisito, per gli oggetti e i metadati viene configurato almeno un nodo di storage per sito.

Quando si assegna spazio al volume 0 di un nuovo nodo di storage, è necessario assicurarsi che vi sia spazio sufficiente per la porzione di tale nodo di tutti i metadati dell'oggetto.

- È necessario assegnare almeno 4 TB al volume 0.

  Se si utilizza un solo volume di storage per un nodo di storage e si assegnano 4 TB o meno al volume, il nodo di storage potrebbe entrare nello stato di sola lettura dello storage all'avvio e memorizzare solo i metadati degli oggetti.

  Se si assegnano meno di 500 GB al volume 0 (solo per uso non in produzione), il 10% della capacità del volume di storage viene riservato ai metadati.

- Le risorse dei nodi di solo metadati basate su software devono corrispondere alle risorse dei nodi di storage esistenti. Ad esempio:
  - Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:
    - 128 GB DI RAM
    - CPU a 8 core
    - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)

    - Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuale con 24 GB di RAM, 8 core CPU e 3 TB o 4TB di memorizzazione di metadati, i nodi basati solo sui metadati del software devono utilizzare risorse simili (24 GB di RAM, 8 core CPU e 4TB di memorizzazione di metadati (rangedb/0).

      Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve almeno StorageGRID corrispondere ai nodi storage dei siti StorageGRID esistenti e alle nuove risorse del sito.

- Se si sta installando un nuovo sistema (StorageGRID 11.6 o superiore) e ciascun nodo di storage dispone di almeno 128 GB di RAM, assegnare 8 TB o più al volume 0. L'utilizzo di un valore maggiore per il volume 0 può aumentare lo spazio consentito per i metadati su ciascun nodo di storage.
- Quando si configurano diversi nodi di storage per un sito, utilizzare la stessa impostazione per il volume 0, se possibile. Se un sito contiene nodi di storage di dimensioni diverse, il nodo di storage con il volume più piccolo 0 determinerà la capacità dei metadati di quel sito.

Per ulteriori informazioni, visitare il sito Web all'indirizzo "Gestire lo storage dei metadati degli oggetti".

Automatizzare l'installazione (VMware)

È possibile utilizzare VMware vSphere per automatizzare l'implementazione dei nodi grid. È inoltre possibile automatizzare la configurazione di StorageGRID.

Automazione dell'implementazione dei nodi grid

USA VMware vSphere per automatizzare l'implementazione dei nodi grid.

Prima di iniziare

- Hai accesso a un sistema Linux/Unix con Bash 3.2 o versione successiva.
- VMware OVF Tool 4.1 è installato e configurato correttamente.
- Conosci il nome utente e la password necessari per accedere a VMware vSphere utilizzando il tool OVF.
- Conosci l'URL dell'infrastruttura virtuale (VI) per la posizione in vSphere in cui desideri implementare le macchine virtuali StorageGRID. In genere, questo URL sarà un vApp o un pool di risorse. Ad esempio: `vi://vcenter.example.com/vi/sgws`

  È possibile utilizzare VMware `ovftool` per determinare questo valore (vedere `ovftool` documentazione per ulteriori dettagli).

  Se si esegue la distribuzione su una vApp, le macchine virtuali non si avviano automaticamente la prima volta ed è necessario accenderle manualmente.

- Sono state raccolte tutte le informazioni necessarie per il file di configurazione. Vedere "Raccogliere informazioni sull'ambiente di implementazione" per informazioni.
- È possibile accedere ai seguenti file dall'archivio di installazione di VMware per StorageGRID:

Nome file	Descrizione
NetApp-SG-version-SHA.vmdk	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid. **Nota:** questo file deve trovarsi nella stessa cartella di `.ovf` e. `.mf` file.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Il file di modello Open Virtualization Format (`.ovf`) e il file manifest (`.mf`) Per l'implementazione del nodo di amministrazione primario.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi amministrativi non primari.
vsphere-archive.ovf vsphere-archive.mf	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi di archiviazione.
vsphere-gateway.ovf vsphere-gateway.mf	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi gateway.
vsphere-storage.ovf vsphere-storage.mf	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi di storage basati su macchine virtuali.
deploy-vsphere-ovftool.sh	Lo script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.
deploy-vsphere-ovftool-sample.ini	Il file di configurazione di esempio da utilizzare con `deploy-vsphere-ovftool.sh` script.

Definire il file di configurazione per l'implementazione

Specificare le informazioni necessarie per implementare i nodi virtual grid per StorageGRID in un file di configurazione, utilizzato da `deploy-vsphere-ovftool.sh` Script bash. È possibile modificare un file di configurazione di esempio, in modo da non dover creare il file da zero.

Fasi

1. Eseguire una copia del file di configurazione di esempio (`deploy-vsphere-ovftool.sample.ini`). Salvare il nuovo file con nome `deploy-vsphere-ovftool.ini` nella stessa directory di `deploy-vsphere-ovftool.sh`.
2. Aprire `deploy-vsphere-ovftool.ini`.
3. Inserire tutte le informazioni necessarie per implementare i nodi virtual grid VMware.

   Vedere Impostazioni del file di configurazione per informazioni.

4. Una volta inserite e verificate tutte le informazioni necessarie, salvare e chiudere il file.

Impostazioni del file di configurazione

Il `deploy-vsphere-ovftool.ini` il file di configurazione contiene le impostazioni necessarie per implementare i nodi virtual grid.

Il file di configurazione elenca prima i parametri globali, quindi i parametri specifici del nodo nelle sezioni definite dal nome del nodo. Quando si utilizza il file:

- I *parametri globali* vengono applicati a tutti i nodi della griglia.
- *Parametri specifici del nodo* sovrascrivono i parametri globali.

Parametri globali

I parametri globali vengono applicati a tutti i nodi della griglia, a meno che non vengano ignorati dalle impostazioni delle singole sezioni. Posizionare i parametri che si applicano a più nodi nella sezione Global Parameter (parametri globali), quindi eseguire l'override di queste impostazioni secondo necessità nelle sezioni relative ai singoli nodi.

- **OVFTOOL_ARGUMENTS**: È possibile specificare OVFTOOL_ARGUMENTS come impostazioni globali oppure applicare gli argomenti singolarmente a nodi specifici. Ad esempio:

  ```
  OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
  --datastore='datastore_name'
  ```

  È possibile utilizzare `--powerOffTarget` e. `--overwrite` opzioni per arrestare e sostituire le macchine virtuali esistenti.

  > È necessario distribuire i nodi in diversi datastore e specificare OVFTOOL_ARGUMENTS per ciascun nodo, invece che globalmente.

- **SOURCE**: Percorso del modello di macchina virtuale StorageGRID (`.vmdk`) e il `.ovf` e. `.mf` file per singoli nodi griglia. Per impostazione predefinita, viene impostata la directory corrente.

  ```
  SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
  ```

- **TARGET**: URL dell'infrastruttura virtuale VMware vSphere (vi) per la posizione in cui verrà implementato StorageGRID. Ad esempio:

  ```
  TARGET = vi://vcenter.example.com/vm/sgws
  ```

- **GRID_NETWORK_CONFIG**: Metodo utilizzato per acquisire indirizzi IP, STATICI o DHCP. L'impostazione predefinita è STATICO. Se tutti o la maggior parte dei nodi utilizzano lo stesso metodo per l'acquisizione degli indirizzi IP, è possibile specificare questo metodo. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
GRID_NETWORK_CONFIG = DHCP
```

- **GRID_NETWORK_TARGET**: Il nome di una rete VMware esistente da utilizzare per Grid Network. Se tutti o la maggior parte dei nodi utilizzano lo stesso nome di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
GRID_NETWORK_TARGET = SG-Admin-Network
```

- **GRID_NETWORK_MASK**: La maschera di rete per Grid Network. Se tutti o la maggior parte dei nodi utilizzano la stessa maschera di rete, è possibile specificarla qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY**: Gateway di rete per Grid Network. Se tutti o la maggior parte dei nodi utilizzano lo stesso gateway di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU**: OPZIONALE. L'unità di trasmissione massima (MTU) sulla rete di rete. Se specificato, il valore deve essere compreso tra 1280 e 9216. Ad esempio:

```
GRID_NETWORK_MTU = 8192
```

  Se omesso, viene utilizzato 1400.

  Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito.

  > Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.

  > Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete.

- **ADMIN_NETWORK_CONFIG**: Metodo utilizzato per acquisire gli indirizzi IP, DISABILITATI, STATICI o DHCP. L'impostazione predefinita è DISATTIVATA. Se tutti o la maggior parte dei nodi utilizzano lo stesso metodo per l'acquisizione degli indirizzi IP, è possibile specificare questo metodo. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi.

Ad esempio:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET**: Il nome di una rete VMware esistente da utilizzare per la rete di amministrazione. Questa impostazione è obbligatoria a meno che la rete amministrativa non sia disattivata. Se tutti o la maggior parte dei nodi utilizzano lo stesso nome di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_TARGET = SG-Admin-Network
```

- **ADMIN_NETWORK_MASK**: La maschera di rete per la rete di amministrazione. Questa impostazione è obbligatoria se si utilizza l'indirizzamento IP statico. Se tutti o la maggior parte dei nodi utilizzano la stessa maschera di rete, è possibile specificarla qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY**: Gateway di rete per la rete di amministrazione. Questa impostazione è necessaria se si utilizza un indirizzo IP statico e si specificano sottoreti esterne nell'impostazione ADMIN_NETWORK_ESL. (Ovvero, non è necessario se ADMIN_NETWORK_ESL è vuoto). Se tutti o la maggior parte dei nodi utilizzano lo stesso gateway di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL**: L'elenco di subnet esterne (route) per la rete amministrativa, specificato come elenco separato da virgole delle destinazioni di routing CIDR. Se tutti o la maggior parte dei nodi utilizzano lo stesso elenco di subnet esterne, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU**: OPZIONALE. L'unità di trasmissione massima (MTU) sulla rete di amministrazione. Non specificare se ADMIN_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omesso, viene utilizzato 1400. Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito. Se tutti o la maggior parte dei nodi utilizzano la stessa MTU per la rete di amministrazione, è possibile specificarla qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG**: Metodo utilizzato per acquisire gli indirizzi IP, DISABILITATI, STATICI o DHCP. L'impostazione predefinita è DISATTIVATA. Se tutti o la maggior parte dei nodi utilizzano lo stesso metodo per l'acquisizione degli indirizzi IP, è possibile specificare questo metodo. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET**: Il nome di una rete VMware esistente da utilizzare per la rete client. Questa impostazione è obbligatoria a meno che la rete client non sia disattivata. Se tutti o la maggior parte dei nodi utilizzano lo stesso nome di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_TARGET = SG-Client-Network
```

- **CLIENT_NETWORK_MASK**: La maschera di rete per la rete client. Questa impostazione è obbligatoria se si utilizza l'indirizzamento IP statico. Se tutti o la maggior parte dei nodi utilizzano la stessa maschera di rete, è possibile specificarla qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY**: Gateway di rete per la rete client. Questa impostazione è obbligatoria se si utilizza l'indirizzamento IP statico. Se tutti o la maggior parte dei nodi utilizzano lo stesso gateway di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU**: OPZIONALE. L'unità di trasmissione massima (MTU) sulla rete client. Non specificare se CLIENT_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omesso, viene utilizzato 1400. Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito. Se tutti o la maggior parte dei nodi utilizzano lo stesso MTU per la rete client, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP**: Consente di rimappare qualsiasi porta utilizzata da un nodo per le comunicazioni interne al nodo di rete o esterne. Il rimapping delle porte è necessario se i criteri di rete aziendali limitano una o più porte utilizzate da StorageGRID. Per l'elenco delle porte utilizzate da StorageGRID, vedere comunicazioni interne del nodo di rete e comunicazioni esterne in "Linee guida per il networking".

Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico.

Se viene impostato solo PORT_REMAP, il mapping specificato viene utilizzato per le comunicazioni in entrata e in uscita. Se VIENE specificato anche PORT_REMAP_INBOUND, PORT_REMAP si applica solo alle comunicazioni in uscita.

Il formato utilizzato è: *network type/protocol/default port used by grid node/new port*, dove il tipo di rete è grid, admin o client e il protocollo è tcp o udp.

Ad esempio:

```
PORT_REMAP = client/tcp/18082/443
```

Se utilizzata da sola, questa impostazione di esempio mappa simmetricamente le comunicazioni in entrata e in uscita per il nodo della griglia dalla porta 18082 alla porta 443. Se utilizzata in combinazione con PORT_REMAP_INBOUND, questa impostazione di esempio mappa le comunicazioni in uscita dalla porta 18082 alla porta 443.

- **PORT_REMAP_INBOUND**: Consente di rimappare le comunicazioni in entrata per la porta specificata. Se si specifica PORT_REMAP_INBOUND ma non si specifica un valore per PORT_REMAP, le comunicazioni in uscita per la porta rimangono invariate.

  Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico.

  Il formato utilizzato è: *network type/protocol/_default port used by grid node/new port*, dove il tipo di rete è grid, admin o client e il protocollo è tcp o udp.

  Ad esempio:

  ```
  PORT_REMAP_INBOUND = client/tcp/443/18082
  ```

  In questo esempio, il traffico inviato alla porta 443 passa attraverso un firewall interno e lo indirizza alla porta 18082, dove il nodo della griglia è in attesa delle richieste S3.

- **TEMPORARY_PASSWORD_TYPE**: Il tipo di password di installazione temporanea da utilizzare quando si accede alla console VM o si utilizza SSH prima che il nodo si unisca alla griglia.

  Se tutti o la maggior parte dei nodi utilizzano lo stesso tipo di password di installazione temporanea, specificare il tipo nella sezione Global Parameter (parametro globale). Quindi, facoltativamente, utilizzare un'impostazione diversa per un singolo nodo. Ad esempio, se si seleziona **Usa password personalizzata** a livello globale, è possibile utilizzare **CUSTOM_TEMPORARY_PASSWORD=<password>** per impostare la password per ciascun nodo.

  TEMPORARY_PASSWORD_TYPE può essere uno dei seguenti:

  - **Usa nome nodo**: Il nome nodo viene utilizzato come password di installazione temporanea.

- **Disattiva password**: Non verrà utilizzata alcuna password di installazione temporanea. Se è necessario accedere alla VM per eseguire il debug dei problemi di installazione, vedere "Risolvere i problemi di installazione".
- **Usa password personalizzata**: Il valore fornito con **CUSTOM_TEMPORARY_PASSWORD=<password>** viene utilizzato come password di installazione temporanea.

> Facoltativamente, è possibile omettere il parametro **TEMPORARY_PASSWORD_TYPE** e specificare solo **CUSTOM_TEMPORARY_PASSWORD=<password>**.

- **CUSTOM_TEMPORARY_PASSWORD=<password>**
  Opzionale. La password temporanea da utilizzare quando si accede a questa macchina virtuale e si utilizza SSH durante l'installazione. Ignorato se **TEMPORARY_PASSWORD_TYPE** è impostato su **use node name** o **Disable password**.

Parametri specifici del nodo

Ogni nodo si trova nella propria sezione del file di configurazione. Ogni nodo richiede le seguenti impostazioni:

- L'Head della sezione definisce il nome del nodo che verrà visualizzato in Grid Manager. È possibile eseguire l'override di tale valore specificando il parametro NODE_NAME opzionale per il nodo.
- **NODE_TYPE**: Nodo_amministrazione_VM, nodo_storage_VM, nodo_archivio_VM o nodo_gateway_API_VM
- **GRID_NETWORK_IP**: L'indirizzo IP del nodo della rete Grid.
- **ADMIN_NETWORK_IP**: L'indirizzo IP del nodo nella rete di amministrazione. Obbligatorio solo se il nodo è collegato alla rete di amministrazione e ADMIN_NETWORK_CONFIG è impostato su STATIC.
- **CLIENT_NETWORK_IP**: L'indirizzo IP del nodo sulla rete client. Obbligatorio solo se il nodo è collegato alla rete client e CLIENT_NETWORK_CONFIG per questo nodo è impostato su STATIC.
- **ADMIN_IP**: L'indirizzo IP del nodo Admin primario sulla rete Grid. Utilizzare il valore specificato come GRID_NETWORK_IP per il nodo di amministrazione primario. Se si omette questo parametro, il nodo tenta di rilevare l'IP del nodo di amministrazione primario utilizzando mDNS. Per ulteriori informazioni, vedere "In che modo i nodi della griglia rilevano il nodo di amministrazione primario".

> Il parametro ADMIN_IP viene ignorato per il nodo di amministrazione primario.

- Tutti i parametri che non sono stati impostati globalmente. Ad esempio, se un nodo è collegato alla rete di amministrazione e non sono stati specificati i parametri ADMIN_NETWORK a livello globale, è necessario specificarli per il nodo.

Nodo amministratore primario

Per il nodo di amministrazione primario sono necessarie le seguenti impostazioni aggiuntive:

- **NODE_TYPE**: Nodo_amministrazione_VM
- **RUOLO_AMMINISTRATORE**: Primario

Questa voce di esempio si intende per un nodo amministratore primario che si trova su tutte e tre le reti:

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

La seguente impostazione aggiuntiva è facoltativa per il nodo di amministrazione primario:

- **DISCO**: Per impostazione predefinita, ai nodi di amministrazione vengono assegnati due dischi rigidi aggiuntivi da 200 GB per l'audit e l'utilizzo del database. È possibile aumentare queste impostazioni utilizzando il parametro DISK. Ad esempio:

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  Per i nodi di amministrazione, LE ISTANZE devono sempre essere uguali a 2.

Nodo di storage

Per i nodi di storage è necessaria la seguente impostazione aggiuntiva:

- **NODE_TYPE**: Nodo_storage_VM

  Questa voce di esempio si applica a un nodo di storage che si trova sulle reti Grid e Admin, ma non sulla rete client. Questo nodo utilizza L'impostazione ADMIN_IP per specificare l'indirizzo IP del nodo di amministrazione primario sulla rete di griglia.

  ```
  [DC1-S1]
    NODE_TYPE = VM_Storage_Node

    GRID_NETWORK_IP = 10.1.0.3
    ADMIN_NETWORK_IP = 10.3.0.3

    ADMIN_IP = 10.1.0.2
  ```

  Questo secondo esempio riguarda un nodo di storage su una rete client in cui la policy di rete aziendale del cliente afferma che un'applicazione client S3 è autorizzata ad accedere al nodo di storage solo utilizzando la porta 80 o 443. Il file di configurazione di esempio utilizza PORT_REMAP per consentire al nodo di storage di inviare e ricevere messaggi S3 sulla porta 443.

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

L'ultimo esempio crea un remapping simmetrico per il traffico ssh dalla porta 22 alla porta 3022, ma imposta esplicitamente i valori per il traffico in entrata e in uscita.

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

La seguente impostazione aggiuntiva è facoltativa per i nodi di storage:

- **DISCO**: Per impostazione predefinita, ai nodi di storage vengono assegnati tre dischi da 4 TB per l'utilizzo di RangeDB. È possibile aumentare queste impostazioni con il parametro DISK. Ad esempio:

```
DISK = INSTANCES=16, CAPACITY=4096
```

Nodo di archiviazione

Per i nodi di archiviazione è necessaria la seguente impostazione aggiuntiva:

- **NODE_TYPE**: Nodo_archivio_VM

Questa voce di esempio si applica a un nodo di archiviazione che si trova nelle reti Grid e Admin, ma non nella rete client.

```
[DC1-ARC1]
  NODE_TYPE = VM_Archive_Node

  GRID_NETWORK_IP = 10.1.0.4
  ADMIN_NETWORK_IP = 10.3.0.4

  ADMIN_IP = 10.1.0.2
```

Nodo gateway

Per i nodi gateway è necessaria la seguente impostazione aggiuntiva:

- **NODE_TYPE**: GATEWAY VM_API

Questa voce di esempio è un nodo gateway di esempio su tutte e tre le reti. In questo esempio, nella sezione globale del file di configurazione non è stato specificato alcun parametro di rete client, pertanto è necessario specificarlo per il nodo:

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG-Client-Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

Nodo amministrativo non primario

Per i nodi amministrativi non primari sono necessarie le seguenti impostazioni aggiuntive:

- **NODE_TYPE**: Nodo_amministrazione_VM
- **RUOLO_AMMINISTRATORE**: Non primario

Questa voce di esempio si trova per un nodo amministrativo non primario che non si trova nella rete client:

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG-Grid-Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

La seguente impostazione aggiuntiva è facoltativa per i nodi di amministrazione non primari:

- **DISCO**: Per impostazione predefinita, ai nodi di amministrazione vengono assegnati due dischi rigidi aggiuntivi da 200 GB per l'audit e l'utilizzo del database. È possibile aumentare queste impostazioni utilizzando il parametro DISK. Ad esempio:

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  Per i nodi di amministrazione, LE ISTANZE devono sempre essere uguali a 2.

Eseguire lo script Bash

È possibile utilizzare `deploy-vsphere-ovftool.sh` Bash script e il file di configurazione deploy-vsphere-ovftool.ini modificati per automatizzare la distribuzione dei nodi StorageGRID in VMware vSphere.

Prima di iniziare

- È stato creato un file di configurazione deploy-vsphere-ovftool.ini per il proprio ambiente.

È possibile utilizzare la guida disponibile con lo script Bash immettendo i comandi della guida (`-h/--help`). Ad esempio:

```
./deploy-vsphere-ovftool.sh -h
```

oppure

```
./deploy-vsphere-ovftool.sh --help
```

Fasi

1. Accedere alla macchina Linux in uso per eseguire lo script Bash.
2. Passare alla directory in cui è stato estratto l'archivio di installazione.

   Ad esempio:

```
cd StorageGRID-Webscale-version/vsphere
```

3. Per implementare tutti i nodi grid, eseguire lo script Bash con le opzioni appropriate per il proprio ambiente.

   Ad esempio:

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
vsphere-ovftool.ini
```

4. Se un nodo Grid non è riuscito a implementare a causa di un errore, risolvere l'errore ed eseguire nuovamente lo script Bash solo per quel nodo.

   Ad esempio:

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
-node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

La distribuzione è completa quando lo stato per ogni nodo è "passato".

```
Deployment Summary
+------------------------------+----------+----------------------+
| node                         | attempts | status               |
+------------------------------+----------+----------------------+
| DC1-ADM1                     |        1 | Passed               |
| DC1-G1                       |        1 | Passed               |
| DC1-S1                       |        1 | Passed               |
| DC1-S2                       |        1 | Passed               |
| DC1-S3                       |        1 | Passed               |
+------------------------------+----------+----------------------+
```

Automatizzare la configurazione di StorageGRID

Una volta implementati i nodi grid, è possibile automatizzare la configurazione del sistema StorageGRID.

Prima di iniziare

- Si conosce la posizione dei seguenti file dall'archivio di installazione.

Nome file	Descrizione
configure-storagegrid.py	Script Python utilizzato per automatizzare la configurazione

Nome file	Descrizione
configure-storagegrid.sample.json	File di configurazione di esempio da utilizzare con lo script
configure-storagegrid.blank.json	File di configurazione vuoto da utilizzare con lo script

- È stato creato un `configure-storagegrid.json` file di configurazione. Per creare questo file, è possibile modificare il file di configurazione di esempio (`configure-storagegrid.sample.json`) o il file di configurazione vuoto (`configure-storagegrid.blank.json`).

È possibile utilizzare `configure-storagegrid.py` Script Python e il `configure-storagegrid.json` File di configurazione per automatizzare la configurazione del sistema StorageGRID.

È inoltre possibile configurare il sistema utilizzando Grid Manager o l'API di installazione.

Fasi

1. Accedere alla macchina Linux in uso per eseguire lo script Python.
2. Passare alla directory in cui è stato estratto l'archivio di installazione.

   Ad esempio:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   dove `platform` è debs, rpms o vsphere.

3. Eseguire lo script Python e utilizzare il file di configurazione creato.

   Ad esempio:

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Risultato

Un pacchetto di ripristino `.zip` il file viene generato durante il processo di configurazione e scaricato nella directory in cui si esegue il processo di installazione e configurazione. È necessario eseguire il backup del file del pacchetto di ripristino in modo da poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi della griglia. Ad esempio, copiarla in una posizione di rete sicura e di backup e in una posizione di cloud storage sicura.

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.

Se si specifica che devono essere generate password casuali, aprire `Passwords.txt` E cercare le password necessarie per accedere al sistema StorageGRID.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Il sistema StorageGRID viene installato e configurato quando viene visualizzato un messaggio di conferma.

```
StorageGRID has been configured and installed.
```

Informazioni correlate

"Accedere a Grid Manager"

"Panoramica dell'API REST per l'installazione"

Implementazione di Virtual Machine Grid Node (VMware)

Raccogliere informazioni sull'ambiente di implementazione

Prima di implementare i nodi grid, è necessario raccogliere informazioni sulla configurazione di rete e sull'ambiente VMware.

> È più efficiente eseguire una singola installazione di tutti i nodi, piuttosto che installare alcuni nodi ora e alcuni nodi successivamente.

Informazioni VMware

È necessario accedere all'ambiente di implementazione e raccogliere informazioni sull'ambiente VMware, sulle reti create per Grid, Admin e Client Network e sui tipi di volumi di storage che si intende utilizzare per i nodi di storage.

È necessario raccogliere informazioni sull'ambiente VMware, tra cui:

- Il nome utente e la password di un account VMware vSphere che dispone delle autorizzazioni appropriate per completare l'implementazione.
- Informazioni sulla configurazione di rete, datastore e host per ogni macchina virtuale a nodi StorageGRID.

> VMware Live vMotion fa saltare il tempo di clock della macchina virtuale e non è supportato per i nodi grid di qualsiasi tipo. Anche se rari, tempi di clock errati possono causare la perdita di dati o aggiornamenti della configurazione.

Informazioni Grid Network

È necessario raccogliere informazioni sulla rete VMware creata per la rete grid StorageGRID (richiesta), tra cui:

- Il nome della rete.
- Metodo utilizzato per assegnare indirizzi IP, statici o DHCP.
  - Se si utilizzano indirizzi IP statici, i dettagli di rete richiesti per ciascun nodo della griglia (indirizzo IP, gateway, maschera di rete).
  - Se si utilizza DHCP, l'indirizzo IP del nodo amministrativo primario sulla rete Grid. Vedere "In che modo i nodi della griglia rilevano il nodo di amministrazione primario" per ulteriori informazioni.

Admin Network Information (informazioni di rete amministratore

Per i nodi che saranno connessi alla rete amministrativa StorageGRID opzionale, è necessario raccogliere informazioni sulla rete VMware creata per questa rete, tra cui:

- Il nome della rete.
- Metodo utilizzato per assegnare indirizzi IP, statici o DHCP.
  - Se si utilizzano indirizzi IP statici, i dettagli di rete richiesti per ciascun nodo della griglia (indirizzo IP, gateway, maschera di rete).
  - Se si utilizza DHCP, l'indirizzo IP del nodo amministrativo primario sulla rete Grid. Vedere "In che modo i nodi della griglia rilevano il nodo di amministrazione primario" per ulteriori informazioni.
- L'elenco di subnet esterne (ESL) per la rete di amministrazione.

Informazioni di rete del client

Per i nodi che saranno connessi alla rete client StorageGRID opzionale, è necessario raccogliere informazioni sulla rete VMware creata per questa rete, tra cui:

- Il nome della rete.
- Metodo utilizzato per assegnare indirizzi IP, statici o DHCP.
- Se si utilizzano indirizzi IP statici, i dettagli di rete richiesti per ciascun nodo della griglia (indirizzo IP, gateway, maschera di rete).

Informazioni su interfacce aggiuntive

È possibile aggiungere interfacce di accesso o trunk alla macchina virtuale in vCenter dopo aver installato il nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (ha).

Le interfacce aggiunte vengono visualizzate nella pagina delle interfacce VLAN e nella pagina dei gruppi ha in Grid Manager.

- Se si aggiunge un'interfaccia di linea, configurare una o più interfacce VLAN per ogni nuova interfaccia principale. Vedere "Configurare le interfacce VLAN".
- Se si aggiunge un'interfaccia di accesso, è necessario aggiungerla direttamente ai gruppi ha. Vedere "configurare i gruppi ad alta disponibilità".

Volumi di storage per nodi di storage virtuali

Per i nodi di storage basati su macchine virtuali, è necessario raccogliere le seguenti informazioni:

- Il numero e la dimensione dei volumi di storage (LUN di storage) che si intende aggiungere. Vedere

"Requisiti di storage e performance"."

Informazioni sulla configurazione della griglia

È necessario raccogliere informazioni per configurare la griglia:

- Licenza Grid
- Indirizzi IP del server NTP (Network Time Protocol)
- Indirizzi IP del server DNS

In che modo i nodi della griglia rilevano il nodo di amministrazione primario

I nodi Grid comunicano con il nodo Admin primario per la configurazione e la gestione. Ciascun nodo della griglia deve conoscere l'indirizzo IP del nodo di amministrazione primario sulla rete di griglia.

Per garantire che un nodo Grid possa accedere al nodo Admin primario, è possibile eseguire una delle seguenti operazioni durante l'implementazione del nodo:

- È possibile utilizzare IL parametro ADMIN_IP per inserire manualmente l'indirizzo IP del nodo di amministrazione primario.
- È possibile omettere il parametro ADMIN_IP per fare in modo che il nodo Grid rilevi automaticamente il valore. Il rilevamento automatico è particolarmente utile quando Grid Network utilizza DHCP per assegnare l'indirizzo IP al nodo di amministrazione primario.

Il rilevamento automatico del nodo di amministrazione primario viene eseguito utilizzando un sistema di nomi di dominio multicast (mDNS). Al primo avvio, il nodo di amministrazione primario pubblica il proprio indirizzo IP utilizzando mDNS. Gli altri nodi della stessa sottorete possono quindi ricercare l'indirizzo IP e acquisirlo automaticamente. Tuttavia, poiché il traffico IP multicast non è normalmente instradabile attraverso le sottoreti, i nodi su altre sottoreti non possono acquisire direttamente l'indirizzo IP del nodo di amministrazione primario.

Se si utilizza la ricerca automatica:

- È necessario includere l'impostazione ADMIN_IP per almeno un nodo Grid su qualsiasi subnet a cui non è collegato direttamente il nodo Admin primario. Questo nodo della griglia pubblicherà quindi l'indirizzo IP del nodo di amministrazione primario per gli altri nodi della subnet da rilevare con mDNS.
- Assicurarsi che l'infrastruttura di rete supporti il passaggio del traffico IP multi-cast all'interno di una subnet.

Implementare un nodo StorageGRID come macchina virtuale

VMware vSphere Web Client consente di implementare ciascun nodo grid come macchina virtuale. Durante l'implementazione, ciascun nodo grid viene creato e connesso a una o più reti StorageGRID.

Se è necessario implementare nodi di storage dell'appliance StorageGRID, vedere "Implementare l'appliance Storage Node".

In alternativa, è possibile rimappare le porte dei nodi o aumentare le impostazioni della CPU o della memoria per il nodo prima di accenderlo.

Prima di iniziare

- Hai esaminato la procedura "pianificare e preparare l'installazione"E comprendete i requisiti relativi a software, CPU e RAM, storage e performance.
- Hai familiarità con VMware vSphere Hypervisor e hai esperienza nell'implementazione di macchine virtuali in questo ambiente.

> Il `open-vm-tools` Il pacchetto, un'implementazione open-source simile a VMware Tools, è incluso nella macchina virtuale StorageGRID. Non è necessario installare VMware Tools manualmente.

- È stata scaricata ed estratta la versione corretta dell'archivio di installazione di StorageGRID per VMware.

> Se si implementa il nuovo nodo come parte di un'operazione di espansione o ripristino, è necessario utilizzare la versione di StorageGRID attualmente in esecuzione sulla griglia.

- Si dispone del disco della macchina virtuale StorageGRID (`.vmdk`) file:

```
NetApp-SG-version-SHA.vmdk
```

- Hai il `.ovf` e. `.mf` file per ogni tipo di nodo griglia che si sta implementando:

Nome file	Descrizione
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Il file di modello e il file manifest per il nodo di amministrazione primario.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Il file di modello e il file manifest per un nodo di amministrazione non primario.
vsphere-storage.ovf vsphere-storage.mf	Il file modello e il file manifesto per un nodo di storage.
vsphere-gateway.ovf vsphere-gateway.mf	Il file di modello e il file manifest per un nodo gateway.
vsphere-archive.ovf vsphere-archive.mf	Il file modello e il file manifesto per un nodo di archiviazione.

- Il `.vdmk`, `.ovf`, e. `.mf` i file si trovano tutti nella stessa directory.
- Hai un piano per ridurre al minimo i domini di guasto. Ad esempio, non è necessario implementare tutti i nodi gateway su un singolo server di macchine virtuali.

In un'implementazione in produzione, non eseguire più di un nodo di storage su un singolo server di macchine virtuali. L'utilizzo di un host di macchina virtuale dedicato per ciascun nodo di storage fornisce un dominio di errore isolato.

- Se si implementa un nodo come parte di un'operazione di espansione o ripristino, si dispone di "Istruzioni per espandere un sistema StorageGRID" o il "istruzioni per il ripristino e la manutenzione".
- Se stai implementando un nodo StorageGRID come macchina virtuale con lo storage assegnato da un sistema NetApp ONTAP, hai verificato che il volume non disponga di una policy di tiering FabricPool abilitata. Ad esempio, se un nodo StorageGRID viene eseguito come macchina virtuale su un host VMware, assicurati che il volume che supporta l'archivio dati del nodo non disponga di una policy di tiering FabricPool abilitata. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

A proposito di questa attività

Seguire queste istruzioni per implementare inizialmente i nodi VMware, aggiungere un nuovo nodo VMware in un'espansione o sostituire un nodo VMware come parte di un'operazione di recovery. Ad eccezione di quanto indicato nei passaggi, la procedura di implementazione del nodo è la stessa per tutti i tipi di nodo, inclusi i nodi Admin, Storage, Gateway e Archive.

Se si sta installando un nuovo sistema StorageGRID:

- È necessario implementare il nodo di amministrazione primario prima di implementare qualsiasi altro nodo della griglia.
- È necessario assicurarsi che ciascuna macchina virtuale possa connettersi al nodo di amministrazione primario tramite la rete di rete.
- È necessario implementare tutti i nodi della griglia prima di configurarla.

Se si sta eseguendo un'operazione di espansione o ripristino:

- È necessario assicurarsi che la nuova macchina virtuale possa connettersi al nodo di amministrazione primario tramite la rete di rete.

Se è necessario rimappare una delle porte del nodo, non accendere il nuovo nodo fino a quando la configurazione del rimappamento delle porte non è completa.

Fasi

1. Utilizzando vCenter, implementare un modello OVF.

   Se si specifica un URL, selezionare una cartella contenente i seguenti file. In caso contrario, selezionare ciascuno di questi file da una directory locale.

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-node.ovf
   vsphere-node.mf
   ```

Ad esempio, se si tratta del primo nodo che si sta implementando, utilizzare questi file per distribuire il nodo di amministrazione primario per il sistema StorageGRID:

```
NetApp-SG-version-SHA.vmdk
vsphere-primary-admin.ovf
vsphere-primary-admin.mf
```

2. Specificare un nome per la macchina virtuale.

   La procedura standard consiste nell'utilizzare lo stesso nome sia per la macchina virtuale che per il nodo Grid.

3. Posizionare la macchina virtuale nella vApp o nel pool di risorse appropriato.
4. Se si sta implementando il nodo di amministrazione principale, leggere e accettare il Contratto di licenza con l'utente finale.

   A seconda della versione di vCenter in uso, l'ordine dei passaggi varia in base all'accettazione del Contratto di licenza con l'utente finale, specificando il nome della macchina virtuale e selezionando un datastore.

5. Selezionare lo storage per la macchina virtuale.

   Se si sta implementando un nodo come parte dell'operazione di ripristino, eseguire le istruzioni in fase di recovery dello storage per aggiungere nuovi dischi virtuali, ricollegare i dischi rigidi virtuali dal nodo grid guasto o da entrambi.

   Quando si implementa un nodo di storage, utilizzare 3 o più volumi di storage, con un volume di storage di 4 TB o superiore. È necessario assegnare almeno 4 TB al volume 0.

   > Il file .ovf del nodo di storage definisce diversi VMDK per lo storage. A meno che questi VMDK non soddisfino i requisiti di storage, è necessario rimuoverli e assegnare VMDK o RDM appropriati per lo storage prima di accendere il nodo. I VMDK sono più comunemente utilizzati negli ambienti VMware e sono più facili da gestire, mentre gli RDM potrebbero fornire performance migliori per i carichi di lavoro che utilizzano oggetti di dimensioni maggiori (ad esempio, superiori a 100 MB).

   > Alcune installazioni StorageGRID potrebbero utilizzare volumi di storage più grandi e attivi rispetto ai carichi di lavoro virtualizzati tipici. Potrebbe essere necessario regolare alcuni parametri dell'hypervisor, ad esempio `MaxAddressableSpaceTB`, per ottenere performance ottimali. In caso di performance scadenti, contatta la risorsa di supporto per la virtualizzazione per determinare se il tuo ambiente potrebbe trarre beneficio dall'ottimizzazione della configurazione specifica del carico di lavoro.

6. Selezionare reti.

   Determinare quali reti StorageGRID utilizzare dal nodo selezionando una rete di destinazione per ciascuna rete di origine.

   - La rete grid è obbligatoria. Selezionare una rete di destinazione nell'ambiente vSphere.
   - Se si utilizza la rete di amministrazione, selezionare un'altra rete di destinazione nell'ambiente vSphere. Se non si utilizza la rete di amministrazione, selezionare la stessa destinazione selezionata

per la rete di griglia.

- Se si utilizza la rete client, selezionare un'altra rete di destinazione nell'ambiente vSphere. Se non si utilizza la rete client, selezionare la stessa destinazione selezionata per la rete griglia.

7. Per **Personalizza modello**, configurare le proprietà del nodo StorageGRID richieste.

   a. Inserire il nome del nodo.

      Se si sta ripristinando un nodo Grid, è necessario immettere il nome del nodo che si sta ripristinando.

   b. Utilizzare il menu a discesa **Password di installazione temporanea** per specificare una password di installazione temporanea, in modo da poter accedere alla console VM o utilizzare SSH prima che il nuovo nodo si unisca alla griglia.

      La password di installazione temporanea viene utilizzata solo durante l'installazione del nodo. Dopo aver aggiunto un nodo alla griglia, è possibile accedervi tramite "password della console del nodo", che è elencato nella `Passwords.txt` Nel pacchetto di ripristino.

      - **Usa nome nodo**: Il valore fornito per il campo **Nome nodo** viene utilizzato come password di installazione temporanea.
      - **Usa password personalizzata**: Viene utilizzata una password personalizzata come password di installazione temporanea.
      - **Disattiva password**: Non verrà utilizzata alcuna password di installazione temporanea. Se è necessario accedere alla VM per eseguire il debug dei problemi di installazione, vedere "Risolvere i problemi di installazione".

   c. Se è stato selezionato **Usa password personalizzata**, specificare la password di installazione temporanea che si desidera utilizzare nel campo **Password personalizzata**.

   d. Nella sezione **Grid Network (eth0)**, selezionare STATIC (STATICO) o DHCP per la configurazione **Grid network IP (IP rete griglia)**.

      - Se si seleziona STATIC (STATICO), inserire **Grid network IP**, **Grid network mask**, **Grid network gateway** e **Grid network MTU**.
      - Se si seleziona DHCP, vengono assegnati automaticamente **Grid network IP**, **Grid network mask** e **Grid network gateway**.

   e. Nel campo **Primary Admin IP** (Indirizzo amministratore primario), immettere l'indirizzo IP del nodo di amministrazione primario per la rete di rete.

      Questo passaggio non si applica se il nodo che si sta implementando è il nodo Admin primario.

   Se si omette l'indirizzo IP principale del nodo di amministrazione, l'indirizzo IP verrà rilevato automaticamente se il nodo di amministrazione primario, o almeno un altro nodo della griglia con ADMIN_IP configurato, è presente sulla stessa sottorete. Tuttavia, si consiglia di impostare qui l'indirizzo IP del nodo di amministrazione principale.

   a. Nella sezione **Admin Network (eth1)**, selezionare STATIC (STATICO), DHCP (DHCP) o DISABLED (DISATTIVATO) per la configurazione **Admin network IP (Indirizzo IP di rete amministratore)**.

      - Se non si desidera utilizzare la rete di amministrazione, selezionare DISABLED (DISATTIVATA) e immettere **0.0.0.0** come IP della rete di amministrazione. È possibile lasciare vuoti gli altri campi.

- Se si seleziona STATICO, inserire **Admin network IP**, **Admin network mask**, **Admin network gateway** e **Admin network MTU**.
- Se si seleziona STATICO, inserire l'elenco **Admin network external subnet list**. È inoltre necessario configurare un gateway.
- Se si seleziona DHCP, vengono assegnati automaticamente **Admin network IP**, **Admin network mask** e **Admin network gateway**.

b. Nella sezione **Client Network (eth2)**, selezionare STATIC (STATICO), DHCP (DHCP) o DISABLED (DISATTIVATO) per la configurazione **Client Network IP (IP di rete client)**.

- Se non si desidera utilizzare la rete client, selezionare DISABLED (DISATTIVATA) e immettere **0.0.0.0** come IP di rete client. È possibile lasciare vuoti gli altri campi.
- Se si seleziona STATIC (STATICO), inserire **Client network IP** (IP di rete client), **Client network mask** (maschera di rete client), **Client network gateway** e **Client network MTU**.
- Se si seleziona DHCP, vengono assegnati automaticamente **IP di rete client**, **maschera di rete client** e **gateway di rete client**.

8. Esaminare la configurazione della macchina virtuale e apportare le modifiche necessarie.
9. Quando si è pronti per il completamento, selezionare **fine** per avviare il caricamento della macchina virtuale.
10. se questo nodo è stato implementato come parte dell'operazione di recovery e non si tratta di un recovery a nodo completo, attenersi alla seguente procedura al termine dell'implementazione:

a. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Edit Settings** (Modifica impostazioni).

b. Selezionare ciascun disco rigido virtuale predefinito designato per lo storage e selezionare **Rimuovi**.

c. A seconda delle circostanze di ripristino dei dati, aggiungere nuovi dischi virtuali in base ai requisiti di storage, ricollegare eventuali dischi rigidi virtuali conservati dal nodo Grid guasto precedentemente rimosso o da entrambi.

Prendere nota delle seguenti importanti linee guida:

- Se si aggiungono nuovi dischi, è necessario utilizzare lo stesso tipo di dispositivo di storage utilizzato prima del ripristino del nodo.
- Il file .ovf del nodo di storage definisce diversi VMDK per lo storage. A meno che questi VMDK non soddisfino i requisiti di storage, è necessario rimuoverli e assegnare VMDK o RDM appropriati per lo storage prima di accendere il nodo. I VMDK sono più comunemente utilizzati negli ambienti VMware e sono più facili da gestire, mentre gli RDM potrebbero fornire performance migliori per i carichi di lavoro che utilizzano oggetti di dimensioni maggiori (ad esempio, superiori a 100 MB).

11. Se è necessario rimappare le porte utilizzate da questo nodo, attenersi alla seguente procedura.

Potrebbe essere necessario rimappare una porta se i criteri di rete aziendali limitano l'accesso a una o più porte utilizzate da StorageGRID. Vedere "linee guida per il networking" Per le porte utilizzate da StorageGRID.

> Non rimappare le porte utilizzate negli endpoint del bilanciamento del carico.

a. Selezionare la nuova VM.

b. Dalla scheda Configura, selezionare **Impostazioni** > **Opzioni vApp**. La posizione di **vApp Options** dipende dalla versione di vCenter.

c. Nella tabella **Proprietà**, individuare PORT_REMAP_INBOUND e PORT_REMAP.

d. Per mappare simmetricamente le comunicazioni in entrata e in uscita per una porta, selezionare **PORT_REMAP**.

> Se viene impostato solo PORT_REMAP, il mapping specificato si applica alle comunicazioni in entrata e in uscita. Se VIENE specificato anche PORT_REMAP_INBOUND, PORT_REMAP si applica solo alle comunicazioni in uscita.

i. Tornare alla parte superiore della tabella e selezionare **Modifica**.

ii. Nella scheda tipo, selezionare **configurabile dall'utente** e selezionare **Salva**.

iii. Selezionare **Imposta valore**.

iv. Inserire la mappatura delle porte:

`<network type>/<protocol>/<default port used by grid node>/<new port>`

`<network type>` è grid, admin o client, e. `<protocol>` è tcp o udp.

Ad esempio, per rimappare il traffico ssh dalla porta 22 alla porta 3022, immettere:

```
client/tcp/22/3022
```

i. Selezionare **OK**.

e. Per specificare la porta utilizzata per le comunicazioni in entrata al nodo, selezionare **PORT_REMAP_INBOUND**.

> Se si specifica PORT_REMAP_INBOUND e non si specifica un valore per PORT_REMAP, le comunicazioni in uscita per la porta rimangono invariate.

i. Tornare alla parte superiore della tabella e selezionare **Modifica**.

ii. Nella scheda tipo, selezionare **configurabile dall'utente** e selezionare **Salva**.

iii. Selezionare **Imposta valore**.

iv. Inserire la mappatura delle porte:

`<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>`

`<network type>` è grid, admin o client, e. `<protocol>` è tcp o udp.

Ad esempio, per rimappare il traffico SSH in entrata inviato alla porta 3022 in modo che venga ricevuto alla porta 22 dal nodo della rete, immettere quanto segue:

```
client/tcp/3022/22
```

i. Selezionare **OK**

12. Se si desidera aumentare la CPU o la memoria per il nodo dalle impostazioni predefinite:

a. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Edit Settings** (Modifica impostazioni).

b. Modificare il numero di CPU o la quantità di memoria secondo necessità.

Impostare **Memory Reservation** alle stesse dimensioni della **Memory** allocata alla macchina virtuale.

c. Selezionare **OK**.

13. Accendere la macchina virtuale.

Al termine

Se questo nodo è stato implementato come parte di una procedura di espansione o ripristino, tornare a queste istruzioni per completare la procedura.

Configurare la griglia e completare l'installazione (VMware)

Accedere a Grid Manager

Il Gestore griglia consente di definire tutte le informazioni necessarie per configurare il sistema StorageGRID.

Prima di iniziare

Il nodo di amministrazione primario deve essere implementato e aver completato la sequenza di avvio iniziale.

Fasi

1. Aprire il browser Web e accedere a uno dei seguenti indirizzi:

   `https://primary_admin_node_ip`

   `https://client_network_ip`

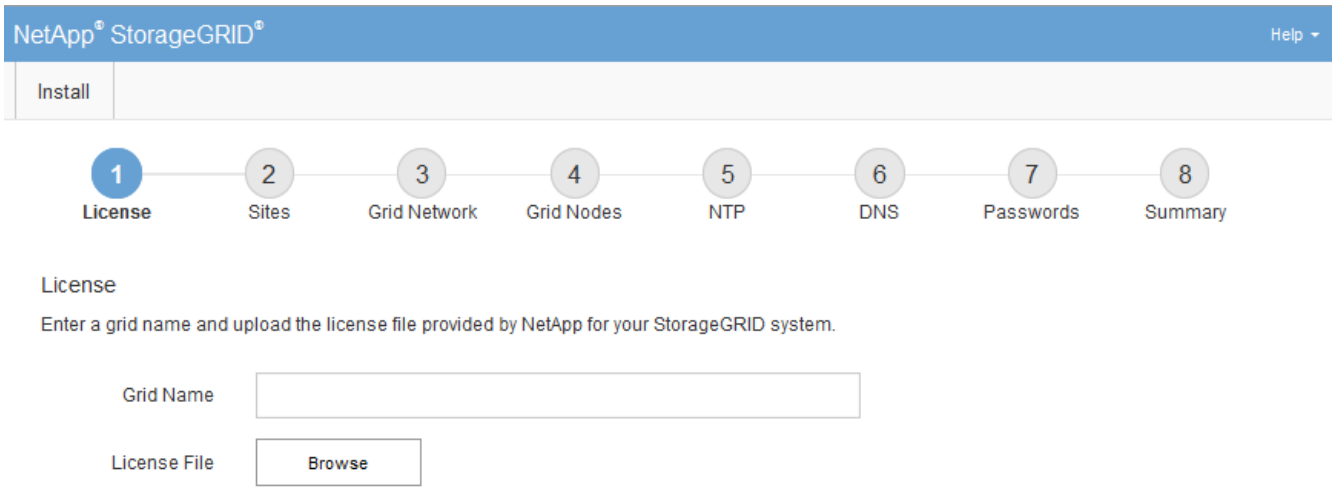
   In alternativa, è possibile accedere a Grid Manager dalla porta 8443:

   `https://primary_admin_node_ip:8443`

   > È possibile utilizzare l'indirizzo IP per l'indirizzo IP del nodo di amministrazione primario sulla rete griglia o sulla rete di amministrazione, a seconda della configurazione di rete. Potrebbe essere necessario utilizzare l'opzione Security/Advanced del browser per accedere a un certificato non attendibile.

2. Selezionare **Installa un sistema StorageGRID**.

   Viene visualizzata la pagina utilizzata per configurare una griglia StorageGRID.



Specificare le informazioni sulla licenza StorageGRID

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

Fasi

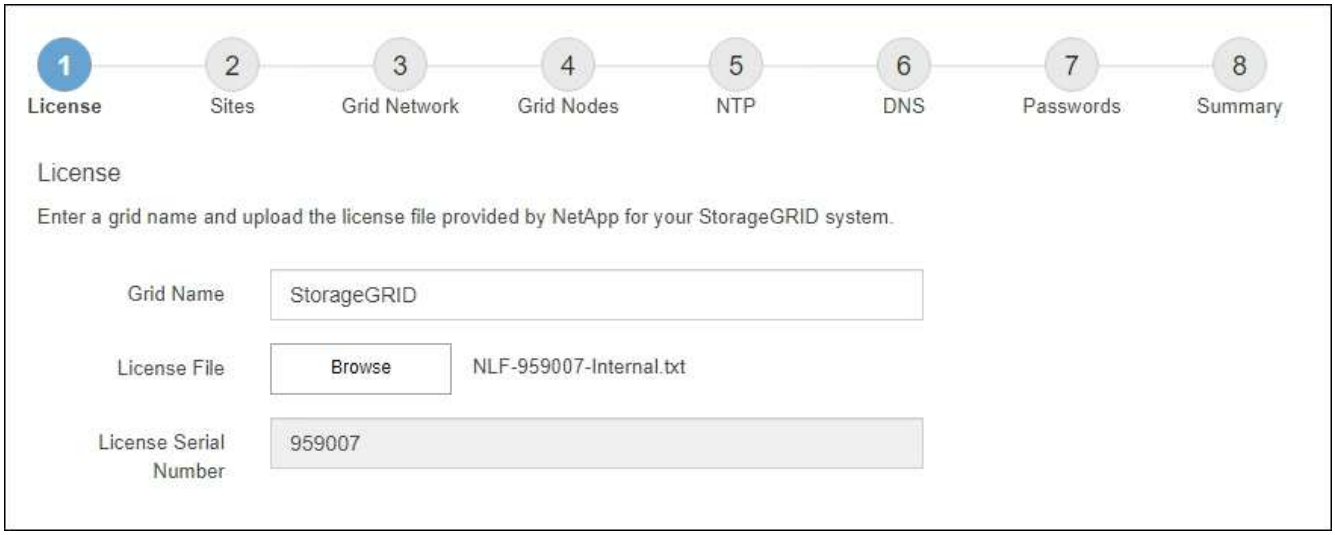
1. Nella pagina licenza, immettere un nome significativo per il sistema StorageGRID nel campo **Nome griglia**.

   Dopo l'installazione, il nome viene visualizzato nella parte superiore del menu Nodes (nodi).

2. Selezionare **Sfoglia**, individuare il file di licenza NetApp (`NLF-unique-id.txt`), quindi selezionare **Apri**.

   Il file di licenza viene validato e viene visualizzato il numero di serie.

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



3. Selezionare **Avanti**.

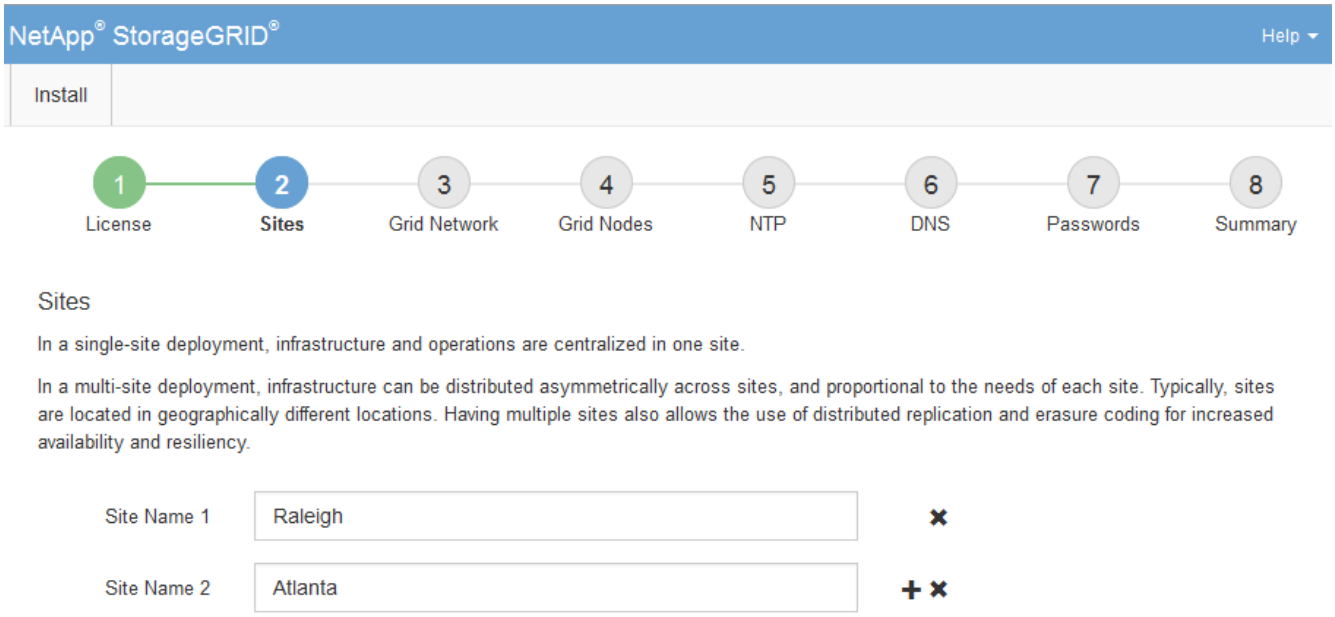
Aggiungere siti

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

Fasi

1. Nella pagina Siti, immettere il nome del sito *.
2. Per aggiungere altri siti, fare clic sul segno più accanto all'ultima voce del sito e inserire il nome nella nuova casella di testo **Nome sito**.

   Aggiungi tutti i siti aggiuntivi necessari per la topologia della griglia. È possibile aggiungere fino a 16 siti.



3. Fare clic su **Avanti**.

Specificare le subnet Grid Network

È necessario specificare le subnet utilizzate nella rete Grid.

A proposito di questa attività

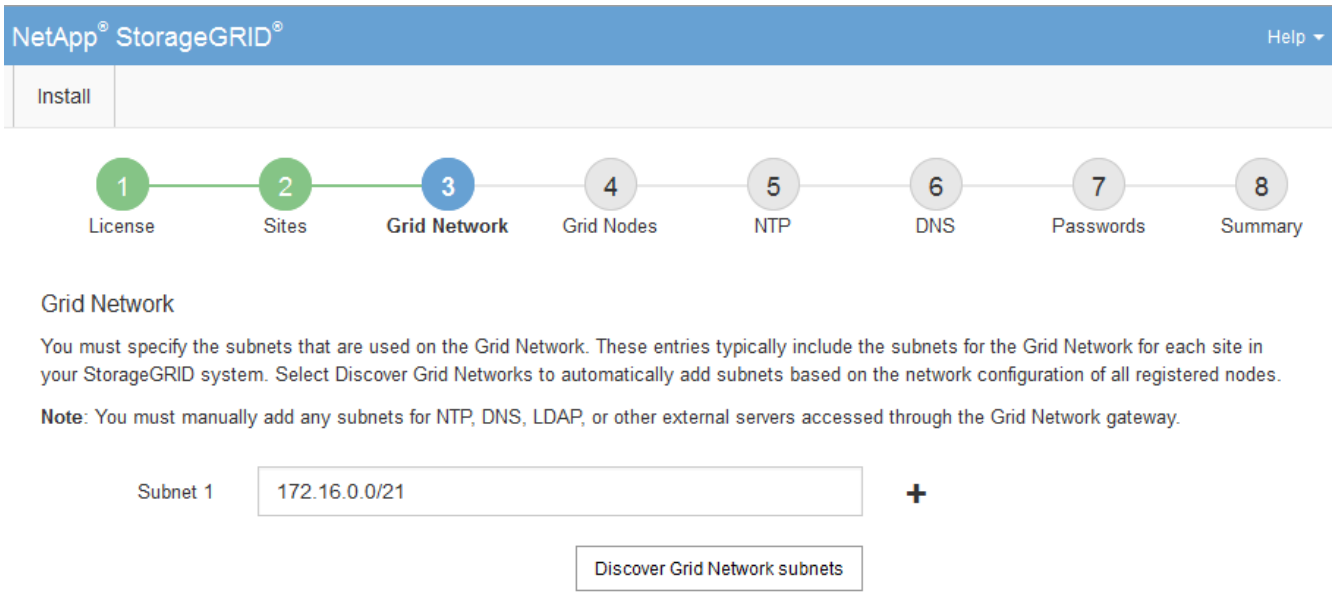
Le voci della subnet includono le subnet della rete di rete per ciascun sito del sistema StorageGRID, nonché le subnet che devono essere raggiungibili tramite la rete di rete.

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

Fasi

1. Specificare l'indirizzo di rete CIDR per almeno una rete griglia nella casella di testo **Subnet 1**.
2. Fare clic sul segno più accanto all'ultima voce per aggiungere una voce di rete aggiuntiva.

   Se è già stato implementato almeno un nodo, fare clic su **Discover Grid Networks Subnet** (rileva subnet Grid Network) per compilare automaticamente Grid Network Subnet List (elenco subnet Grid Network) con le subnet segnalate dai nodi Grid registrati con Grid Manager.



3. Fare clic su **Avanti**.

Approvare i nodi griglia in sospeso

È necessario approvare ciascun nodo della griglia prima che possa unirsi al sistema StorageGRID.

Prima di iniziare

Hai implementato tutti i nodi grid delle appliance virtuali e StorageGRID.

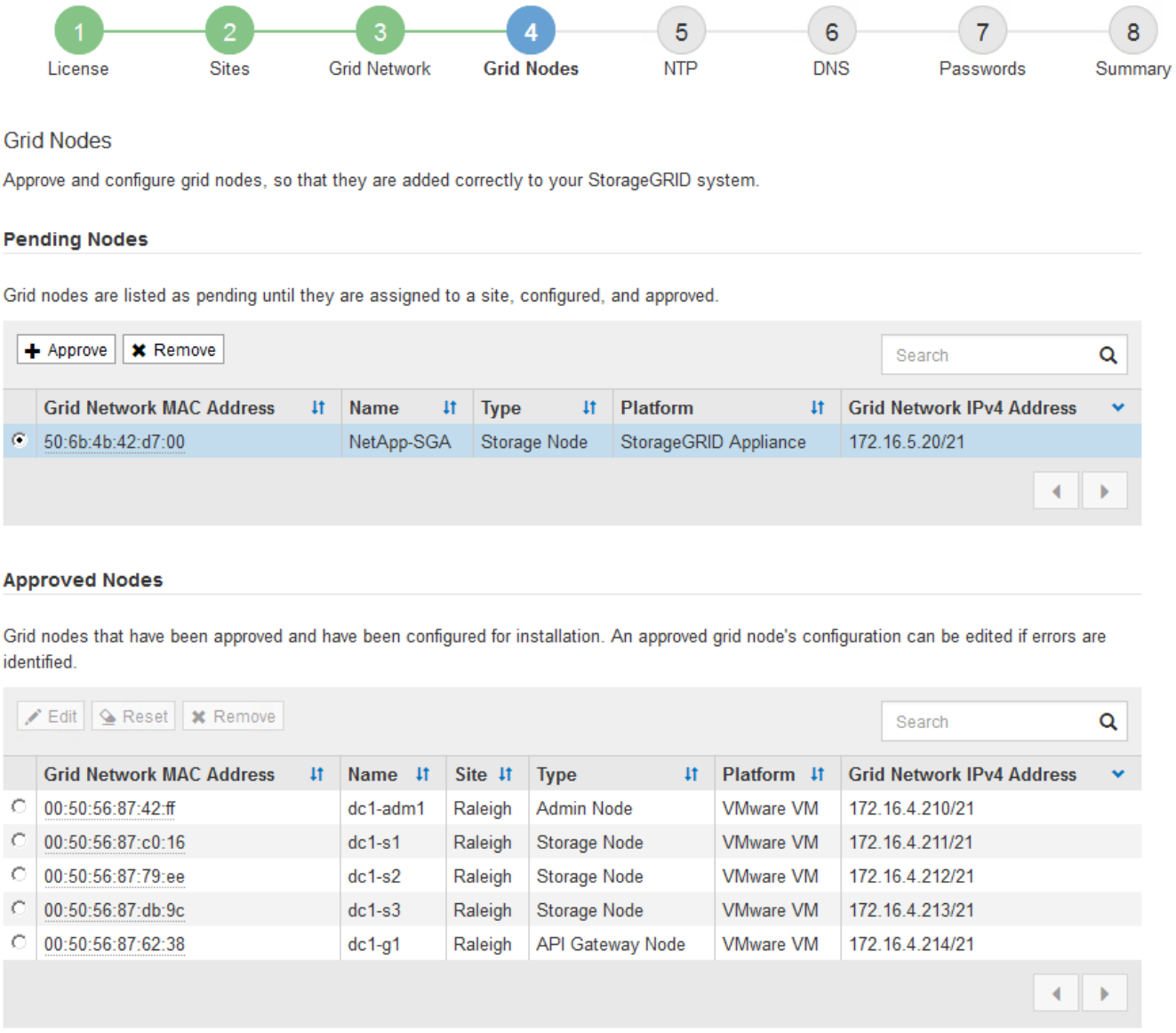
> È più efficiente eseguire una singola installazione di tutti i nodi, piuttosto che installare alcuni nodi ora e alcuni nodi successivamente.

Fasi

1. Esaminare l'elenco Pending Nodes (nodi in sospeso) e confermare che mostra tutti i nodi della griglia implementati.

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

2. Selezionare il pulsante di opzione accanto al nodo in sospeso che si desidera approvare.



3. Fare clic su **approva**.
4. In General Settings (Impostazioni generali), modificare le impostazioni per le seguenti proprietà, in base alle necessità:

   - **Sito**: Il nome di sistema del sito per questo nodo della griglia.
   - **Name**: Il nome del sistema per il nodo. Il nome predefinito corrisponde al nome specificato al momento della configurazione del nodo.

     I nomi di sistema sono necessari per le operazioni StorageGRID interne e non possono essere modificati dopo aver completato l'installazione. Tuttavia, durante questa fase del processo di installazione, è possibile modificare i nomi di sistema in base alle esigenze.

     Per un nodo VMware, è possibile modificare il nome qui, ma questa azione non cambierà il nome della macchina virtuale in vSphere.

   - **Ruolo NTP**: Ruolo NTP (Network Time Protocol) del nodo Grid. Le opzioni disponibili sono **automatico**, **primario** e **Client**. Selezionando **automatico**, il ruolo primario viene assegnato ai nodi di amministrazione, ai nodi di storage con servizi ADC, ai nodi gateway e a tutti i nodi di griglia che hanno

indirizzi IP non statici. A tutti gli altri nodi della griglia viene assegnato il ruolo Client.

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

- **Tipo di archiviazione** (solo nodi di archiviazione): Specificare che un nuovo nodo di archiviazione deve essere utilizzato esclusivamente per i metadati. Le opzioni sono **oggetti e metadati** e **solo metadati**. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

  > Quando si installa un grid con nodi solo metadati, il grid deve anche contenere un numero minimo di nodi per lo storage a oggetti. Per un grid a sito singolo, vengono configurati almeno due nodi storage per oggetti e metadati. Per un grid multisito, per gli oggetti e i metadati viene configurato almeno un nodo di storage per sito.

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

5. In Grid Network, modificare le impostazioni per le seguenti proprietà secondo necessità:

   - **IPv4 Address (CIDR)**: L'indirizzo di rete CIDR per l'interfaccia Grid Network (eth0 all'interno del container). Ad esempio: 192.168.1.234/21
   - **Gateway**: Il gateway Grid Network. Ad esempio: 192.168.0.1

     > Il gateway è necessario se sono presenti più subnet di rete.

   > Se si seleziona DHCP per la configurazione Grid Network e si modifica il valore, il nuovo valore verrà configurato come indirizzo statico sul nodo. Assicurarsi che l'indirizzo IP risultante non si trovi all'interno di un pool di indirizzi DHCP.

6. Se si desidera configurare la rete amministrativa per il nodo della griglia, aggiungere o aggiornare le impostazioni nella sezione rete amministrativa secondo necessità.

   Inserire le subnet di destinazione dei percorsi fuori da questa interfaccia nella casella di testo **subnet (CIDR)**. Se sono presenti più subnet Admin, è necessario il gateway Admin.

   > Se si seleziona DHCP per la configurazione Admin Network e si modifica il valore, il nuovo valore verrà configurato come indirizzo statico sul nodo. Assicurarsi che l'indirizzo IP risultante non si trovi all'interno di un pool di indirizzi DHCP.

   Appliance: per un'appliance StorageGRID, se la rete amministrativa non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione dell'appliance StorageGRID, non è possibile configurarla in questa finestra di dialogo. È invece necessario attenersi alla seguente procedura:

   a. Riavviare l'appliance: Nel programma di installazione dell'appliance, selezionare **Avanzate** > **Riavvia**.

      Il riavvio può richiedere alcuni minuti.

b. Selezionare **Configure Networking** > **link Configuration** (Configura rete) e abilitare le reti appropriate.
c. Selezionare **Configura rete** > **Configurazione IP** e configurare le reti abilitate.
d. Tornare alla Home page e fare clic su **Avvia installazione**.
e. In Grid Manager: Se il nodo è elencato nella tabella Approved Nodes (nodi approvati), rimuoverlo.
f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).
g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).
h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP del programma di installazione dell'appliance.

   Per ulteriori informazioni, consultare "Avvio rapido per l'installazione dell'hardware" per individuare le istruzioni relative all'apparecchio.

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

   > Se si seleziona DHCP per la configurazione di rete client e si modifica il valore, il nuovo valore verrà configurato come indirizzo statico sul nodo. Assicurarsi che l'indirizzo IP risultante non si trovi all'interno di un pool di indirizzi DHCP.

   Appliance: per un'appliance StorageGRID, se la rete client non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione dell'appliance StorageGRID, non è possibile configurarla in questa finestra di dialogo. È invece necessario attenersi alla seguente procedura:

   a. Riavviare l'appliance: Nel programma di installazione dell'appliance, selezionare **Avanzate** > **Riavvia**.

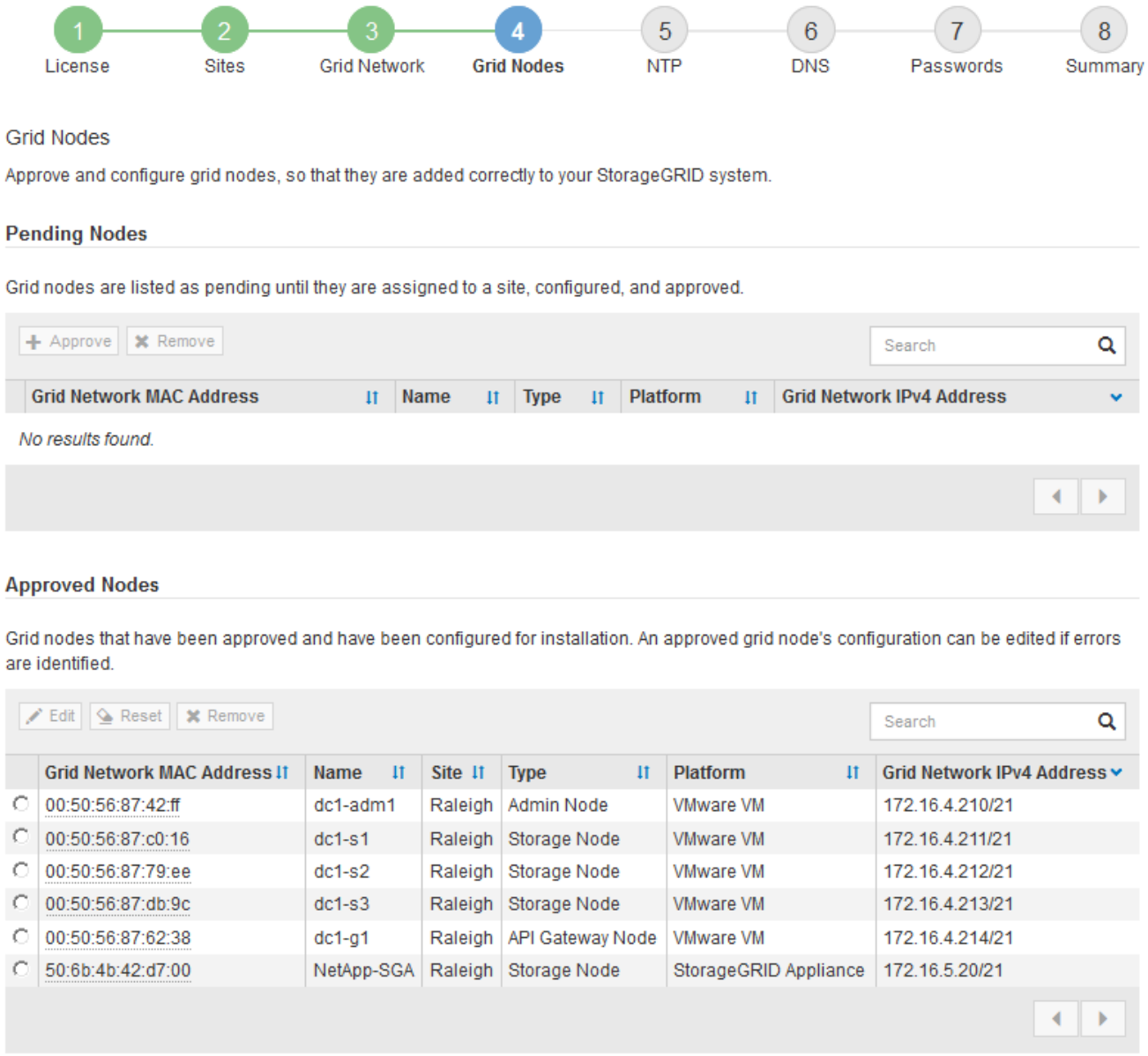
      Il riavvio può richiedere alcuni minuti.

   b. Selezionare **Configure Networking** > **link Configuration** (Configura rete) e abilitare le reti appropriate.
   c. Selezionare **Configura rete** > **Configurazione IP** e configurare le reti abilitate.
   d. Tornare alla Home page e fare clic su **Avvia installazione**.
   e. In Grid Manager: Se il nodo è elencato nella tabella Approved Nodes (nodi approvati), rimuoverlo.
   f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).
   g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).
   h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP del programma di installazione dell'appliance.

      Per ulteriori informazioni, consultare "Avvio rapido per l'installazione dell'hardware" per individuare le istruzioni relative all'apparecchio.

8. Fare clic su **Save** (Salva).

   La voce del nodo della griglia viene spostata nell'elenco dei nodi approvati.



9. Ripetere questi passaggi per ogni nodo griglia in sospeso che si desidera approvare.

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

10. Una volta completata l'approvazione dei nodi griglia, fare clic su **Avanti**.

Specificare le informazioni sul server Network Time Protocol

È necessario specificare le informazioni di configurazione del protocollo NTP (Network Time Protocol) per il sistema StorageGRID, in modo che le operazioni eseguite su server separati possano essere mantenute sincronizzate.

A proposito di questa attività

Specificare gli indirizzi IPv4 per i server NTP.

Specificare server NTP esterni. I server NTP specificati devono utilizzare il protocollo NTP.

È necessario specificare quattro riferimenti al server NTP di strato 3 o superiore per evitare problemi con la deriva del tempo.

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

"Supportare il limite per configurare il servizio Time di Windows per ambienti ad alta precisione"

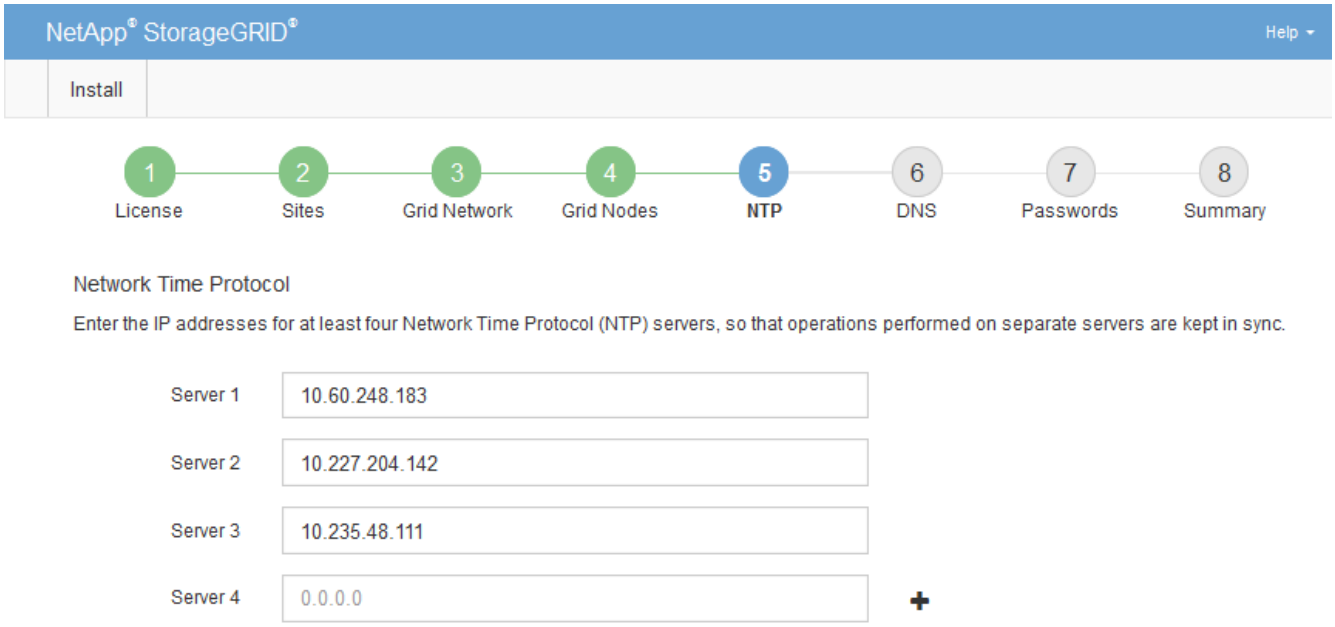
I server NTP esterni vengono utilizzati dai nodi ai quali sono stati precedentemente assegnati ruoli NTP primari.

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

Eseguire ulteriori controlli per VMware, ad esempio per assicurarsi che l'hypervisor utilizzi la stessa origine NTP della macchina virtuale e utilizzare VMTools per disattivare la sincronizzazione temporale tra l'hypervisor e le macchine virtuali StorageGRID.

Fasi

1. Specificare gli indirizzi IPv4 per almeno quattro server NTP nelle caselle di testo da **Server 1** a **Server 4**.
2. Se necessario, selezionare il segno più accanto all'ultima voce per aggiungere altre voci del server.



3. Selezionare **Avanti**.

Specificare le informazioni sul server DNS

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

A proposito di questa attività

Specificare "Informazioni sul server DNS" Consente di utilizzare nomi host FQDN (Fully Qualified Domain Name) piuttosto che indirizzi IP per le notifiche e-mail e AutoSupport.

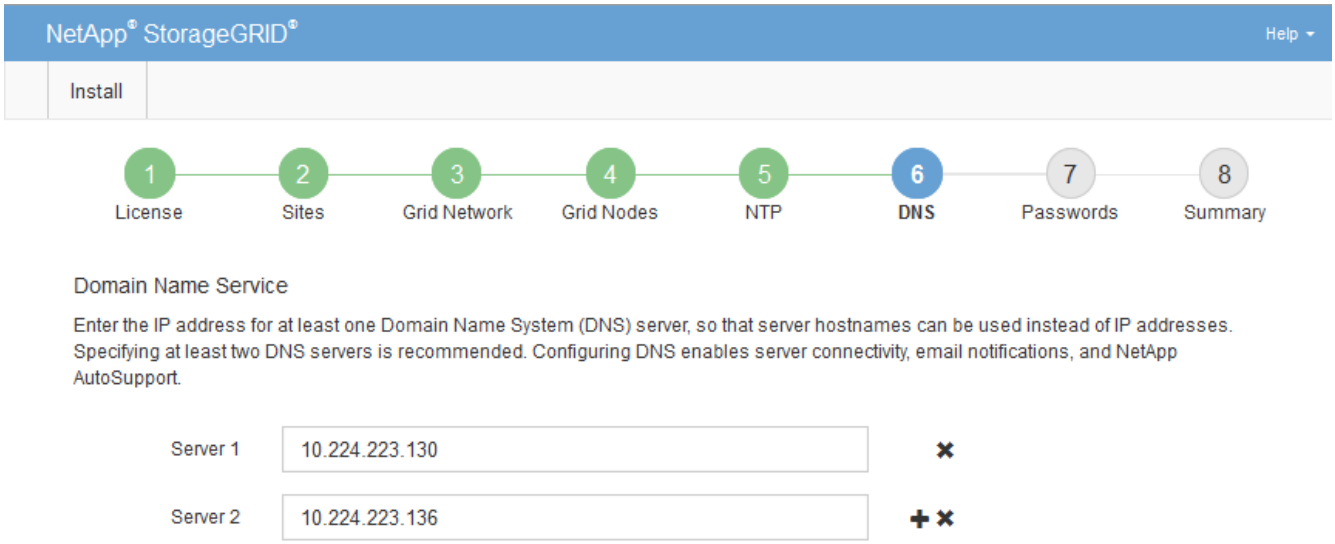
Per garantire il corretto funzionamento, specificare due o tre server DNS. Se si specificano più di tre, è possibile che ne vengano utilizzati solo tre a causa delle limitazioni del sistema operativo note su alcune piattaforme. Se nel proprio ambiente sono presenti restrizioni di routing, è possibile "Personalizzare l'elenco dei server DNS" Per i singoli nodi (in genere tutti i nodi di un sito) di utilizzare un set diverso di un massimo di tre server DNS.

Se possibile, utilizzare i server DNS a cui ciascun sito può accedere localmente per garantire che un sito islanded possa risolvere i FQDN per le destinazioni esterne.

Se le informazioni del server DNS vengono omesse o configurate in modo errato, viene attivato un allarme DNST sul servizio SSM di ciascun nodo della rete. L'allarme viene cancellato quando il DNS è configurato correttamente e le nuove informazioni sul server hanno raggiunto tutti i nodi della griglia.

Fasi

1. Specificare l'indirizzo IPv4 per almeno un server DNS nella casella di testo **Server 1**.
2. Se necessario, selezionare il segno più accanto all'ultima voce per aggiungere altre voci del server.



   Si consiglia di specificare almeno due server DNS. È possibile specificare fino a sei server DNS.

3. Selezionare **Avanti**.

Specificare le password di sistema di StorageGRID

Durante l'installazione del sistema StorageGRID, è necessario inserire le password da utilizzare per proteggere il sistema ed eseguire attività di manutenzione.

A proposito di questa attività

Utilizzare la pagina Installa password per specificare la passphrase di provisioning e la password utente root di gestione della griglia.

- La passphrase di provisioning viene utilizzata come chiave di crittografia e non viene memorizzata dal sistema StorageGRID.
- È necessario disporre della passphrase di provisioning per le procedure di installazione, espansione e manutenzione, incluso il download del pacchetto di ripristino. Pertanto, è importante memorizzare la passphrase di provisioning in una posizione sicura.
- È possibile modificare la passphrase di provisioning da Grid Manager, se si dispone di quella corrente.
- La password utente root della gestione della griglia può essere modificata utilizzando Grid Manager.
- Le password SSH e la console della riga di comando generate in modo casuale vengono memorizzate in `Passwords.txt` Nel pacchetto di ripristino.

Fasi

1. In **Provisioning Passphrase**, immettere la passphrase di provisioning necessaria per apportare modifiche alla topologia grid del sistema StorageGRID.

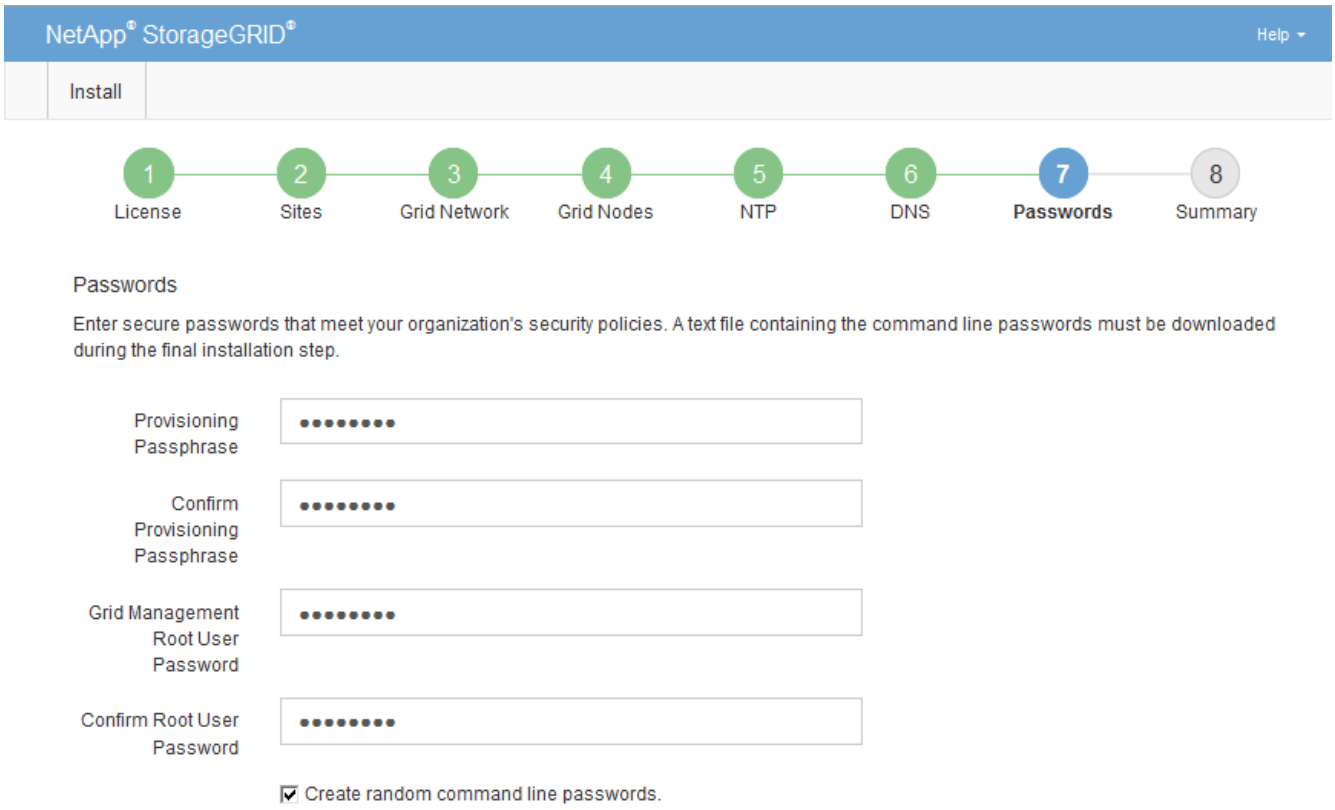
   Memorizzare la passphrase di provisioning in un luogo sicuro.

   > Se, al termine dell'installazione, si desidera modificare la passphrase di provisioning in un secondo momento, è possibile utilizzare Grid Manager. Selezionare **CONFIGURATION** > **Access control** > **Grid passwords**.

2. In **Confirm Provisioning Passphrase** (Conferma password di provisioning), immettere nuovamente la passphrase di provisioning per confermarla.
3. In **Grid Management Root User Password**, immettere la password da utilizzare per accedere al Grid Manager come utente "root".

   Memorizzare la password in un luogo sicuro.

4. In **Confirm Root User Password** (Conferma password utente root), immettere nuovamente la password di Grid Manager per confermarla.



5. Se si sta installando una griglia a scopo dimostrativo o dimostrativo, deselezionare la casella di controllo **Create random command line passwords** (Crea password della riga di comando casuale).

   Per le implementazioni in produzione, le password casuali devono essere sempre utilizzate per motivi di sicurezza. Cancella **Crea password casuali della riga di comando** solo per le griglie demo se desideri utilizzare password predefinite per accedere ai nodi della griglia dalla riga di comando utilizzando l'account "root" o "admin".

   > Viene richiesto di scaricare il file del pacchetto di ripristino (`sgws-recovery-package-id-revision.zip`) Dopo aver fatto clic su **Install** (Installa) nella pagina Summary (Riepilogo). È necessario "scarica questo file" per completare l'installazione. Le password richieste per accedere al sistema vengono memorizzate in `Passwords.txt` File, contenuto nel file del pacchetto di ripristino.

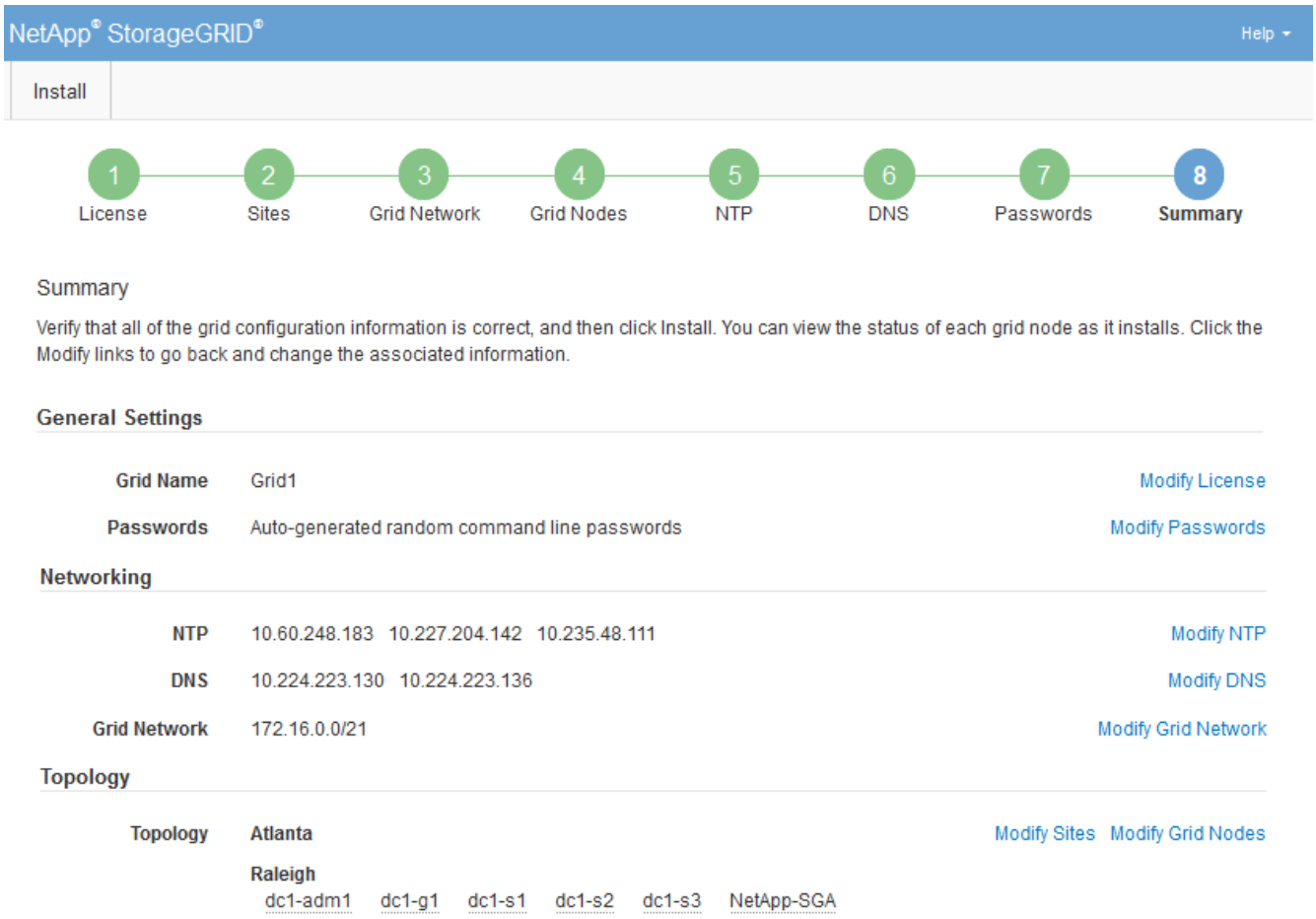
6. Fare clic su **Avanti**.

Esaminare la configurazione e completare l'installazione

È necessario esaminare attentamente le informazioni di configurazione inserite per assicurarsi che l'installazione venga completata correttamente.

Fasi

1. Visualizza la pagina **Riepilogo**.



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

> Se un nodo è configurato per utilizzare la rete client, il gateway predefinito per quel nodo passa dalla rete griglia alla rete client quando si fa clic su **Installa**. In caso di perdita della connettività, assicurarsi di accedere al nodo di amministrazione primario tramite una subnet accessibile. Vedere "Linee guida per il networking" per ulteriori informazioni.

4. Fare clic su **Download Recovery Package**.

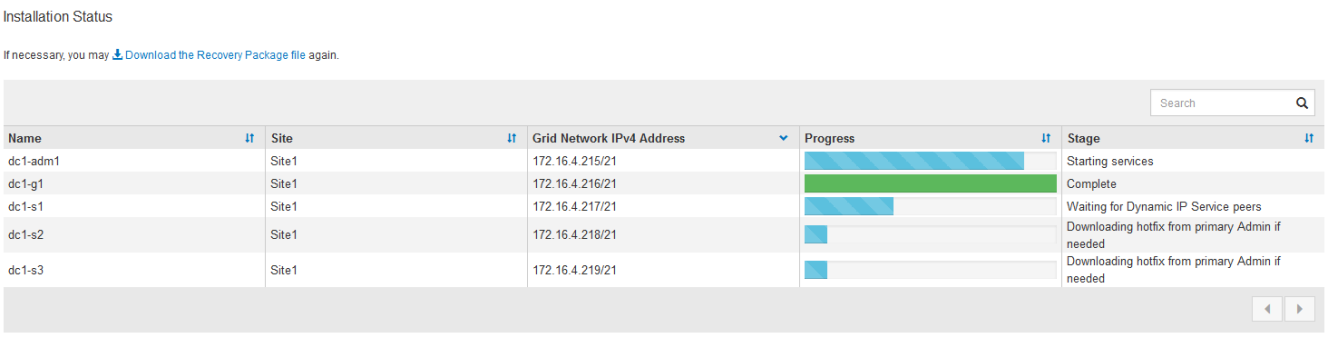
   Quando l'installazione prosegue fino al punto in cui è definita la topologia della griglia, viene richiesto di scaricare il file del pacchetto di ripristino (`.zip`) e confermare che sia possibile accedere al contenuto del file. È necessario scaricare il file del pacchetto di ripristino in modo da poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi griglia. L'installazione continua in background, ma non è possibile completare l'installazione e accedere al sistema StorageGRID fino a quando non si scarica e si verifica questo file.

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

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

6. Selezionare la casella di controllo **ho scaricato e verificato il file del pacchetto di ripristino** e fare clic su **Avanti**.

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



   Una volta raggiunta la fase completa per tutti i nodi della griglia, viene visualizzata la pagina di accesso per Grid Manager.

7. Accedere a Grid Manager utilizzando l'utente "root" e la password specificata durante l'installazione.

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. Impossibile 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.

Panoramica dell'API REST per l'installazione

StorageGRID fornisce l'API di installazione di StorageGRID per eseguire le attività di installazione.

L'API utilizza la piattaforma API open source Swagger per fornire la documentazione API. Swagger consente agli sviluppatori e ai non sviluppatori di interagire con l'API in un'interfaccia utente che illustra il modo in cui l'API risponde a parametri e opzioni. La presente documentazione presuppone che l'utente abbia familiarità con le tecnologie Web standard e il formato dati JSON.

Tutte le operazioni API eseguite utilizzando la pagina web API Docs sono operazioni live. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Ogni comando REST API include l'URL dell'API, un'azione HTTP, qualsiasi parametro URL richiesto o opzionale e una risposta API prevista.

API di installazione StorageGRID

L'API di installazione di StorageGRID è disponibile solo quando si configura inizialmente il sistema StorageGRID e se è necessario eseguire un ripristino primario del nodo di amministrazione. È possibile accedere all'API di installazione tramite HTTPS da Grid Manager.

Per accedere alla documentazione API, accedere alla pagina Web di installazione nel nodo di amministrazione principale e selezionare **Guida** > **documentazione API** dalla barra dei menu.

L'API di installazione di StorageGRID include le seguenti sezioni:

- **Config** — operazioni relative alla release del prodotto e alle versioni dell'API. È possibile elencare la versione di release del prodotto e le principali versioni dell'API supportate da tale release.
- **Grid** — operazioni di configurazione a livello di griglia. È possibile ottenere e aggiornare le impostazioni della griglia, inclusi i dettagli della griglia, le subnet Grid Network, le password della griglia e gli indirizzi IP dei server NTP e DNS.
- **Nodi** — operazioni di configurazione a livello di nodo. È possibile recuperare un elenco di nodi griglia, eliminare un nodo griglia, configurare un nodo griglia, visualizzare un nodo griglia e ripristinare la configurazione di un nodo griglia.
- **Provision** — operazioni di provisioning. È possibile avviare l'operazione di provisioning e visualizzare lo stato dell'operazione di provisioning.
- **Recovery** — operazioni di recovery del nodo di amministrazione principale. È possibile ripristinare le informazioni, caricare il pacchetto di ripristino, avviare il ripristino e visualizzare lo stato dell'operazione di ripristino.
- **Recovery-package** — operazioni per scaricare il pacchetto di ripristino.
- **Schemi** — schemi API per implementazioni avanzate
- **Siti** — operazioni di configurazione a livello di sito. È possibile creare, visualizzare, eliminare e modificare un sito.

Dove andare

Dopo aver completato un'installazione, eseguire le attività di integrazione e configurazione richieste. È possibile eseguire le attività opzionali in base alle necessità.

Attività richieste

- Configurare VMware vSphere Hypervisor per il riavvio automatico.

  È necessario configurare l'hypervisor per riavviare le macchine virtuali al riavvio del server. Senza un riavvio automatico, le macchine virtuali e i nodi della griglia rimangono spenti dopo il riavvio del server. Per ulteriori informazioni, consultare la documentazione di VMware vSphere Hypervisor.

- "Creare un account tenant" Per ogni protocollo client (Swift o S3) che verrà utilizzato per memorizzare gli oggetti nel sistema StorageGRID.

- "Controllare l'accesso al sistema" configurando gruppi e account utente. Se lo si desidera, è possibile "configurare un'origine di identità federata" (Ad esempio Active Directory o OpenLDAP), in modo da poter importare utenti e gruppi di amministrazione. In alternativa, è possibile "creare utenti e gruppi locali".
- Integrare e testare "API S3" oppure "API Swift" Applicazioni client che verranno utilizzate per caricare oggetti nel sistema StorageGRID.
- "Configurare le regole ILM (Information Lifecycle Management) e i criteri ILM" da utilizzare per proteggere i dati degli oggetti.
- Se l'installazione include nodi di storage dell'appliance, utilizzare SANtricity OS per completare le seguenti operazioni:
  - Connessione a ogni appliance StorageGRID.
  - Verificare la ricezione dei dati AutoSupport.

    Vedere "Configurare l'hardware".
- Esaminare e seguire "Linee guida per la protezione avanzata del sistema StorageGRID" eliminare i rischi per la sicurezza.
- "Configurare le notifiche e-mail per gli avvisi di sistema".
- Se il sistema StorageGRID include nodi di archiviazione (non più presenti), configurare la connessione del nodo di archiviazione al sistema di archiviazione esterno di destinazione.

Attività facoltative

- "Aggiornare gli indirizzi IP del nodo griglia" Se sono state modificate dopo la pianificazione dell'implementazione e la generazione del pacchetto di ripristino.
- "Configurare la crittografia dello storage", se necessario.
- "Configurare la compressione dello storage" ridurre le dimensioni degli oggetti memorizzati, se necessario.

Risolvere i problemi di installazione

Se si verificano problemi durante l'installazione del sistema StorageGRID, è possibile accedere ai file di log dell'installazione.

Di seguito sono riportati i principali file di log dell'installazione, che potrebbero essere necessari al supporto tecnico per risolvere i problemi.

- `/var/local/log/install.log` (trovato su tutti i nodi della griglia)
- `/var/local/log/gdu-server.log` (Trovato sul nodo di amministrazione primario)

Informazioni correlate

Per informazioni su come accedere ai file di registro, vedere "Riferimenti ai file di log".

Se hai bisogno di ulteriore assistenza, contatta "Supporto NetApp".

La prenotazione delle risorse delle macchine virtuali richiede una modifica

I file OVF includono una riserva di risorse progettata per garantire che ciascun nodo di griglia disponga di RAM e CPU sufficienti per funzionare in modo efficiente. Se si creano macchine virtuali implementando questi file OVF su VMware e il numero predefinito di risorse non è disponibile, le macchine virtuali non si avviano.

A proposito di questa attività

Se si è certi che l'host della macchina virtuale disponga di risorse sufficienti per ciascun nodo della griglia, regolare manualmente le risorse allocate per ciascuna macchina virtuale, quindi provare ad avviare le macchine virtuali.

Fasi

1. Nell'albero del client di VMware vSphere Hypervisor, selezionare la macchina virtuale non avviata.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Edit Settings** (Modifica impostazioni).-
3. Dalla finestra Virtual Machines Properties (Proprietà macchine virtuali), selezionare la scheda **Resources** (risorse).
4. Regolare le risorse allocate alla macchina virtuale:
   a. Selezionare **CPU**, quindi utilizzare il dispositivo di scorrimento Reservation (prenotazione) per regolare i MHz riservati per questa macchina virtuale.
   b. Selezionare **memoria**, quindi utilizzare il dispositivo di scorrimento prenotazione per regolare il MB riservato per questa macchina virtuale.
5. Fare clic su **OK**.
6. Ripetere la procedura secondo necessità per altre macchine virtuali ospitate sullo stesso host di macchine virtuali.

La password di installazione temporanea è stata disattivata

Quando si implementa un nodo VMware, è possibile specificare facoltativamente una password di installazione temporanea. È necessario disporre di questa password per accedere alla console VM o utilizzare SSH prima che il nuovo nodo si unisca alla griglia.

Se si è scelto di disattivare la password di installazione temporanea, è necessario eseguire ulteriori operazioni per eseguire il debug dei problemi di installazione.

È possibile effettuare una delle seguenti operazioni:

- Ridistribuire la VM ma specificare una password di installazione temporanea in modo da poter accedere alla console o utilizzare SSH per eseguire il debug dei problemi di installazione.
- Utilizzare vCenter per impostare la password:
  a. Vai su **VM**, seleziona la scheda **Configura** e seleziona **opzioni vApp**.
  b. Aggiornare **CUSTOM_TEMPORARY_PASSWORD** con il valore della password personalizzata o aggiornare **TEMPORARY_PASSWORD_TYPE** con il valore **use node name**.
  c. Riavviare la macchina virtuale per applicare la nuova password.

Aggiornare il software StorageGRID

Aggiornamento del software StorageGRID: Panoramica

Seguire queste istruzioni per aggiornare un sistema StorageGRID a una nuova release.

A proposito di queste istruzioni

Queste istruzioni descrivono le novità di StorageGRID 11,8 e forniscono istruzioni dettagliate per aggiornare tutti i nodi del sistema StorageGRID alla nuova versione.

Prima di iniziare

Esaminate questi argomenti per scoprire le nuove funzioni e i miglioramenti di StorageGRID 11,8, determinare se alcune funzioni sono state deprecate o rimosse e scoprire le modifiche alle API StorageGRID.

- "Novità di StorageGRID 11,8"
- "Funzionalità rimosse o obsolete"
- "Modifiche all'API Grid Management"
- "Modifiche all'API di gestione del tenant"

Novità di StorageGRID 11,8

Questa versione di StorageGRID introduce le seguenti funzionalità e modifiche funzionali.

Installazione, aggiornamento, hotfix

Password di installazione temporanea

Quando vuoi "Implementare un nodo StorageGRID come macchina virtuale" Oppure utilizza VMware vSphere per "automatizzare l'implementazione dei nodi grid", viene ora richiesto di impostare una password di installazione temporanea. Questa password viene utilizzata solo se è necessario accedere alla console della macchina virtuale o utilizzare SSH prima che il nuovo nodo si unisca alla griglia.

Appliance

Sito della documentazione per le apparecchiature

La documentazione per le appliance StorageGRID è stata spostata in una nuova "sito della documentazione relativa alle apparecchiature".

Supporto FIPS

Supporto per la crittografia validata FIPS 140-2.

SGF6112 miglioramenti

Supporto per StorageGRID 11,8 e StorageGRID Appliance Installer versione firmware 3.8.0:

- Miglioramento significativo delle prestazioni di MESSA per le nuove installazioni SGF6112.
- Avvio protetto UEFI su nodi SGF6112 aggiornati e nuovi.
- Gestore delle chiavi locale per le password delle unità SSD DAS NVMe.

Configurare e gestire

Impostazione predefinita per l'intera griglia di coerenza

È possibile modificare "coerenza predefinita a livello di griglia" Utilizzando il Grid Manager o l'endpoint grid-config di "API privata di Grid Management". Il nuovo default verrà applicato ai bucket creati dopo la modifica.

Destinazioni di controllo predefinite

Le nuove installazioni di StorageGRID 11,8 sono predefinite per le destinazioni di controllo dei nodi locali. In precedenza, i messaggi di controllo venivano inviati al registro di controllo (`/var/local/log/audit.log`) solo sui nodi Admin.

Per informazioni sulla modifica delle destinazioni del registro di controllo, fare riferimento alla sezione "Selezionare le destinazioni delle informazioni di audit".

Tag dei criteri ILM

Consente il controllo delle policy ILM per bucket con etichette bucket. Possono esistere più criteri ILM attivi e inattivi contemporaneamente. Vedere "Criteri ILM: Panoramica".

Endpoint Kafka

Supporto per endpoint Kafka per "notifiche eventi bucket".

Bilanciamento del carico per il traffico delle interfacce di gestione

Creare endpoint di bilanciamento del carico per gestire il carico di lavoro dell'interfaccia di gestione sui nodi amministrativi. Vedere "considerazioni per il bilanciamento del carico". Come parte di questa modifica, è ora possibile utilizzare le porte 443, 8443 e 9443 di Grid Manager e Tenant Manager quando si creano endpoint di bilanciamento del carico HTTPS per l'accesso client S3 o Swift.

Scheda Gestisci unità

Aggiunto "Scheda Gestisci unità" Per l'apparecchio SGF6112.

Nodi di storage solo metadati

È ora possibile specificare un nuovo "Nodo storage basato su software" verranno utilizzati per memorizzare solo i metadati al posto degli oggetti e dei metadati.

SSO supporta i nomi principali degli utenti

Quando "Configurazione SSO (Single Sign-on)" Per Active Directory Federation Service (ad FS) o PingFederate, è ora possibile mappare il nome principale utente a. `Name ID` nella regola delle richieste di rimborso o a. `sAMAccountName=${username}` nell'istanza della scheda.

Configurazione delle policy TLS e supporto KMIP

- StorageGRID ora supporta il protocollo TLS 1,2 o TLS 1,3 per le connessioni KMIP. Vedere "Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi".
- "Hashicorp è ora completamente supportato per KMIP".
- Sono stati apportati miglioramenti a. "Configurazione dei criteri TLS".

Espandi il grid, mantieni la grid, ripristina o sostituisci i nodi

Miglioramento dei cloni degli account

Gli account esistenti possono essere clonati in una griglia remota. Vedere "Cos'è il clone dell'account".

I nodi di archivio possono essere dismessi

È ora possibile utilizzare la procedura nodi di decompressione per rimuovere tutti i nodi di archiviazione non utilizzati che sono disconnessi dalla griglia. Vedere "Decommissionare nodi di rete disconnessi".

> I nodi di archivio sono stati deprecati in StorageGRID 11,7.

Ripristino automatico del volume

È stato aggiunto un interruttore per il ripristino automatico del volume. Vedere "Ripristinare i dati degli oggetti utilizzando Grid Manager".

Erasure coding, modifiche alle configurazioni e procedura di ribilanciamento

Miglioramenti alle configurazioni di erasure coding.

Ridistribuzione dei frammenti sottoposti a erasure coding tra i nodi storage nuovi ed esistenti. Ricalcolare il bilanciamento durante le attività di manutenzione per fornire una distribuzione migliore al termine delle attività. Vedere "Procedura di ribilanciamento dell'erasure coding".

Traccia stack API di gestione

L'impostazione di protezione **Management API Stack Trace** consente di controllare se una traccia stack viene restituita nelle risposte agli errori di Grid Manager e Tenant Manager API. Vedere "Modificare le impostazioni di sicurezza dell'interfaccia".

Procedura di riavvio in sequenza

È ora possibile utilizzare "procedura di riavvio in sequenza" per riavviare più nodi grid senza causare un'interruzione del servizio.

Grid Manager

Reti client non attendibili, informazioni sulle porte aggiuntive

L'elenco delle porte aperte alla rete client non attendibile di Grid Manager si trova ora in una colonna denominata "Apri a rete client non attendibile" in **CONFIGURAZIONE** > **rete** > **endpoint del bilanciamento del carico** > **interfaccia di gestione** (precedentemente situata nella pagina di controllo del firewall). Vedere "Configurare gli endpoint del bilanciamento del carico".

Manager tenant

S3 Console non più sperimentale

Funzionalità aggiuntive descritte in "Utilizzare la console S3".

Permesso tenant

Il "autorizzazione gestione tenant", È stato aggiunto Visualizza tutti i bucket.

API REST S3

- "Modifiche al supporto delle API REST S3".
- S3 eliminare i marcatori con UUID. Vedere "Modalità di eliminazione degli oggetti" e. "SDEL: ELIMINAZIONE S3".
- "S3 selezionare ScanRange" Viene utilizzato quando viene fornito nelle richieste di file CSV e Parquet.

Funzioni e funzionalità rimosse o obsolete

Alcune funzioni e funzionalità sono state rimosse o obsolete in questa release. Esaminare questi elementi per capire se è necessario aggiornare le applicazioni client o modificare la configurazione prima di eseguire l'aggiornamento.

Definizioni

Obsoleto

La funzione **non deve** essere utilizzata in nuovi ambienti di produzione. Gli ambienti di produzione esistenti possono continuare a utilizzare questa funzione.

Fine del ciclo di vita

Ultima versione fornita che contiene la funzione. Nessuna versione futura supporterà la funzione.

Rimosso

Prima versione che **non** contiene la funzione.

Fine del supporto delle funzionalità di StorageGRID 11,8

Le funzioni obsolete verranno rimosse nelle versioni principali N+2. Ad esempio, se una funzione è deprecata nella versione N (ad esempio, 6,3), l'ultima versione in cui la funzione esisterà è N+1 (ad esempio, 6,4). La versione N+2 (ad esempio, 6,5) è la prima versione quando la funzione non esiste nel prodotto.

Vedere "Pagina supporto versione software" per ulteriori informazioni.

> In alcune situazioni, NetApp potrebbe interrompere il supporto per determinate funzioni prima di quanto indicato.

Funzione	Obsoleto	Fine del ciclo di vita	Rimosso
Supporto nodo di archivio	11,7	11,8	11,9
Esportazione di audit tramite CIFS/Samba	11,1	11,6	11,7
Servizio CLB	11,4	11,6	11,7
Runtime dei container Docker	11,8	11,9	12,0
Esportazione con audit NFS	11,8	11,9	12,0
Supporto API Swift	11,7	11,9	12,0

Modifiche all'API Grid Management

StorageGRID 11,8 utilizza la versione 4 dell'API di gestione delle griglie. La versione 4 depreca la versione 3; tuttavia, le versioni 1, 2 e 3 sono ancora supportate.

> È possibile continuare a utilizzare versioni obsolete dell'API di gestione con StorageGRID 11,8; tuttavia, il supporto per queste versioni dell'API verrà rimosso in una versione futura di StorageGRID. Dopo l'aggiornamento a StorageGRID 11,8, è possibile disattivare le API obsolete utilizzando `PUT /grid/config/management` API.

Per ulteriori informazioni, visitare il sito Web all'indirizzo "Utilizzare l'API Grid Management".

Modifiche per `ilm-policies` API v4

A partire da StorageGRID 11,8, versione 4 di `ilm-policies` API contiene le seguenti differenze rispetto alla versione 3:

- I criteri storici non vengono più restituiti. È stata aggiunta una nuova API separata per ottenere i dati dei criteri storici e dei tag in `/grid/ilm-history`.
- Proprietà rimosse: `proposed`, `historical`, `historicalRules`, `activationTime`.
- Proprietà aggiunte: `active` (booleano), `activatedBy` (Matrice di UUID tag a cui è assegnato il criterio).
- Parametro di query di tipo opzionale per `GET ilm-policies` ora prende i valori `inactive` e. `active`. I valori precedenti erano `proposed`, `active`, e. `historical`.

Nuovi endpoint per la gestione dei dischi

È possibile utilizzare gli endpoint dell'API **/grid/drive-details/{NodeID}** per eseguire operazioni sulle unità in modelli specifici di nodi di storage dell'appliance.

Modifiche all'API di gestione del tenant

StorageGRID 11,8 utilizza la versione 4 dell'API di gestione dei tenant. La versione 4 depreca la versione 3; tuttavia, le versioni 1, 2 e 3 sono ancora supportate.

> È possibile continuare a utilizzare le versioni obsolete dell'API di gestione dei tenant con StorageGRID 11,8; tuttavia, il supporto per queste versioni dell'API verrà rimosso in una versione futura di StorageGRID. Dopo l'aggiornamento a StorageGRID 11,8, è possibile disattivare le API obsolete utilizzando `PUT /grid/config/management` API.

Per ulteriori informazioni, visitare il sito Web all'indirizzo "Comprendere l'API di gestione dei tenant".

Nuovi endpoint per i tag dei criteri ILM

È possibile utilizzare gli endpoint dell'API **/org/ilm-policy-tags** e **/org/containers/{bucketName}/ilm-policy-tags** per eseguire operazioni correlate ai tag dei criteri ILM.

Pianificare e prepararsi per l'upgrade

Stima del tempo necessario per completare un aggiornamento

Considerare quando eseguire l'aggiornamento, in base alla durata dell'aggiornamento. È importante sapere quali operazioni è possibile e non è possibile eseguire in ciascuna fase dell'aggiornamento.

A proposito di questa attività

Il tempo necessario per completare un aggiornamento di StorageGRID dipende da una varietà di fattori, come il carico del client e le performance dell'hardware.

La tabella riassume le principali attività di aggiornamento ed elenca il tempo approssimativo necessario per ciascuna attività. I passaggi successivi alla tabella forniscono le istruzioni da utilizzare per stimare il tempo di aggiornamento del sistema.

Attività di upgrade	Descrizione	Tempo approssimativo richiesto	Durante questa attività
Eseguire i controlli preliminari e aggiornare il nodo di amministrazione primario	Vengono eseguiti i controlli preliminari per l'aggiornamento e il nodo di amministrazione primario viene arrestato, aggiornato e riavviato.	da 30 minuti a 1 ora, con nodi di appliance di assistenza che richiedono la maggior parte del tempo. Gli errori di pre-controllo non risolti aumenteranno questo tempo.	Impossibile accedere al nodo di amministrazione primario. Potrebbero essere segnalati errori di connessione che è possibile ignorare. L'esecuzione dei controlli preliminari per l'aggiornamento prima di avviare l'aggiornamento consente di risolvere eventuali errori prima della finestra di manutenzione pianificata per l'aggiornamento.
Avviare il servizio di aggiornamento	Il file software viene distribuito e il servizio di aggiornamento viene avviato.	3 minuti per nodo di rete	
Aggiornare altri nodi grid	Il software su tutti gli altri nodi griglia viene aggiornato nell'ordine in cui vengono approvati i nodi. Ogni nodo del sistema verrà spento uno alla volta.	da 15 minuti a 1 ora per nodo, con nodi appliance che richiedono il maggior numero di tempo **Nota**: Per i nodi appliance, il programma di installazione dell'appliance StorageGRID viene aggiornato automaticamente alla versione più recente.	• Non modificare la configurazione della griglia. • Non modificare la configurazione del livello di audit. • Non aggiornare la configurazione ILM. • Non è possibile eseguire altre procedure di manutenzione, ad esempio hotfix, decommissionare o espandere. **Nota**: Per eseguire un ripristino, contattare il supporto tecnico.
Abilitare le funzioni	Le nuove funzioni della nuova versione sono attivate.	Meno di 5 minuti	• Non modificare la configurazione della griglia. • Non modificare la configurazione del livello di audit. • Non aggiornare la configurazione ILM. • Non è possibile eseguire un'altra procedura di manutenzione.

Attività di upgrade	Descrizione	Tempo approssimativo richiesto	Durante questa attività
Aggiornare il database	Il processo di aggiornamento controlla ciascun nodo per verificare che il database Cassandra non debba essere aggiornato.	10 secondi per nodo o pochi minuti per l'intera griglia	L'upgrade da StorageGRID 11,7 a 11,8 non richiede un aggiornamento del database Cassandra; tuttavia, il servizio Cassandra verrà arrestato e riavviato su ogni nodo storage. Per le future versioni delle funzionalità di StorageGRID, il completamento della fase di aggiornamento del database Cassandra potrebbe richiedere diversi giorni.
Fasi finali dell'upgrade	I file temporanei vengono rimossi e l'aggiornamento alla nuova release viene completato.	5 minuti	Una volta completata l'attività **fasi finali dell'aggiornamento**, è possibile eseguire tutte le procedure di manutenzione.

Fasi

1. Stima del tempo necessario per l'aggiornamento di tutti i nodi della griglia.
   a. Moltiplicare il numero di nodi nel sistema StorageGRID per 1 ora/nodo.

      Come regola generale, l'aggiornamento dei nodi appliance richiede più tempo rispetto ai nodi basati su software.

   b. Aggiungere 1 ora a questo intervallo di tempo per tenere conto del tempo necessario per scaricare `.upgrade` archiviare, eseguire le validazioni di pre-controllo e completare le fasi finali dell'aggiornamento.
2. Se si dispone di nodi Linux, aggiungere 15 minuti per ciascun nodo per tenere conto del tempo necessario per scaricare e installare il pacchetto RPM o DEB.
3. Calcola il tempo totale stimato per l'aggiornamento aggiungendo i risultati dei passaggi 1 e 2.

Esempio: Tempo stimato per l'aggiornamento a StorageGRID 11,8

Si supponga che il sistema disponga di 14 nodi grid, di cui 8 nodi Linux.

1. Moltiplicare 14 per 1 ora/nodo.
2. Aggiungere 1 ora per tenere conto del download, del controllo preliminare e dei passaggi finali.

   Il tempo stimato per l'aggiornamento di tutti i nodi è di 15 ore.

3. Moltiplicare 8 per 15 minuti/nodo per il tempo di installazione del pacchetto RPM o DEB sui nodi Linux.

   Il tempo stimato per questa fase è di 2 ore.

4. Sommare i valori.

   Sono necessarie fino a 17 ore per completare l'aggiornamento del sistema a StorageGRID 11,8.0.

Se necessario, è possibile dividere la finestra di manutenzione in finestre più piccole approvando i sottoinsiemi di nodi della griglia da aggiornare in più sessioni. Ad esempio, si consiglia di aggiornare i nodi nel sito A in una sessione e quindi aggiornare i nodi nel sito B in una sessione successiva. Se si sceglie di eseguire l'aggiornamento in più sessioni, tenere presente che non è possibile iniziare a utilizzare le nuove funzionalità fino a quando tutti i nodi non sono stati aggiornati.

Impatto del sistema durante l'aggiornamento

Scopri in che modo il tuo sistema StorageGRID sarà influenzato durante l'aggiornamento.

Gli aggiornamenti di StorageGRID sono senza interruzioni

Il sistema StorageGRID è in grado di acquisire e recuperare i dati dalle applicazioni client durante l'intero processo di aggiornamento. Se si approvano tutti i nodi dello stesso tipo per l'aggiornamento (ad esempio, i nodi di storage), i nodi vengono disattivati uno alla volta, in modo che non vi sia tempo in cui tutti i nodi di griglia o tutti i nodi di griglia di un determinato tipo non siano disponibili.

Per consentire la disponibilità continua, assicurarsi che il criterio ILM contenga regole che specificano la memorizzazione di più copie di ciascun oggetto. È inoltre necessario assicurarsi che tutti i client S3 o Swift esterni siano configurati per inviare richieste a uno dei seguenti:

- Un indirizzo IP virtuale del gruppo ad alta disponibilità (ha)
- Bilanciamento del carico di terze parti ad alta disponibilità
- Nodi gateway multipli per ogni client
- Più nodi di storage per ogni client

Le applicazioni client potrebbero riscontrare interruzioni a breve termine

Il sistema StorageGRID può acquisire e recuperare i dati dalle applicazioni client durante tutto il processo di upgrade, tuttavia le connessioni client a singoli nodi di gateway o nodi storage potrebbero essere temporaneamente interrotte se l'upgrade deve riavviare i servizi su tali nodi. La connettività viene ripristinata al termine del processo di upgrade e i servizi vengono ripristinati nei singoli nodi.

Potrebbe essere necessario pianificare i tempi di inattività per applicare un aggiornamento se la perdita di connettività per un breve periodo non è accettabile. È possibile utilizzare l'approvazione selettiva per pianificare l'aggiornamento di determinati nodi.

È possibile utilizzare più gateway e gruppi di alta disponibilità (ha) per fornire il failover automatico durante il processo di upgrade. Consultare le istruzioni per "configurazione di gruppi ad alta disponibilità".

Il firmware dell'appliance viene aggiornato

Durante l'aggiornamento a StorageGRID 11,8:

- Tutti i nodi di appliance StorageGRID vengono aggiornati automaticamente alla versione 3,8 del firmware del programma di installazione dell'appliance StorageGRID.
- Le appliance SG6060 e SGF6024 vengono automaticamente aggiornate alla versione del firmware del BIOS 3B07.EX e al firmware BMC versione 3.99.07.
- Le appliance SG100 e SG1000 vengono aggiornate automaticamente alla versione del firmware del BIOS

3B12.EC e al firmware BMC versione 4.73.07.

- L'appliance SGF6112 viene aggiornata automaticamente alla versione del firmware del BIOS 3A10.QD e al firmware BMC versione 3.15.07.
- SGF6112 viene convertito dalla modalità di avvio legacy alla modalità di avvio UEFI con l'avvio protetto abilitato.
- Le appliance SG110 e SG1100 sono state fornite con il firmware del BIOS compatibile con StorageGRID 11,8.

Le policy ILM vengono gestite in modo diverso in base al loro stato

- Il criterio attivo rimane lo stesso dopo l'aggiornamento.
- Solo le ultime 10 politiche storiche vengono mantenute al momento dell'aggiornamento.
- Se esiste una policy proposta, verrà eliminata durante l'aggiornamento.

Potrebbero essere attivati degli avvisi

Gli avvisi potrebbero essere attivati all'avvio e all'arresto dei servizi e quando il sistema StorageGRID funziona come ambiente a versione mista (alcuni nodi di griglia che eseguono una versione precedente, mentre altri sono stati aggiornati a una versione successiva). Al termine dell'aggiornamento potrebbero essere attivati altri avvisi.

Ad esempio, potrebbe essere visualizzato l'avviso **Impossibile comunicare con il nodo** quando i servizi vengono arrestati, oppure potrebbe essere visualizzato l'avviso **errore di comunicazione Cassandra** quando alcuni nodi sono stati aggiornati a StorageGRID 11,8 ma altri nodi eseguono ancora StorageGRID 11,7. In generale, questi avvisi verranno visualizzati al termine dell'aggiornamento.

L'avviso **posizionamento ILM non raggiungibile** potrebbe essere attivato quando i nodi di archiviazione vengono arrestati durante l'aggiornamento a StorageGRID 11,8. Questo avviso potrebbe persistere per 1 giorno dopo il completamento dell'aggiornamento.

Una volta completato l'aggiornamento, è possibile rivedere gli avvisi relativi all'aggiornamento selezionando **Avvisi risolti di recente** o **Avvisi correnti** dalla dashboard di Grid Manager.

Vengono generate molte notifiche SNMP

Tenere presente che è possibile che vengano generate numerose notifiche SNMP quando i nodi della griglia vengono arrestati e riavviati durante l'aggiornamento. Per evitare notifiche eccessive, deselezionare la casella di controllo **Enable SNMP Agent Notifications** (**CONFIGURATION** > **Monitoring** > **SNMP Agent**) per disattivare le notifiche SNMP prima di avviare l'aggiornamento. Quindi, riattivare le notifiche al termine dell'aggiornamento.

Le modifiche alla configurazione sono limitate

> Questo elenco si applica in particolare agli aggiornamenti da StorageGRID 11,7 a StorageGRID 11,8. Se si esegue l'aggiornamento a un'altra release di StorageGRID, fare riferimento all'elenco delle modifiche limitate nelle istruzioni di aggiornamento per tale release.

Fino al completamento dell'attività **Enable New Feature**:

- Non apportare modifiche alla configurazione della griglia.
- Non attivare o disattivare nuove funzioni.

- Non aggiornare la configurazione ILM. In caso contrario, potrebbe verificarsi un comportamento ILM inconsistente e imprevisto.
- Non applicare una correzione rapida o ripristinare un nodo della griglia.

> Contattare il supporto tecnico se è necessario ripristinare un nodo durante l'aggiornamento.

- Durante l'aggiornamento a StorageGRID 11,8, non è necessario gestire gruppi ha, interfacce VLAN o endpoint di bilanciamento del carico.
- Non eliminare alcun gruppo ha fino al completamento dell'aggiornamento a StorageGRID 11,8. Gli indirizzi IP virtuali in altri gruppi ha potrebbero diventare inaccessibili.

Fino al completamento dell'attività **fasi finali dell'aggiornamento**:

- Non eseguire una procedura di espansione.
- Non eseguire una procedura di decommissionamento.

Non puoi visualizzare i dettagli del bucket o gestire i bucket dal tenant Manager

Durante l'aggiornamento a StorageGRID 11,8 (ovvero quando il sistema funziona come un ambiente in versione mista), non è possibile visualizzare i dettagli del bucket o gestire i bucket utilizzando Gestione tenant. Nella pagina Bucket di Tenant Manager viene visualizzato uno dei seguenti errori:

- Non puoi utilizzare questa API durante l'aggiornamento alla versione 11,8.
- Non è possibile visualizzare i dettagli delle versioni dei bucket in Tenant Manager durante l'aggiornamento a 11,8.

Questo errore viene risolto al termine dell'aggiornamento a 11,8.

Soluzione alternativa

Mentre è in corso l'aggiornamento 11,8, utilizzare i seguenti strumenti per visualizzare i dettagli del bucket o gestire i bucket, invece di utilizzare il Tenant Manager:

- Per eseguire operazioni S3 standard su un bucket, utilizzare "API REST S3" o il "API di gestione del tenant".
- Per eseguire operazioni personalizzate di StorageGRID su un bucket (ad esempio, visualizzazione e modifica della coerenza del bucket, attivazione o disattivazione degli aggiornamenti dell'ora dell'ultimo accesso o configurazione dell'integrazione della ricerca), utilizzare l'API Gestione tenant.

Impatto di un aggiornamento su gruppi e account utente

Potrebbe essere necessario aggiornare correttamente i gruppi e gli account utente al termine dell'aggiornamento.

Modifiche alle autorizzazioni e alle opzioni del gruppo

Dopo l'aggiornamento a StorageGRID 11,8, assegnare facoltativamente le seguenti nuove autorizzazioni ai gruppi di utenti tenant.

Permesso	Descrizione	Dettagli
Visualizza tutti i bucket	Consente agli utenti di visualizzare tutte le configurazioni di bucket e bucket.	L'autorizzazione Gestisci tutti i bucket sostituisce l'autorizzazione Visualizza tutti i bucket.

Vedere "Permessi di gestione del tenant".

Verificare la versione installata di StorageGRID

Prima di avviare l'aggiornamento, verificare che la versione precedente di StorageGRID sia attualmente installata con la correzione rapida più recente disponibile applicata.

A proposito di questa attività

Prima di eseguire l'aggiornamento a StorageGRID 11,8, sulla griglia deve essere installato StorageGRID 11,7. Se si sta utilizzando una versione precedente di StorageGRID, è necessario installare tutti i file di aggiornamento precedenti insieme ai relativi aggiornamenti rapidi più recenti (vivamente consigliato) fino a quando la versione corrente della griglia non è StorageGRID 11,7.*x.y*.

Un possibile percorso di aggiornamento viene mostrato nella 7 dalla versione 11,5,esempio.

> NetApp consiglia vivamente di applicare la correzione rapida più recente per ciascuna versione di StorageGRID prima di eseguire l'aggiornamento alla versione successiva e di applicare la correzione rapida più recente per ogni nuova versione installata. In alcuni casi, è necessario applicare una correzione rapida per evitare il rischio di perdita dei dati. Vedere "Download NetApp: StorageGRID" e le note di rilascio per ogni hotfix per saperne di più.

Fasi

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Nella parte superiore di Grid Manager, selezionare **Guida** > **informazioni**.
3. Verificare che **versione** sia 11,7.*x.y*.

   Nel numero di versione di StorageGRID 11,7.*x.y*:

   - La **release principale** ha un valore *x* di 0 (11,7.0).
   - Un **hotfix**, se è stato applicato, ha un valore *y* (ad esempio, 11,7.0,1).
4. Se **versione** non è 11,7.*x.y*, andare a. "Download NetApp: StorageGRID" per scaricare i file per ciascuna release precedente, inclusa la hotfix più recente per ciascuna release.
5. Ottenere le istruzioni di aggiornamento per ciascuna versione scaricata. Quindi, eseguire la procedura di aggiornamento del software per tale release e applicare la correzione rapida più recente per tale release (vivamente consigliata).

   Vedere "Procedura di hotfix StorageGRID".

Esempio: Aggiornamento a StorageGRID 11,7 dalla versione 11,5

Nell'esempio seguente vengono illustrati i passaggi per l'aggiornamento da versione 11,5 a StorageGRID versione 11,7 in preparazione per un aggiornamento a StorageGRID 11,8.

Scaricare e installare il software nella sequenza seguente per preparare il sistema per l'aggiornamento:

1. Applicare la correzione rapida StorageGRID 11,5.0.*y* più recente.
2. Eseguire l'aggiornamento alla versione principale di StorageGRID 11.6.0.
3. Applicare la correzione rapida StorageGRID 11,6.0.*y* più recente.
4. Eseguire l'aggiornamento alla versione principale di StorageGRID 11.7.0.
5. Applicare la correzione rapida StorageGRID 11,7.0.*y* più recente.

Ottenere il materiale necessario per un aggiornamento del software

Prima di iniziare l'aggiornamento del software, procurarsi tutto il materiale necessario.

Elemento	Note
Laptop di assistenza	Il laptop di assistenza deve disporre di: • Porta di rete • Client SSH (ad esempio, putty)
"Browser Web supportato"	Il supporto del browser in genere cambia per ogni release di StorageGRID. Assicurarsi che il browser sia compatibile con la nuova versione di StorageGRID.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non è elencata in `Passwords.txt` file.
Linux RPM o archivio DEB	Se vengono implementati nodi su host Linux, è necessario "Scaricare e installare il pacchetto RPM o DEB su tutti gli host" prima di iniziare l'aggiornamento. **Importante**: Assicurati che il tuo sistema operativo sia aggiornato al kernel Linux 4.15 o superiore.
Documentazione StorageGRID	• "Note di rilascio" Per StorageGRID 11,8 (accesso richiesto). Leggere attentamente queste informazioni prima di avviare l'aggiornamento. • "Guida alla risoluzione degli aggiornamenti del software StorageGRID" per la versione principale a cui si esegue l'aggiornamento (è necessario effettuare l'accesso) • Altro "Documentazione di StorageGRID 11,8", secondo necessità.

Controllare le condizioni del sistema

Prima di aggiornare un sistema StorageGRID, verificare che il sistema sia pronto per l'aggiornamento. Verificare che il sistema funzioni normalmente e che tutti i nodi della griglia siano operativi.

Fasi

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Verificare la presenza di eventuali avvisi attivi e risolverli.

3. Verificare che non vi siano attività della griglia in conflitto attive o in sospeso.
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***Site*** > ***Primary Admin Node*** > **CMN** > **Grid Tasks** > **Configuration**.

      I task ILME (Information Lifecycle Management Evaluation) sono gli unici task grid che possono essere eseguiti contemporaneamente all'aggiornamento del software.

   c. Se altre attività della griglia sono attive o in sospeso, attendere il completamento o rilasciare il blocco.

      Contattare il supporto tecnico se un'attività non termina o non rilascia il blocco.

4. Fare riferimento a. "Comunicazioni interne al nodo di rete" e. "Comunicazioni esterne" Per garantire che tutte le porte richieste per StorageGRID 11,8 siano aperte prima dell'aggiornamento.

   Non sono richieste porte aggiuntive per l'upgrade a StorageGRID 11,8.

   La seguente porta richiesta è stata aggiunta in StorageGRID 11,7. Assicurarsi che sia disponibile prima di eseguire l'aggiornamento a StorageGRID 11,8.

Porta	Descrizione
18086	Porta TCP utilizzata per le richieste S3 dal bilanciamento del carico StorageGRID a LDR e al nuovo servizio LDR. Prima di eseguire l'aggiornamento, verificare che la porta sia aperta da tutti i nodi della griglia a tutti i nodi di archiviazione. Il blocco di questa porta causerà S3 interruzioni del servizio dopo l'aggiornamento a StorageGRID 11,8.

Se sono state aperte porte firewall personalizzate, viene inviata una notifica durante la verifica preliminare dell'aggiornamento. È necessario contattare il supporto tecnico prima di procedere con l'aggiornamento.

Aggiornare il software

Avvio rapido dell'aggiornamento

Prima di iniziare l'aggiornamento, esaminare il flusso di lavoro generale. La pagina aggiornamento StorageGRID guida l'utente attraverso ogni fase di aggiornamento.

1 **Preparare gli host Linux**

Se vengono implementati nodi StorageGRID su host Linux, "Installare il pacchetto RPM o DEB su ciascun host" prima di iniziare l'aggiornamento.

2 **Caricare i file di aggiornamento e hotfix**

Dal nodo di amministrazione principale, accedere alla pagina di aggiornamento StorageGRID e caricare il file di aggiornamento e il file di correzione rapida, se necessario.

3 Scarica Recovery Package

Scaricare il pacchetto di ripristino corrente prima di avviare l'aggiornamento.

4 Eseguire controlli preliminari dell'aggiornamento

I controlli preliminari dell'aggiornamento consentono di rilevare i problemi, in modo da poterli risolvere prima di avviare l'aggiornamento effettivo.

5 Avviare l'aggiornamento

Quando si avvia l'aggiornamento, i controlli preliminari vengono eseguiti nuovamente e il nodo amministrativo primario viene aggiornato automaticamente. Impossibile accedere a Grid Manager durante l'aggiornamento del nodo di amministrazione primario. Anche i registri di controllo non saranno disponibili. L'aggiornamento può richiedere fino a 30 minuti.

6 Scarica Recovery Package

Una volta aggiornato il nodo di amministrazione primario, scaricare un nuovo pacchetto di ripristino.

7 Approva nodi

È possibile approvare singoli nodi griglia, gruppi di nodi griglia o tutti i nodi griglia.

> Non approvare l'aggiornamento per un nodo grid a meno che non si sia certi che il nodo sia pronto per essere arrestato e riavviato.

8 Riprendere le operazioni

Una volta aggiornati tutti i nodi della griglia, vengono attivate nuove funzionalità ed è possibile riprendere le operazioni. È necessario attendere l'esecuzione di una procedura di decommissionamento o espansione fino al completamento dell'attività **Upgrade database** in background e dell'attività **Final upgrade steps**.

Informazioni correlate

"Stima del tempo necessario per completare un aggiornamento"

Linux: Scaricare e installare il pacchetto RPM o DEB su tutti gli host

Se un qualsiasi nodo StorageGRID viene distribuito su host Linux, scaricare e installare un pacchetto RPM o DEB aggiuntivo su ciascuno di questi host prima di avviare l'aggiornamento.

Scarica i file di aggiornamento, Linux e hotfix

Quando si esegue un aggiornamento StorageGRID da Grid Manager, viene richiesto di scaricare l'archivio di aggiornamento e le correzioni rapide necessarie come primo passaggio. Tuttavia, se è necessario scaricare i file per aggiornare gli host Linux, è possibile risparmiare tempo scaricando tutti i file richiesti in anticipo.

Fasi

1. Passare a. "Download NetApp: StorageGRID".
2. Selezionare il pulsante per scaricare l'ultima versione oppure selezionare un'altra versione dal menu a discesa e selezionare **Go**.

   Le versioni del software StorageGRID hanno questo formato: 11.*x.y*. Le hotfix StorageGRID hanno questo formato: 11.*x.a. .z*.

3. Accedi con il nome utente e la password del tuo account NetApp.
4. Se viene visualizzato un avviso di attenzione/MustRead, annotare il numero della correzione rapida e selezionare la casella di controllo.
5. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).

   Viene visualizzata la pagina dei download per la versione selezionata. La pagina contiene tre colonne.

6. Dalla seconda colonna (**Upgrade StorageGRID**), scaricare due file:
   - L'archivio di aggiornamento per l'ultima release (questo è il file nella sezione denominata **VMware, SG1000 o SG100 Primary Admin Node**). Sebbene questo file non sia necessario fino a quando non si esegue l'aggiornamento, il download di questo file consente di risparmiare tempo.
   - Un archivio RPM o DEB in entrambi `.tgz` oppure `.zip` formato. Selezionare `.zip` File se si esegue Windows sul laptop di assistenza.
     - Red Hat Enterprise Linux
       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
     - Ubuntu o Debian
       `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
       `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
7. Se è necessario accettare un avviso di attenzione/MustRead a causa di una correzione rapida richiesta, scaricare la correzione rapida:
   a. Tornare a. "Download NetApp: StorageGRID".
   b. Selezionare il numero della correzione rapida dall'elenco a discesa.
   c. Accettare nuovamente l'avviso di attenzione e l'EULA.
   d. Scaricare e salvare la correzione rapida e il relativo README.

      Quando si avvia l'aggiornamento, viene richiesto di caricare il file hotfix nella pagina aggiornamento StorageGRID.

Installare l'archivio su tutti gli host Linux

Eseguire questa procedura prima di aggiornare il software StorageGRID.

Fasi

1. Estrarre i pacchetti RPM o DEB dal file di installazione.
2. Installare i pacchetti RPM o DEB su tutti gli host Linux.

   Consultare la procedura per l'installazione dei servizi host StorageGRID nelle istruzioni di installazione:

   - "Red Hat Enterprise Linux: Installazione dei servizi host StorageGRID"
   - "Ubuntu o Debian: Installare i servizi host di StorageGRID"

   I nuovi pacchetti vengono installati come pacchetti aggiuntivi. Non rimuovere i pacchetti esistenti.

Eseguire l'aggiornamento

È possibile eseguire l'aggiornamento a StorageGRID 11,8 e applicare contemporaneamente la correzione rapida più recente per tale versione. La pagina di aggiornamento di StorageGRID fornisce il percorso di aggiornamento consigliato e i collegamenti diretti alle pagine di download corrette.

Prima di iniziare

Hai esaminato tutte le considerazioni e completato tutte le fasi di pianificazione e preparazione.

Accedere alla pagina aggiornamento StorageGRID

Come primo passo, accedi alla pagina aggiornamento StorageGRID in Gestione griglia.

Fasi

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Selezionare **MANUTENZIONE** > **sistema** > **aggiornamento software**.
3. Dal riquadro di aggiornamento di StorageGRID, selezionare **Aggiorna**.

Selezionare file

Il percorso di aggiornamento nella pagina di aggiornamento di StorageGRID indica quali versioni principali (ad esempio, 11,8.0) e gli aggiornamenti rapidi (ad esempio, 11,8.0,1) è necessario installare per ottenere la versione più recente di StorageGRID. Installare le versioni consigliate e gli aggiornamenti rapidi nell'ordine indicato.

> Se non viene visualizzato alcun percorso di aggiornamento, il browser potrebbe non essere in grado di accedere al sito di supporto NetApp oppure la casella di controllo **Controlla aggiornamenti software** nella pagina AutoSupport (**SUPPORT** > **Tools** > **AutoSupport**) potrebbe essere disattivata.

Fasi

1. Per l'operazione **Select Files**, esaminare il percorso di aggiornamento.
2. Dalla sezione Download Files (Scarica file), selezionare ciascun collegamento **Download** per scaricare i file richiesti dal NetApp Support Site.

   Se non viene visualizzato alcun percorso di aggiornamento, passare a. "Download NetApp: StorageGRID" per determinare se è disponibile una nuova versione o una correzione rapida e per scaricare i file necessari.

Se è necessario scaricare e installare un pacchetto RPM o DEB su tutti gli host Linux, è possibile che i file di aggiornamento e hotfix di StorageGRID siano già elencati nel percorso di aggiornamento.

3. Selezionare **Sfoglia** per caricare il file di aggiornamento della versione su StorageGRID: `NetApp_StorageGRID_11.8.0_Software_uniqueID.upgrade`

   Al termine del processo di caricamento e convalida, accanto al nome del file viene visualizzato un segno di spunta verde.

4. Se è stato scaricato un file di hotfix, selezionare **Sfoglia** per caricarlo. La correzione rapida verrà applicata automaticamente come parte dell'aggiornamento della versione.
5. Selezionare **continua**.

Eseguire i controlli preliminari

L'esecuzione dei controlli preliminari consente di rilevare e risolvere eventuali problemi di aggiornamento prima di iniziare l'aggiornamento del grid.

Fasi

1. Per il passaggio **Esegui controlli preliminari**, iniziare inserendo la passphrase di provisioning per la griglia.
2. Selezionare **Download recovery package** (Scarica pacchetto di ripristino).

   Scaricare la copia corrente del file del pacchetto di ripristino prima di aggiornare il nodo di amministrazione primario. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

3. Una volta scaricato il file, verificare che sia possibile accedere ai contenuti, incluso il `Passwords.txt` file.
4. Copiare il file scaricato (`.zip`) in due posizioni sicure e separate.

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

5. Selezionare **Esegui pre-controlli** e attendere il completamento dei controlli preliminari.
6. Esaminare i dettagli di ogni pre-controllo segnalato e risolvere eventuali errori segnalati. Vedere "Guida alla risoluzione degli aggiornamenti del software StorageGRID" Per la versione StorageGRID 11,8.

   Prima di poter aggiornare il sistema, è necessario risolvere tutti gli errori di pre-controllo. Tuttavia, non è necessario eseguire il controllo preliminare *warnings* prima di eseguire l'aggiornamento.

   Se sono state aperte porte firewall personalizzate, viene inviata una notifica durante la convalida del controllo preliminare. È necessario contattare il supporto tecnico prima di procedere con l'aggiornamento.

7. Se sono state apportate modifiche alla configurazione per risolvere i problemi segnalati, selezionare di nuovo **Esegui controlli preliminari** per ottenere risultati aggiornati.

   Se tutti gli errori sono stati risolti, viene richiesto di avviare l'aggiornamento.

Avviare l'aggiornamento e aggiornare il nodo di amministrazione primario

Quando si avvia l'aggiornamento, i controlli preliminari dell'aggiornamento vengono eseguiti di nuovo e il nodo di amministrazione primario viene aggiornato automaticamente. Questa parte dell'aggiornamento può richiedere fino a 30 minuti.

> Non sarà possibile accedere ad altre pagine di Grid Manager durante l'aggiornamento del nodo di amministrazione primario. Anche i registri di controllo non saranno disponibili.

Fasi

1. Selezionare **Avvia aggiornamento**.

   Viene visualizzato un avviso per ricordare che l'accesso a Grid Manager verrà temporaneamente perso.

2. Selezionare **OK** per confermare l'avviso e avviare l'aggiornamento.
3. Attendere l'esecuzione delle verifiche preliminari dell'aggiornamento e l'aggiornamento del nodo di amministrazione primario.

   > Se vengono segnalati errori di pre-controllo, risolverli e selezionare di nuovo **Avvia aggiornamento**.

   Se la griglia dispone di un altro nodo Admin in linea e pronto, è possibile utilizzarlo per monitorare lo stato del nodo Admin primario. Non appena il nodo di amministrazione primario viene aggiornato, è possibile approvare gli altri nodi della griglia.

4. Se necessario, selezionare **continua** per accedere alla fase **Aggiorna altri nodi**.

Aggiornare altri nodi

È necessario aggiornare tutti i nodi grid, ma è possibile eseguire più sessioni di aggiornamento e personalizzare la sequenza di aggiornamento. Ad esempio, si consiglia di aggiornare i nodi nel sito A in una sessione e quindi aggiornare i nodi nel sito B in una sessione successiva. Se si sceglie di eseguire l'aggiornamento in più sessioni, tenere presente che non è possibile iniziare a utilizzare le nuove funzionalità fino a quando tutti i nodi non sono stati aggiornati.

Se l'ordine in cui i nodi vengono aggiornati è importante, approvare i nodi o i gruppi di nodi uno alla volta e attendere il completamento dell'aggiornamento su ciascun nodo prima di approvare il nodo o il gruppo di nodi successivo.

> Quando l'aggiornamento inizia su un nodo grid, i servizi su quel nodo vengono interrotti. In seguito, il nodo Grid viene riavviato. Per evitare interruzioni del servizio per le applicazioni client che comunicano con il nodo, non approvare l'aggiornamento per un nodo a meno che non si sia certi che il nodo sia pronto per essere arrestato e riavviato. Se necessario, pianificare una finestra di manutenzione o avvisare i clienti.

Fasi

1. Per la fase **Upgrade other Nodes** (Aggiorna altri nodi), consultare il Riepilogo, che fornisce l'ora di inizio dell'aggiornamento nel suo complesso e lo stato di ogni importante attività di upgrade.
   - **Avvia servizio di aggiornamento** è la prima attività di aggiornamento. Durante questa attività, il file software viene distribuito ai nodi grid e il servizio di aggiornamento viene avviato su ciascun nodo.
   - Una volta completata l'attività **Avvia aggiornamento**, viene avviata l'attività **Aggiorna altri nodi della griglia** e viene richiesto di scaricare una nuova copia del pacchetto di ripristino.

2. Quando richiesto, inserire la passphrase di provisioning e scaricare una nuova copia del pacchetto di ripristino.

> È necessario scaricare una nuova copia del file del pacchetto di ripristino dopo l'aggiornamento del nodo amministrativo primario. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

3. Esaminare le tabelle di stato per ciascun tipo di nodo. Sono disponibili tabelle per i nodi amministrativi non primari, i nodi gateway, i nodi storage e i nodi archivio.

   Un nodo della griglia può trovarsi in una di queste fasi quando le tabelle vengono visualizzate per la prima volta:

   - Disimballaggio dell'aggiornamento
   - Download in corso
   - In attesa di approvazione

4. quando sei pronto a selezionare i nodi di griglia per l'upgrade (o se devi annullare l'approvazione dei nodi selezionati), utilizza queste istruzioni:

Attività	**Istruzioni**
Cercare nodi specifici da approvare, ad esempio tutti i nodi di un determinato sito	Inserire la stringa di ricerca nel campo **Search**
Selezionare tutti i nodi per l'aggiornamento	Selezionare **approva tutti i nodi**
Selezionare tutti i nodi dello stesso tipo per l'aggiornamento (ad esempio, tutti i nodi di storage)	Selezionare il pulsante **approva tutto** per il tipo di nodo Se si approvano più nodi dello stesso tipo, questi verranno aggiornati uno alla volta.
Selezionare un singolo nodo per l'aggiornamento	Selezionare il pulsante **approva** per il nodo
Posticipare l'aggiornamento su tutti i nodi selezionati	Selezionare **Annulla approvazione di tutti i nodi**
Posticipare l'aggiornamento su tutti i nodi selezionati dello stesso tipo	Selezionare il pulsante **Annulla approvazione tutto** per il tipo di nodo
Posticipare l'aggiornamento su un singolo nodo	Selezionare il pulsante **Annulla approvazione** per il nodo

5. Attendere che i nodi approvati procedano con le seguenti fasi di aggiornamento:
   - Approvato e in attesa di aggiornamento
   - Interruzione dei servizi

> Non puoi rimuovere un nodo quando il suo Stage raggiunge **arresto dei servizi**. Il pulsante **Annulla approvazione** è disattivato.

- Arresto del container
- Pulizia delle immagini Docker
- Aggiornamento dei pacchetti del sistema operativo di base

> Quando un nodo appliance raggiunge questa fase, il software di installazione dell'appliance StorageGRID viene aggiornato. Questo processo automatizzato garantisce che la versione del programma di installazione dell'appliance StorageGRID rimanga sincronizzata con la versione del software StorageGRID.

- Riavvio in corso

> Alcuni modelli di appliance potrebbero riavviarsi più volte per aggiornare il firmware e il BIOS.

- Esecuzione dei passaggi dopo il riavvio
- Avvio dei servizi
- Fatto

6. Ripetere il fase di approvazione il numero di volte necessario fino a quando tutti i nodi di rete non sono stati aggiornati.

Aggiornamento completo

Quando tutti i nodi della griglia hanno completato le fasi di aggiornamento, l'attività **Upgrade other grid Node** (Aggiorna altri nodi della griglia) viene visualizzata come completata. Le restanti attività di aggiornamento vengono eseguite automaticamente in background.

Fasi

1. Una volta completata l'attività **Enable Features** (che si verifica rapidamente), è possibile iniziare a utilizzare "nuove funzionalità" Nella versione aggiornata di StorageGRID.
2. Durante l'attività **Upgrade database**, il processo di aggiornamento controlla ciascun nodo per verificare che il database Cassandra non debba essere aggiornato.

> L'upgrade da StorageGRID 11,7 a 11,8 non richiede un aggiornamento del database Cassandra; tuttavia, il servizio Cassandra verrà arrestato e riavviato su ogni nodo storage. Per le future versioni delle funzionalità di StorageGRID, il completamento della fase di aggiornamento del database Cassandra potrebbe richiedere diversi giorni.

3. Una volta completata l'attività **Upgrade database**, attendere alcuni minuti per il completamento delle **fasi finali dell'aggiornamento**.
4. Una volta completate le **fasi finali dell'aggiornamento**, l'aggiornamento viene eseguito. Il primo passaggio, **Select Files**, viene visualizzato nuovamente con un banner verde di successo.
5. Verificare che le operazioni della griglia siano tornate alla normalità:
   a. Verificare che i servizi funzionino normalmente e che non siano presenti avvisi imprevisti.
   b. Verificare che le connessioni client al sistema StorageGRID funzionino come previsto.

Risolvere i problemi di aggiornamento

Se si verifica un errore durante l'esecuzione di un aggiornamento, potrebbe essere possibile risolvere il problema da soli. Se non riesci a risolvere un problema, raccogli tutte le informazioni possibili e contatta il supporto tecnico.

L'aggiornamento non viene completato

Le sezioni seguenti descrivono come eseguire il ripristino da situazioni in cui l'aggiornamento non è riuscito parzialmente.

Errori di controllo preliminare dell'aggiornamento

Per rilevare e risolvere i problemi, è possibile eseguire manualmente i controlli preliminari dell'aggiornamento prima di avviare l'aggiornamento effettivo. La maggior parte degli errori di pre-controllo fornisce informazioni su come risolvere il problema.

Errori di provisioning

Se il processo di provisioning automatico non riesce, contattare il supporto tecnico.

Il nodo Grid si blocca o non si avvia

Se un nodo grid si blocca durante il processo di aggiornamento o non si avvia correttamente al termine dell'aggiornamento, contattare il supporto tecnico per investigare e correggere eventuali problemi sottostanti.

L'acquisizione o il recupero dei dati viene interrotto

Se l'acquisizione o il recupero dei dati viene interrotto inaspettatamente quando non si aggiorna un nodo di griglia, contattare il supporto tecnico.

Errori di aggiornamento del database

Se l'aggiornamento del database non riesce e viene visualizzato un errore, riprovare. Se il problema persiste, contattare il supporto tecnico.

Informazioni correlate

"Verifica delle condizioni del sistema prima dell'aggiornamento del software"

Problemi dell'interfaccia utente

Potrebbero verificarsi problemi con Grid Manager o con il tenant Manager durante o dopo l'aggiornamento.

Grid Manager visualizza più messaggi di errore durante l'aggiornamento

Se si aggiorna il browser o si accede a un'altra pagina di Grid Manager mentre il nodo amministrativo principale viene aggiornato, è possibile che vengano visualizzati più messaggi "503: Servizio non disponibile" e "problema di connessione al server". È possibile ignorare questi messaggi in modo sicuro, che smetteranno di essere visualizzati non appena il nodo viene aggiornato.

Se questi messaggi vengono visualizzati per più di un'ora dopo l'avvio dell'aggiornamento, potrebbe essersi verificato un problema che ha impedito l'aggiornamento del nodo di amministrazione primario. Se non riesci a risolvere il problema da solo, contatta il supporto tecnico.

L'interfaccia Web non risponde come previsto

Dopo l'aggiornamento del software StorageGRID, il gestore di rete o il tenant manager potrebbero non rispondere come previsto.

In caso di problemi con l'interfaccia Web:

- Assicurarsi di utilizzare un "browser web supportato".

  Il supporto del browser in genere cambia per ogni release di StorageGRID.

- Cancellare la cache del browser Web.

  La cancellazione della cache rimuove le risorse obsolete utilizzate dalla versione precedente del software StorageGRID e consente all'interfaccia utente di funzionare nuovamente correttamente. Per istruzioni, consultare la documentazione del browser Web.

Messaggi di errore "controllo disponibilità immagine Docker"

Quando si tenta di avviare il processo di upgrade, potrebbe essere visualizzato un messaggio di errore che indica che la suite di convalida del controllo di disponibilità dell'immagine Docker ha identificato i seguenti problemi. Tutti i problemi devono essere risolti prima di poter completare l'aggiornamento.

In caso di dubbi sulle modifiche necessarie per risolvere i problemi identificati, contattare il supporto tecnico.

Messaggio	Causa	Soluzione
Impossibile determinare la versione dell'aggiornamento. File di informazioni sulla versione di aggiornamento `{file_path}` il formato non corrisponde a quello previsto.	Il pacchetto di aggiornamento è corrotto.	Caricare nuovamente il pacchetto di aggiornamento e riprovare. Se il problema persiste, contattare il supporto tecnico.
File di informazioni sulla versione di aggiornamento `{file_path}` non trovato. Impossibile determinare la versione dell'aggiornamento.	Il pacchetto di aggiornamento è corrotto.	Caricare nuovamente il pacchetto di aggiornamento e riprovare. Se il problema persiste, contattare il supporto tecnico.
Impossibile determinare la versione della release attualmente installata su `{node_name}`.	Un file critico sul nodo è corrotto.	Contattare il supporto tecnico.
Errore di connessione durante il tentativo di elencare le versioni su `{node_name}`	Il nodo è offline o la connessione è stata interrotta.	Verificare che tutti i nodi siano in linea e raggiungibili dal nodo di amministrazione primario e riprovare.

Messaggio	Causa	Soluzione
L'host per il nodo `{node_name}` Non dispone di StorageGRID `{upgrade_version}` immagine caricata. Prima di procedere con l'aggiornamento, è necessario installare immagini e servizi sull'host.	I pacchetti RPM o DEB per l'aggiornamento non sono stati installati sull'host in cui è in esecuzione il nodo oppure le immagini sono ancora in fase di importazione. **Nota:** questo errore si applica solo ai nodi in esecuzione come container su Linux.	Assicurarsi che i pacchetti RPM o DEB siano stati installati su tutti gli host Linux in cui sono in esecuzione i nodi. Assicurarsi che la versione sia corretta sia per il servizio che per il file di immagini. Attendere alcuni minuti e riprovare. Vedere "Linux: Installare il pacchetto RPM o DEB su tutti gli host".
Errore durante il controllo del nodo `{node_name}`	Si è verificato un errore imprevisto.	Attendere alcuni minuti e riprovare.
Errore irreversibile durante l'esecuzione dei controlli preliminari. `{error_string}`	Si è verificato un errore imprevisto.	Attendere alcuni minuti e riprovare.

Applicare la correzione rapida StorageGRID

Procedura di hotfix StorageGRID: Panoramica

Potrebbe essere necessario applicare una hotfix al sistema StorageGRID se vengono rilevati e risolti problemi relativi al software tra una versione e l'altra.

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. Inoltre, ogni release di hotfix contiene un rolup di tutti gli hotfix precedenti all'interno della funzionalità o della release di patch.

Considerazioni per l'applicazione di una correzione rapida

Non è possibile applicare una correzione rapida StorageGRID quando è in esecuzione un'altra procedura di manutenzione. Ad esempio, non è possibile applicare una correzione rapida mentre è in esecuzione una procedura di decommissionamento, espansione o ripristino.

> Se la procedura di decommissionamento di un nodo o di un sito è in pausa, è possibile applicare una correzione rapida in tutta sicurezza. Inoltre, potrebbe essere possibile applicare una correzione rapida durante le fasi finali di una procedura di aggiornamento di StorageGRID. Per ulteriori informazioni, consultare le istruzioni per l'aggiornamento del software StorageGRID.

Dopo aver caricato la correzione rapida in Grid Manager, la correzione rapida viene applicata automaticamente al nodo di amministrazione primario. Quindi, è possibile approvare l'applicazione della correzione rapida agli altri nodi nel sistema StorageGRID.

Se una correzione rapida non viene applicata a uno o più nodi, il motivo dell'errore viene visualizzato nella colonna Dettagli della tabella di avanzamento della correzione rapida. È necessario risolvere i problemi che hanno causato gli errori e riprovare l'intero processo. I nodi con un'applicazione della correzione rapida precedentemente riuscita verranno ignorati nelle applicazioni successive. È possibile riprovare il processo di

hotfix tutte le volte necessarie fino a quando tutti i nodi non sono stati aggiornati. Per completare l'applicazione, la correzione rapida deve essere installata correttamente su tutti i nodi della griglia.

Mentre 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.

Modalità di applicazione degli hotfix per il ripristino e l'espansione

Una volta applicata una correzione rapida alla griglia, il nodo di amministrazione primario installa automaticamente la stessa versione della correzione rapida su qualsiasi nodo ripristinato mediante operazioni di ripristino o aggiunto in un'espansione.

Tuttavia, se è necessario ripristinare il nodo di amministrazione primario, è necessario installare manualmente la versione corretta di StorageGRID e applicare la correzione rapida. La versione finale di StorageGRID del nodo di amministrazione primario deve corrispondere alla versione degli altri nodi nella griglia.

Nell'esempio seguente viene illustrato come applicare una correzione rapida durante il ripristino del nodo di amministrazione primario:

1. Si supponga che la griglia stia eseguendo una versione di StorageGRID 11.*A.B* con la correzione rapida più recente. La "versione griglia" è 11.*A.B.y*.
2. Si verifica un errore nel nodo di amministrazione primario.
3. Il nodo di amministrazione primario viene ridistribuita utilizzando StorageGRID 11.*A.B* ed è possibile eseguire la procedura di ripristino.

> In base alle esigenze della versione grid, è possibile utilizzare una release minore durante la distribuzione del nodo; non è necessario implementare prima la release principale.

4. Quindi, applicare la correzione rapida 11.*A.B.y* al nodo di amministrazione primario.

Per ulteriori informazioni, vedere "Configurare il nodo amministrativo primario sostitutivo".

Impatto del sistema quando si applica una correzione rapida

Quando si applica una hotfix, è necessario comprendere in che modo il sistema StorageGRID verrà influenzato.

Le correzioni rapide di StorageGRID non provocano interruzioni

Il sistema StorageGRID è in grado di acquisire e recuperare i dati dalle applicazioni client durante tutto il processo di hotfix. Se si approvano tutti i nodi dello stesso tipo per la correzione rapida (ad esempio, nodi di archiviazione), i nodi vengono abbassati uno alla volta, quindi non c'è tempo quando tutti i nodi della griglia o tutti i nodi della griglia di un determinato tipo non sono disponibili.

Per consentire la disponibilità continua, assicurarsi che il criterio ILM contenga regole che specificano la memorizzazione di più copie di ciascun oggetto. È inoltre necessario assicurarsi che tutti i client S3 o Swift esterni siano configurati per inviare richieste a uno dei seguenti:

- Un indirizzo IP virtuale del gruppo ad alta disponibilità (ha)
- Bilanciamento del carico di terze parti ad alta disponibilità
- Nodi gateway multipli per ogni client

- Più nodi di storage per ogni client

Le applicazioni client potrebbero riscontrare interruzioni a breve termine

Il sistema StorageGRID è in grado di acquisire e recuperare i dati dalle applicazioni client durante l'intero processo di hotfix; tuttavia, le connessioni client a singoli nodi gateway o nodi di storage potrebbero essere temporaneamente interrottate se la hotfix deve riavviare i servizi su tali nodi. La connettività verrà ripristinata al termine del processo di hotfix e i servizi riprenderanno sui singoli nodi.

Potrebbe essere necessario pianificare il downtime per applicare una correzione rapida se la perdita di connettività per un breve periodo non è accettabile. È possibile utilizzare l'approvazione selettiva per pianificare l'aggiornamento di determinati nodi.

È possibile utilizzare più gateway e gruppi ad alta disponibilità (ha) per fornire il failover automatico durante il processo di hotfix. Consultare le istruzioni per "configurazione di gruppi ad alta disponibilità".

Potrebbero essere attivati avvisi e notifiche SNMP

Gli avvisi e le notifiche SNMP potrebbero essere attivati al riavvio dei servizi e quando il sistema StorageGRID funziona come ambiente a versione mista (alcuni nodi di griglia che eseguono una versione precedente, mentre altri sono stati aggiornati a una versione successiva). In generale, al termine della correzione rapida, gli avvisi e le notifiche verranno deselezionati.

Le modifiche alla configurazione sono limitate

Quando si applica una correzione rapida a StorageGRID:

- Non apportare modifiche alla configurazione della griglia (ad esempio, specificando subnet Grid Network o approvando i nodi della griglia in sospeso) fino a quando la correzione rapida non è stata applicata a tutti i nodi.
- Non aggiornare la configurazione ILM fino a quando la correzione rapida non è stata applicata a tutti i nodi.

Ottenere il materiale necessario per la correzione rapida

Prima di applicare una hotfix, è necessario procurarsi tutti i materiali necessari.

Elemento	Note
File di hotfix StorageGRID	È necessario scaricare il file di hotfix StorageGRID.
• Porta di rete • "Browser Web supportato" • Client SSH (ad esempio, putty)	

Elemento	Note
Pacchetto di ripristino (`.zip`)	Prima di applicare una correzione rapida, "Scaricare il file del pacchetto di ripristino più recente" in caso di problemi durante la correzione rapida. Quindi, dopo aver applicato la correzione rapida, scaricare una nuova copia del file del pacchetto di ripristino e salvarlo in un luogo sicuro. Il file Recovery Package aggiornato consente di ripristinare il sistema in caso di errore.
File Passwords.txt	Facoltativo e utilizzato solo se si applica manualmente una correzione rapida utilizzando il client SSH. Il `Passwords.txt` Il file fa parte del pacchetto di ripristino `.zip` file.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non è elencata in `Passwords.txt` file.
Documentazione correlata	`readme.txt` file per la correzione rapida. Questo file è incluso nella pagina di download della correzione rapida. Assicurarsi di esaminare `readme` archiviare attentamente prima di applicare la correzione rapida.

Scaricare il file hotfix

Prima di applicare la correzione rapida, è necessario scaricare il file della correzione rapida.

Fasi

1. Passare a. "Download NetApp: StorageGRID".
2. Selezionare la freccia verso il basso sotto **Software disponibile** per visualizzare un elenco di hotfix disponibili per il download.

   Le versioni dei file hotfix hanno il formato: 11.4.*x.y*.

3. Esaminare le modifiche incluse nell'aggiornamento.

   Se hai solo "Ripristinato nodo amministratore primario" è inoltre necessario applicare una correzione rapida, selezionare la stessa versione della correzione rapida installata sugli altri nodi della griglia.

   a. Selezionare la versione della correzione rapida che si desidera scaricare e selezionare **Go**.
   b. Accedi utilizzando il nome utente e la password del tuo account NetApp.
   c. Leggere e accettare il Contratto di licenza con l'utente finale.

      Viene visualizzata la pagina di download della versione selezionata.

   d. Scaricare la correzione rapida `readme.txt` file per visualizzare un riepilogo delle modifiche incluse nella correzione rapida.
4. Selezionare il pulsante di download per la correzione rapida e salvare il file.

Non modificare il nome del file.

Se si utilizza un dispositivo macOS, il file hotfix potrebbe essere salvato automaticamente come `.txt` file. In tal caso, è necessario rinominare il file senza `.txt` interno.

5. Selezionare una posizione per il download e selezionare **Salva**.

Controllare le condizioni del sistema prima di applicare la correzione rapida

Verificare che il sistema sia pronto per la correzione rapida.

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Se possibile, assicurarsi che il sistema funzioni correttamente e che tutti i nodi della rete siano collegati alla rete.

   I nodi connessi presentano segni di spunta verdi Nella pagina nodi.

3. Controllare e risolvere eventuali avvisi correnti, se possibile.
4. Assicurarsi che non siano in corso altre procedure di manutenzione, ad esempio una procedura di upgrade, recovery, espansione o decommissionamento.

   Prima di applicare una correzione rapida, attendere il completamento delle procedure di manutenzione attive.

   Non è possibile applicare una correzione rapida StorageGRID quando è in esecuzione un'altra procedura di manutenzione. Ad esempio, non è possibile applicare una correzione rapida mentre è in esecuzione una procedura di decommissionamento, espansione o ripristino.

   Se si tratta di un nodo o di un sito "la procedura di decommissionamento è in pausa", è possibile applicare una correzione rapida in tutta sicurezza. Inoltre, potrebbe essere possibile applicare una correzione rapida durante le fasi finali di una procedura di aggiornamento di StorageGRID. Consultare le istruzioni per "Aggiornamento del software StorageGRID".

Applicare la correzione rapida

La correzione rapida viene applicata automaticamente 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 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.

Prima di iniziare

- Hai esaminato il "considerazioni per l'applicazione di una correzione rapida".
- Si dispone della passphrase di provisioning.
- Si dispone dell'autorizzazione di accesso root o di manutenzione.

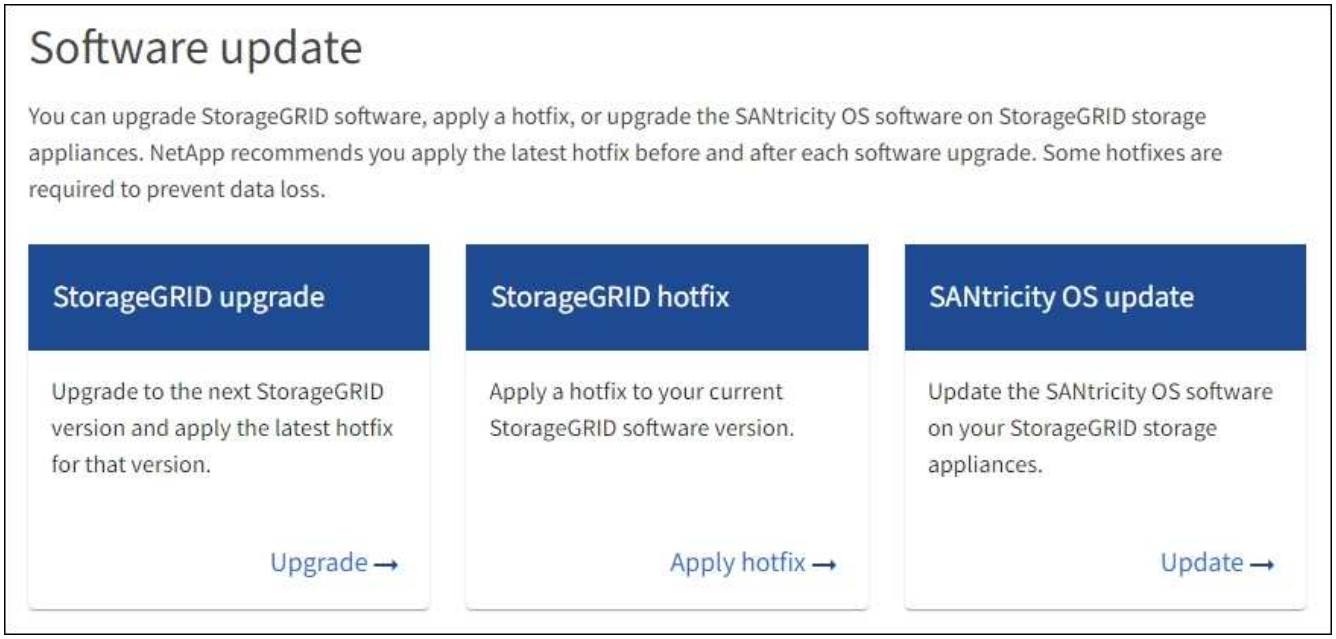
A proposito di questa attività

- È possibile ritardare l'applicazione di una hotfix a un nodo, ma il processo di hotfix non viene completato fino a quando non si applica la hotfix a tutti i nodi.
- Non è possibile eseguire un aggiornamento del software StorageGRID o del sistema operativo SANtricity fino a quando non viene completata la procedura di correzione rapida.

Fasi

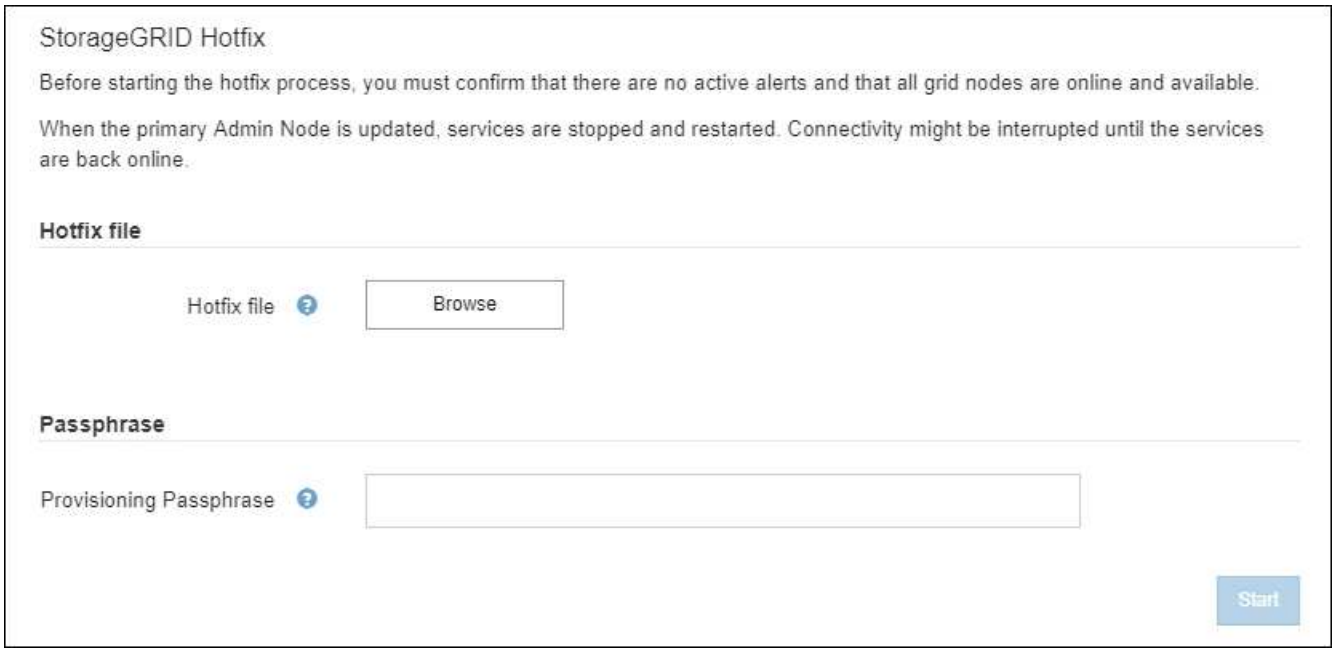
1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Selezionare **MANUTENZIONE** > **sistema** > **aggiornamento software**.

   Viene visualizzata la pagina Software Update (aggiornamento software).



3. Selezionare **Apply Hotfix** (Applica correzione rapida).

   Viene visualizzata la pagina Hotfix StorageGRID.



4. Selezionare il file hotfix scaricato dal NetApp Support Site.

   a. Selezionare **Sfoglia**.

   b. Individuare e selezionare il file.

      `hotfix-install-version`

   c. Selezionare **Apri**.

      Il file viene caricato. Al termine del caricamento, il nome del file viene visualizzato nel campo Dettagli.

      Non modificare il nome del file perché fa parte del processo di verifica.

5. Inserire la passphrase di provisioning nella casella di testo.

   Il pulsante **Start** viene attivato.

6. Selezionare **Start**.

   Viene visualizzato un avviso che indica che la connessione del browser potrebbe andare persa temporaneamente quando i servizi sul nodo di amministrazione primario vengono riavviati.

7. Selezionare **OK** per avviare l'applicazione della correzione rapida al nodo di amministrazione primario.

   All'avvio della correzione rapida:

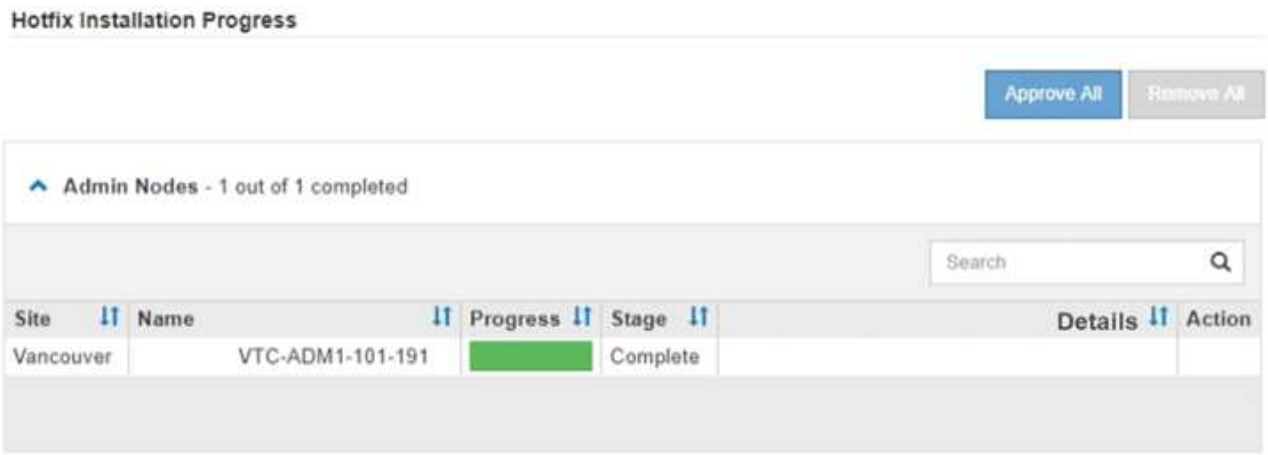
   a. Vengono eseguite le validazioni della correzione rapida.

      Se vengono segnalati errori, risolverli, caricare nuovamente il file di correzione rapida e selezionare di nuovo **Avvia**.

   b. Viene visualizzata la tabella di avanzamento dell'installazione della correzione rapida.

      Questa tabella mostra tutti i nodi della griglia e la fase corrente dell'installazione della correzione rapida per ciascun nodo. I nodi nella tabella sono raggruppati per tipo (nodi di amministrazione, nodi gateway, nodi di storage e nodi di archivio).

   c. La barra di avanzamento raggiunge il completamento, quindi il nodo amministrativo primario viene visualizzato come "completo".



8. Facoltativamente, ordinare gli elenchi di nodi in ciascun raggruppamento in ordine crescente o decrescente per **Sito**, **Nome**, **avanzamento**, **fase** o **Dettagli**. In alternativa, inserire un termine nella casella **Search** per cercare nodi specifici.
9. Approvare i nodi della griglia pronti per l'aggiornamento. I nodi approvati dello stesso tipo vengono aggiornati uno alla volta.

   Non approvare la correzione rapida per un nodo a meno che non si sia certi che il nodo sia pronto per l'aggiornamento. Quando la correzione rapida viene applicata a un nodo Grid, alcuni servizi su tale nodo potrebbero essere riavviati. Queste operazioni potrebbero causare interruzioni del servizio per i client che comunicano con il nodo.

   - Selezionare uno o più pulsanti **approva** per aggiungere uno o più singoli nodi alla coda degli aggiornamenti rapidi.
   - Selezionare il pulsante **approva tutto** all'interno di ciascun gruppo per aggiungere tutti i nodi dello stesso tipo alla coda degli hotfix. Se sono stati immessi criteri di ricerca nella casella **Cerca**, il pulsante **approva tutto** si applica a tutti i nodi selezionati dai criteri di ricerca.

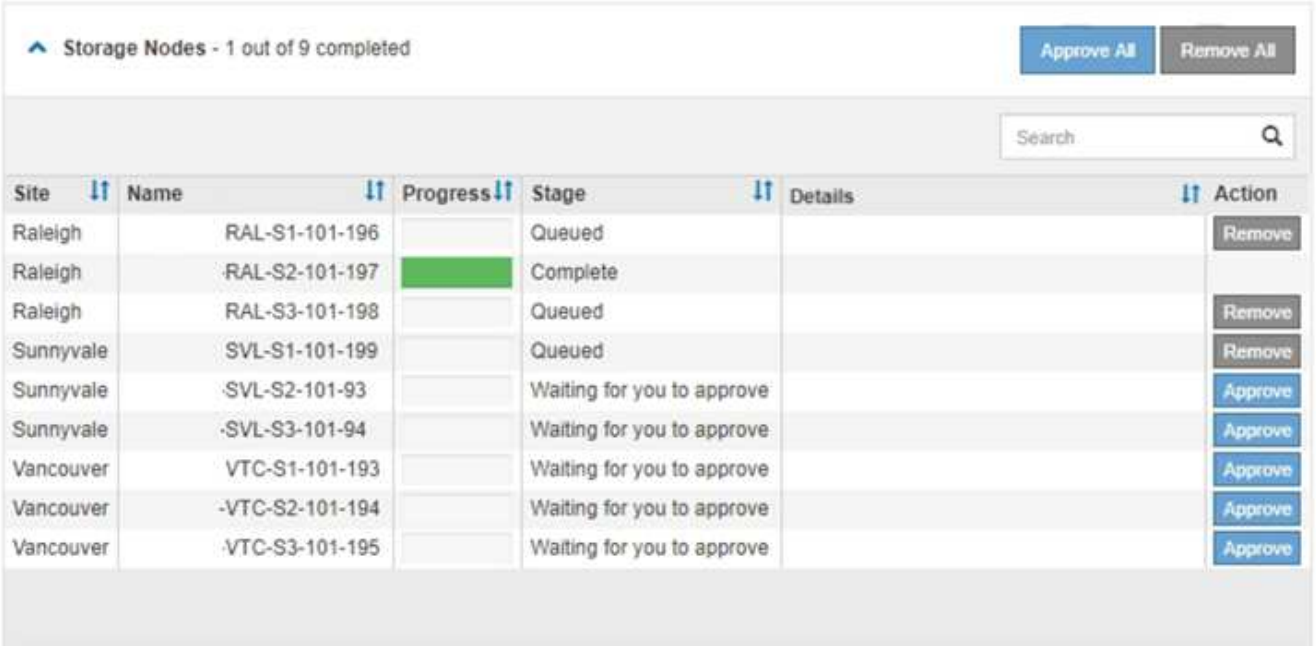
     Il pulsante **approva tutto** nella parte superiore della pagina approva tutti i nodi elencati nella pagina, mentre il pulsante **approva tutto** nella parte superiore di un raggruppamento di tabelle approva solo tutti i nodi di quel gruppo. Se l'ordine in cui i nodi vengono aggiornati è importante, approvare i nodi o i gruppi di nodi uno alla volta e attendere il completamento dell'aggiornamento su ciascun nodo prima di approvare i nodi successivi.

   - Selezionare il pulsante di primo livello **approva tutto** nella parte superiore della pagina per aggiungere tutti i nodi della griglia alla coda degli aggiornamenti rapidi.

     È necessario completare la correzione rapida StorageGRID prima di poter avviare un aggiornamento software diverso. Se non si riesce a completare la correzione rapida, contattare il supporto tecnico.

   - Selezionare **Remove** o **Remove All** per rimuovere un nodo o tutti i nodi dalla coda di hotfix.

     Quando Stage va oltre "in coda", il pulsante **Rimuovi** è nascosto e non è più possibile rimuovere il nodo dal processo di correzione rapida.



10. Attendere che la correzione rapida venga applicata a ciascun nodo della griglia approvato.

    Una volta che la correzione rapida è stata installata correttamente su tutti i nodi, la tabella di avanzamento dell'installazione della correzione rapida si chiude. Un banner verde mostra la data e l'ora in cui la correzione rapida è stata completata.

11. Se la correzione rapida non può essere applicata a nessun nodo, esaminare l'errore per ciascun nodo, risolvere il problema e ripetere la procedura.

    La procedura non è completa fino a quando la correzione rapida non viene applicata correttamente a tutti i nodi. È possibile riprovare il processo di correzione rapida tutte le volte necessarie fino al completamento.

Configurare e gestire un sistema StorageGRID

Amministrare StorageGRID

Administer StorageGRID: Panoramica

Seguire queste istruzioni per configurare e amministrare un sistema StorageGRID.

A proposito di queste istruzioni

Le attività principali per la configurazione e l'amministrazione di StorageGRID consentono di:

- Utilizzare il Grid Manager per impostare gruppi e utenti
- Creare account tenant per consentire alle applicazioni client S3 e Swift di memorizzare e recuperare oggetti
- Configurare e gestire le reti StorageGRID
- Configurare AutoSupport
- Gestire le impostazioni dei nodi

Prima di iniziare

- Hai una conoscenza generale del sistema StorageGRID.
- Hai una conoscenza abbastanza dettagliata delle shell dei comandi Linux, delle reti e della configurazione e configurazione dell'hardware del server.

Inizia subito con Grid Manager

Requisiti del browser Web

È necessario utilizzare un browser Web supportato.

Browser Web	Versione minima supportata
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Impostare la larghezza consigliata per la finestra del browser.

Larghezza del browser	Pixel
Minimo	1024
Ottimale	1280

Accedi a Grid Manager

Per accedere alla pagina di accesso di Grid Manager, immettere il nome di dominio completo (FQDN) o l'indirizzo IP di un nodo amministratore nella barra degli indirizzi di un browser Web supportato.

Panoramica

Ogni sistema StorageGRID include un nodo di amministrazione primario e un numero qualsiasi di nodi di amministrazione non primari. Per gestire il sistema StorageGRID, è possibile accedere a Grid Manager da qualsiasi nodo amministrativo. Tuttavia, i nodi Admin non sono esattamente gli stessi:

- Le conferme di allarme (sistema legacy) eseguite su un nodo di amministrazione non vengono copiate in altri nodi di amministrazione. Per questo motivo, le informazioni visualizzate per gli allarmi potrebbero non apparire identiche su ciascun nodo di amministrazione.
- Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

Connettersi al gruppo ha

Se i nodi di amministrazione sono inclusi in un gruppo ad alta disponibilità (ha), la connessione viene eseguita utilizzando l'indirizzo IP virtuale del gruppo ha o un nome di dominio completo che viene mappato all'indirizzo IP virtuale. Il nodo di amministrazione primario deve essere selezionato come interfaccia principale del gruppo, in modo che quando si accede a Grid Manager, si accede al nodo di amministrazione primario, a meno che il nodo di amministrazione primario non sia disponibile. Vedere "Gestire i gruppi ad alta disponibilità".

Utilizzare SSO

Le fasi di accesso sono leggermente diverse se "È stato configurato Single Sign-on (SSO)".

Accedi a Grid Manager sul primo nodo di amministrazione

Prima di iniziare

- Si dispone delle credenziali di accesso.
- Si sta utilizzando un "browser web supportato".
- I cookie sono attivati nel browser Web.
- L'utente appartiene a un gruppo di utenti che dispone di almeno un'autorizzazione.
- Hai l'URL per Grid Manager:

  `https://FQDN_or_Admin_Node_IP/`

  È possibile utilizzare il nome di dominio completo, l'indirizzo IP di un nodo amministrativo o l'indirizzo IP virtuale di un gruppo ha di nodi amministrativi.

  Per accedere a Grid Manager su una porta diversa da quella predefinita per HTTPS (443), includere il numero di porta nell'URL:

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO non è disponibile sulla porta di Restricted Grid Manager. È necessario utilizzare la porta 443.

Fasi

1. Avviare un browser Web supportato.
2. Nella barra degli indirizzi del browser, immettere l'URL per Grid Manager.
3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser. Vedere "Gestire i certificati di sicurezza".
4. Accedi a Grid Manager.

   La schermata di accesso visualizzata dipende dalla configurazione di SSO (Single Sign-on) per StorageGRID.

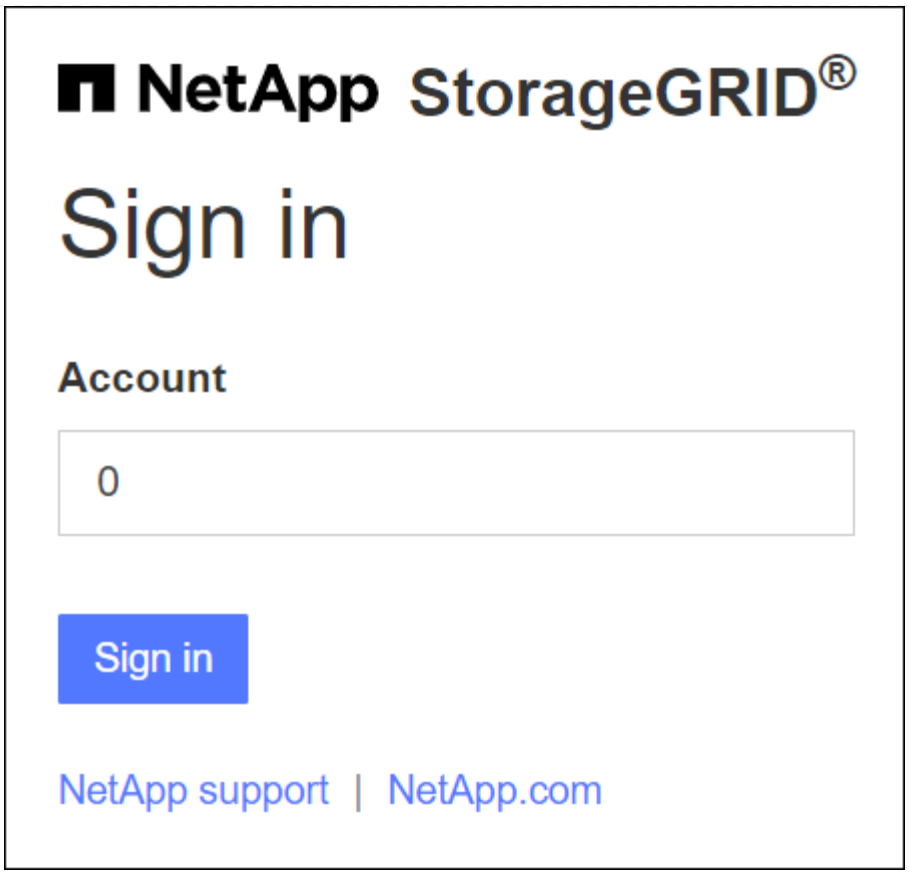
Non si utilizza SSO

a. Immettere il nome utente e la password per Grid Manager.

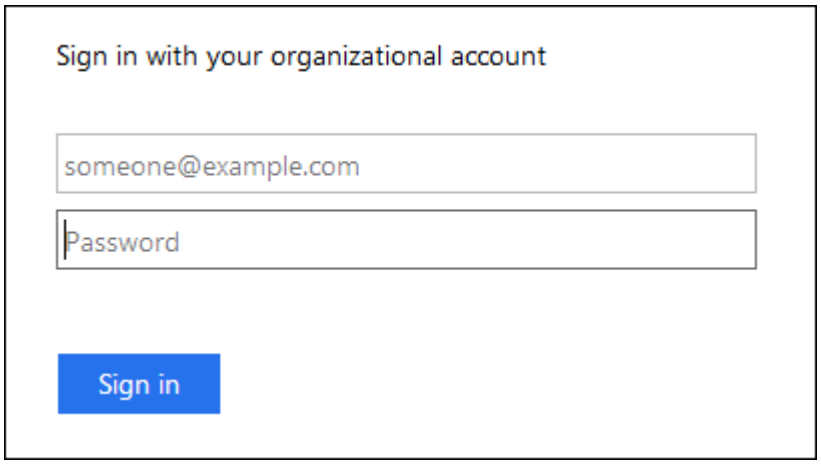
b. Selezionare **Accedi**.

Utilizzo di SSO

- Se StorageGRID utilizza SSO ed è la prima volta che si accede all'URL dal browser:
  i. Selezionare **Accedi**. È possibile lasciare lo 0 nel campo account.



ii. Immettere le credenziali SSO standard nella pagina di accesso SSO dell'organizzazione. Ad esempio:



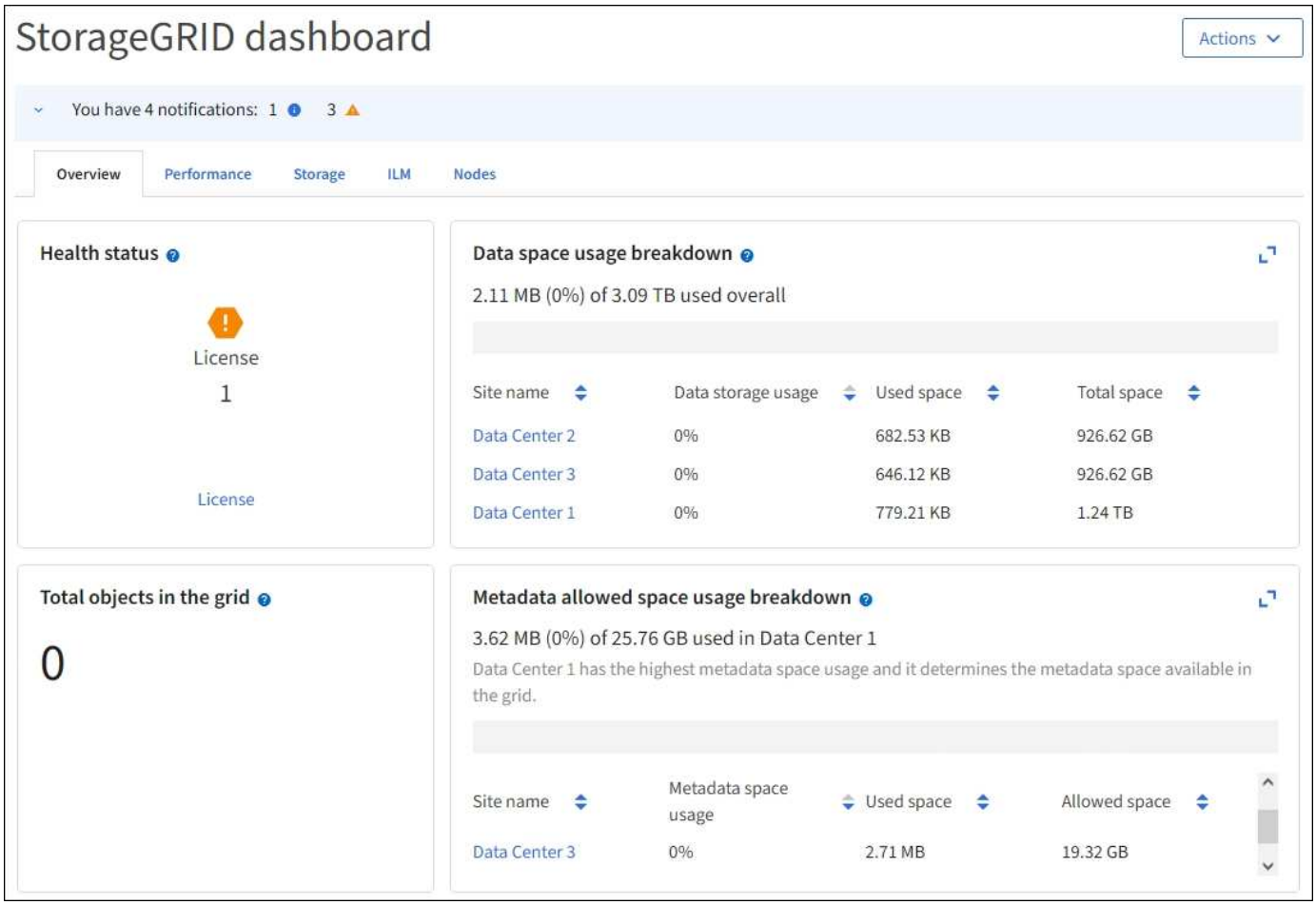
- Se StorageGRID utilizza SSO e si è precedentemente effettuato l'accesso a Grid Manager o a un account tenant:

  i. Inserire **0** (l'ID account per Grid Manager) o selezionare **Grid Manager** se compare nell'elenco degli account recenti.

ii. Selezionare **Accedi**.

iii. Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

Una volta effettuato l'accesso, viene visualizzata la home page di Grid Manager, che include la dashboard. Per informazioni sulle informazioni fornite, vedere "Visualizzare e gestire la dashboard".



Accedere a un altro nodo amministratore

Per accedere a un altro nodo amministratore, procedere come segue.

Non si utilizza SSO

Fasi

1. Nella barra degli indirizzi del browser, inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Includere il numero di porta come richiesto.
2. Immettere il nome utente e la password per Grid Manager.
3. Selezionare **Accedi**.

Utilizzo di SSO

Se StorageGRID utilizza SSO ed è stato effettuato l'accesso a un nodo amministratore, è possibile accedere ad altri nodi amministrativi senza dover effettuare nuovamente l'accesso.

Fasi

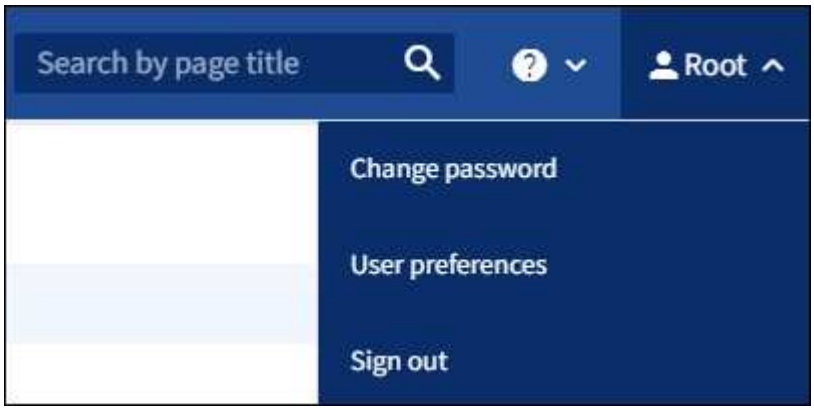
1. Inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione nella barra degli indirizzi del browser.
2. Se la sessione SSO è scaduta, immettere nuovamente le credenziali.

Disconnettersi da Grid Manager

Una volta terminato l'utilizzo di Grid Manager, è necessario disconnettersi per garantire che gli utenti non autorizzati non possano accedere al sistema StorageGRID. La chiusura del browser potrebbe non disconnettersi dal sistema, in base alle impostazioni dei cookie del browser.

Fasi

1. Selezionare il nome utente nell'angolo in alto a destra.



2. Selezionare **Disconnetti**.

Opzione	Descrizione
SSO non in uso	Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso di Grid Manager. **Nota:** se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.
SSO attivato	Si è disconnessi da tutti i nodi di amministrazione ai quali si stava accedendo. Viene visualizzata la pagina di accesso a StorageGRID. **Grid Manager** è elencato come predefinito nell'elenco a discesa **Recent Accounts** (account recenti) e il campo **account ID** (ID account) mostra 0. **Nota:** se SSO è attivato e si è anche connessi al tenant manager, è necessario "disconnettersi dall'account tenant" a. "Disconnettersi da SSO".

Modificare la password

Gli utenti locali di Grid Manager possono modificare la propria password.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

Se si accede a StorageGRID come utente federato o se è attivato il Single Sign-on (SSO), non è possibile modificare la password in Grid Manager. È invece necessario modificare la password nell'origine dell'identità esterna, ad esempio Active Directory o OpenLDAP.

Fasi

1. Dall'intestazione Grid Manager, selezionare ***Nome*** > **Modifica password**.
2. Inserire la password corrente.
3. Digitare una nuova password.

   La password deve contenere almeno 8 e non più di 32 caratteri. Le password distinguono tra maiuscole e minuscole.

4. Immettere nuovamente la nuova password.
5. Selezionare **Salva**.

Visualizzare le informazioni sulla licenza StorageGRID

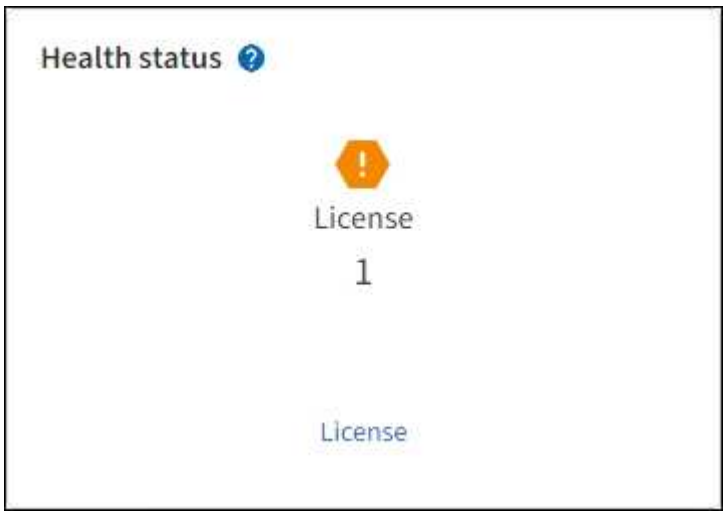
Se necessario, è possibile visualizzare le informazioni sulla licenza del sistema StorageGRID, ad esempio la capacità di storage massima del grid.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

In caso di problemi con la licenza software per questo sistema StorageGRID, la scheda di stato dello stato di salute sul dashboard include un'icona di stato della licenza e un collegamento **licenza**. Il numero indica il numero di problemi relativi alla licenza.



Fasi

1. Accedere alla pagina License (licenza) effettuando una delle seguenti operazioni:
   - Selezionare **MANUTENZIONE** > **sistema** > **licenza**.
   - Dalla scheda Health status (Stato) sul dashboard, selezionare l'icona License status (Stato licenza) o il collegamento **License** (licenza).

     Questo collegamento viene visualizzato solo in caso di problemi con la licenza.

2. Visualizzare i dettagli di sola lettura per la licenza corrente:
    - ID sistema StorageGRID, che è il numero di identificazione univoco per l'installazione di StorageGRID
    - Numero di serie della licenza
    - Tipo di licenza, **Perpetual** o **Subscription**
    - Capacità di storage concessa in licenza del grid
    - Capacità di storage supportata
    - Data di fine della licenza. **N/A** appare per una licenza perpetua.
    - Data di fine supporto

      Questa data viene letta dal file di licenza corrente e potrebbe non essere aggiornata se si estende o si rinnova il contratto del servizio di supporto dopo aver ottenuto il file di licenza. Per aggiornare questo valore, vedere "Aggiornare le informazioni sulla licenza StorageGRID". È inoltre possibile visualizzare la data di fine effettiva del contratto utilizzando Active IQ.

    - Contenuto del file di testo della licenza

Aggiornare le informazioni sulla licenza StorageGRID

È necessario aggiornare le informazioni di licenza per il sistema StorageGRID in qualsiasi momento in cui i termini della licenza cambiano. Ad esempio, è necessario aggiornare le informazioni sulla licenza se si acquista ulteriore capacità di storage per il grid.

Prima di iniziare

- Si dispone di un nuovo file di licenza da applicare al sistema StorageGRID.
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Si dispone della passphrase di provisioning.

Fasi

1. Selezionare **MANUTENZIONE** > **sistema** > **licenza**.
2. Nella sezione Aggiorna licenza, selezionare **Sfoglia**.
3. Individuare e selezionare il nuovo file di licenza (`.txt`).

   Il nuovo file di licenza viene validato e visualizzato.

4. Inserire la passphrase di provisioning.
5. Selezionare **Salva**.

Utilizzare l'API

Utilizzare l'API Grid Management

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Grid Management invece dell'interfaccia utente di Grid Manager. Ad esempio, è possibile utilizzare l'API per automatizzare le operazioni o creare più entità, ad esempio gli utenti, più rapidamente.

Risorse di alto livello

L'API Grid Management fornisce le seguenti risorse di primo livello:

- `/grid`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate.
- `/org`: L'accesso è limitato agli utenti che appartengono a un gruppo LDAP locale o federato per un account tenant. Per ulteriori informazioni, vedere "Utilizzare un account tenant".
- `/private`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate. Le API private sono soggette a modifiche senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

Emettere richieste API

L'API Grid Management utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che consente a sviluppatori e non sviluppatori di eseguire operazioni in tempo reale in StorageGRID con l'API.

L'interfaccia utente di Swagger fornisce dettagli completi e documentazione per ogni operazione API.

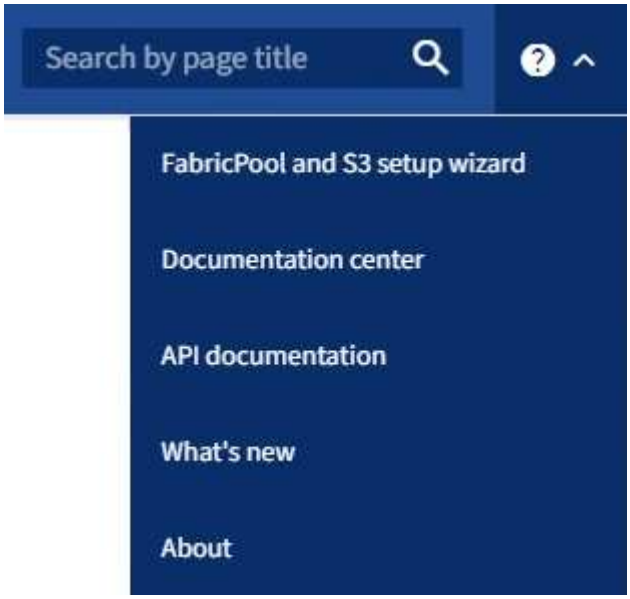
Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

> Tutte le operazioni API eseguite utilizzando la pagina web API Docs sono operazioni live. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Fasi

1. Dall'intestazione Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.



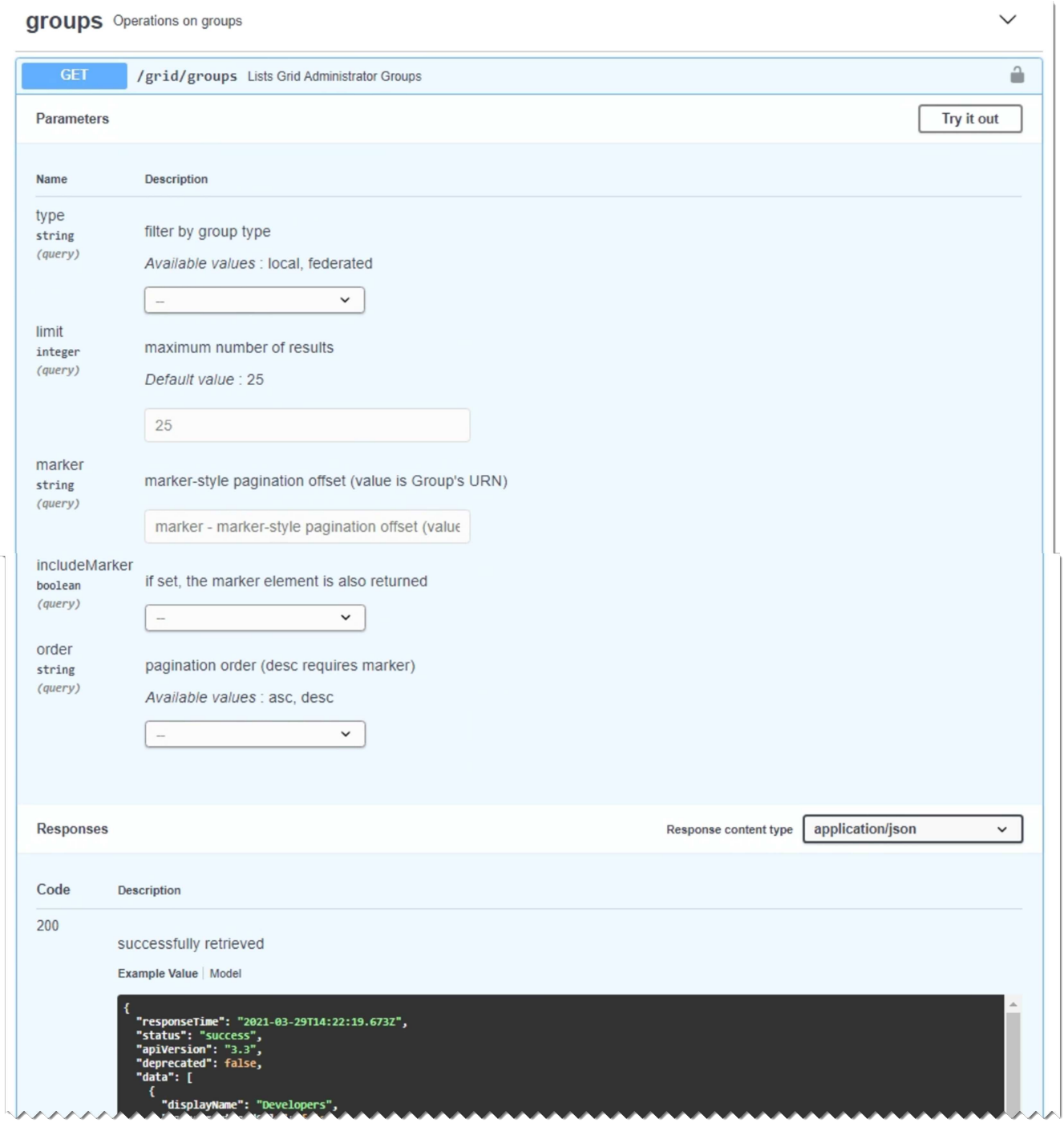
2. Per eseguire un'operazione con l'API privata, selezionare **Vai alla documentazione API privata** nella pagina API di gestione StorageGRID.

   Le API private sono soggette a modifiche senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

3. Selezionare l'operazione desiderata.

   Quando si espande un'operazione API, è possibile visualizzare le azioni HTTP disponibili, ad esempio GET, PUT, UPDATE ed DELETE.

4. Selezionare un'azione HTTP per visualizzare i dettagli della richiesta, tra cui l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le possibili risposte.



5. Determinare se la richiesta richiede parametri aggiuntivi, ad esempio un ID utente o un gruppo. Quindi, ottenere questi valori. Potrebbe essere necessario emettere prima una richiesta API diversa per ottenere le informazioni necessarie.

6. Determinare se è necessario modificare il corpo della richiesta di esempio. In tal caso, è possibile selezionare **modello** per conoscere i requisiti di ciascun campo.
7. Selezionare **Provalo**.
8. Fornire i parametri richiesti o modificare il corpo della richiesta secondo necessità.
9. Selezionare **Esegui**.
10. Esaminare il codice di risposta per determinare se la richiesta ha avuto esito positivo.

Operazioni API di Grid Management

L'API Grid Management organizza le operazioni disponibili nelle seguenti sezioni.

Questo elenco include solo le operazioni disponibili nell'API pubblica.

- **Account**: Operazioni per la gestione degli account del tenant di storage, inclusa la creazione di nuovi account e il recupero dell'utilizzo dello storage per un determinato account.
- **Alarms**: Operazioni per elencare gli allarmi correnti (sistema legacy) e restituire informazioni sullo stato della griglia, inclusi gli avvisi correnti e un riepilogo degli stati di connessione del nodo.
- **Alert-history**: Operazioni su avvisi risolti.
- **Ricevitori di avvisi**: Operazioni sui destinatari di notifiche di avvisi (e-mail).
- **Alert-rules**: Operazioni sulle regole di allerta.
- **Silenzi di allerta**: Operazioni di silenzi di allerta.
- **Alerts**: Operazioni sugli avvisi.
- **Audit**: Operazioni per elencare e aggiornare la configurazione dell'audit.
- **Auth**: Operazioni per l'autenticazione della sessione utente.

  L'API Grid Management supporta lo schema di autenticazione del token del bearer. Per effettuare l'accesso, inserisci un nome utente e una password nel corpo JSON della richiesta di autenticazione (ovvero `POST /api/v3/authorize`). Se l'utente viene autenticato correttamente, viene restituito un token di sicurezza. Questo token deve essere fornito nell'intestazione delle richieste API successive ("Authorization: Bearer *token*"). Il token scade dopo 16 ore.

  Se per il sistema StorageGRID è attivato il single sign-on, è necessario eseguire diversi passaggi per l'autenticazione. Vedere "autenticazione nell'API se è attivato il single sign-on".

  Per informazioni sul miglioramento della protezione dell'autenticazione, vedere "protezione contro la contraffazione delle richieste tra siti".

- **Certificati-client**: Operazioni per configurare i certificati client in modo che sia possibile accedere in modo sicuro a StorageGRID utilizzando strumenti di monitoraggio esterni.
- **Config**: Operazioni relative alla release del prodotto e alle versioni dell'API Grid Management. È possibile elencare la versione del prodotto e le principali versioni dell'API Grid Management supportate da tale release ed è possibile disattivare le versioni obsolete dell'API.
- **Disattivato-funzioni**: Operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **dns-servers**: Operazioni per elencare e modificare i server DNS esterni configurati.
- **Dettagli unità**: Operazioni su unità per modelli di appliance di archiviazione specifici.

- **Nomi-dominio-endpoint**: Operazioni per elencare e modificare i nomi di dominio degli endpoint S3.
- **Erasure coding**: Operazioni sui profili di erasure coding.
- **Espansione**: Operazioni di espansione (a livello di procedura).
- **Expansion-node**: Operazioni di espansione (a livello di nodo).
- **Expansion-sites**: Operazioni di espansione (a livello di sito).
- **Grid-networks**: Operazioni per elencare e modificare l'elenco Grid Network.
- **Grid-password**: Operazioni per la gestione delle password grid.
- **Gruppi**: Operazioni per gestire i gruppi di amministratori di griglia locali e recuperare i gruppi di amministratori di griglia federati da un server LDAP esterno.
- **Identity-source**: Operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **ilm**: Operazioni sulla gestione del ciclo di vita delle informazioni (ILM).
- **Procedure in corso**: Recupera le procedure di manutenzione attualmente in corso.
- **Licenza**: Operazioni per recuperare e aggiornare la licenza StorageGRID.
- **Logs**: Operazioni per la raccolta e il download dei file di log.v
- **Metriche**: Operazioni su metriche StorageGRID, incluse query metriche istantanee in un singolo punto nel tempo e query metriche di intervallo in un intervallo di tempo. L'API Grid Management utilizza lo strumento di monitoraggio dei sistemi Prometheus come origine dei dati back-end. Per informazioni sulla creazione di query Prometheus, visitare il sito Web Prometheus.

> Metriche che includono `private` i loro nomi sono destinati esclusivamente all'uso interno. Queste metriche sono soggette a modifiche senza preavviso tra le versioni di StorageGRID.

- **Node-details**: Operazioni sui dettagli del nodo.
- **Node-Health**: Operazioni sullo stato di salute del nodo.
- **Node-storage-state**: Operazioni sullo stato dello storage del nodo.
- **ntp-servers**: Operazioni per elencare o aggiornare server NTP (Network Time Protocol) esterni.
- **Objects**: Operazioni su oggetti e metadati di oggetti.
- **Recovery**: Operazioni per la procedura di recovery.
- **Recovery-package**: Operazioni per il download del Recovery Package.
- **Regioni**: Operazioni per visualizzare e creare regioni.
- **s3-Object-lock**: Operazioni sulle impostazioni generali di blocco oggetti S3.
- **Server-certificate**: Operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp**: Operazioni sulla configurazione SNMP corrente.
- **Filigrane-archiviazione**: Filigrane del nodo di archiviazione.
- **Classi di traffico**: Operazioni per le policy di classificazione del traffico.
- **Untrusted-client-network**: Operazioni sulla configurazione Untrusted Client Network.
- **Utenti**: Operazioni per visualizzare e gestire gli utenti di Grid Manager.

L'API Grid Management utilizza il controllo delle versioni per supportare aggiornamenti senza interruzioni.

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

`https://hostname_or_ip_address/api/v4/authorize`

La versione principale dell'API viene modificata quando vengono apportate modifiche che sono *non compatibili* con le versioni precedenti. La versione secondaria dell'API viene modificata quando vengono apportate modifiche che sono *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o di nuove proprietà.

Nell'esempio seguente viene illustrato il modo in cui la versione dell'API viene modificata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Versione precedente	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene attivata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova release di funzionalità di StorageGRID, si continua ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.

> È possibile configurare le versioni supportate. Vedere la sezione **config** della documentazione Swagger API per "API di Grid Management" per ulteriori informazioni. È necessario disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API per utilizzare la versione più recente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Deprecated: True"
- Il corpo di risposta JSON include "deprecato": Vero
- Viene aggiunto un avviso obsoleto a nms.log. Ad esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinare quali versioni API sono supportate nella release corrente

Utilizzare `GET /versions` Richiesta API per restituire un elenco delle versioni principali dell'API supportate. Questa richiesta si trova nella sezione **config** della documentazione dell'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione dell'API utilizzando un parametro path (`/api/v4`) o un'intestazione (`Api-Version: 4`). Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protezione contro la contraffazione delle richieste (CSRF)

Puoi contribuire a proteggere dagli attacchi di cross-site request forgery (CSRF) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se attivarla al momento dell'accesso.

Un utente malintenzionato in grado di inviare una richiesta a un sito diverso (ad esempio con UN HTTP Form POST) può causare l'esecuzione di determinate richieste utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggere dagli attacchi CSRF utilizzando token CSRF. Se attivato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro POST-body specifico.

Per attivare la funzione, impostare `csrfToken` parametro a. `true` durante l'autenticazione. L'impostazione predefinita è `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando è vero, un `GridCsrfToken` Il cookie viene impostato con un valore casuale per l'accesso a Grid Manager e a. `AccountCsrfToken` Il cookie viene impostato con un valore casuale per l'accesso a Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere una delle seguenti opzioni:

- Il `X-Csrf-Token` Header, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo con codifica a modulo: A. `csrfToken` parametro del corpo della richiesta codificato dal modulo.

Per ulteriori esempi e dettagli, consultare la documentazione API online.

> Le richieste che dispongono di un set di cookie token CSRF applicheranno anche l'intestazione "Content-Type: Application/json" per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzare l'API se è attivato il Single Sign-on

Utilizzare l'API se è attivato il single sign-on (Active Directory)

Se lo hai fatto "SSO (Single Sign-on) configurato e abilitato" Se si utilizza Active Directory come provider SSO, è necessario emettere una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Accedere all'API se è attivato il Single Sign-on

Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO.

Prima di iniziare

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare uno dei seguenti esempi:

- Il `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione di StorageGRID (`./rpms` Per Red Hat Enterprise Linux, `./debs` Per Ubuntu o Debian, e. `./vsphere` Per VMware).

- Un esempio di workflow di richieste di curl.

  Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: `A valid SubjectConfirmation was not found on this Response`.

  > L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: `Unsupported SAML version`.

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
   - Utilizzare `storagegrid-ssoauth.py` Script Python. Andare alla fase 2.
   - USA richieste di curl. Passare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` Passare lo script all'interprete Python ed eseguirlo.

   Quando richiesto, inserire i valori per i seguenti argomenti:

   - Il metodo SSO. Immettere ADFS o adfs.
   - Il nome utente SSO
   - Il dominio in cui è installato StorageGRID
   - L'indirizzo per StorageGRID
   - L'ID account tenant, se si desidera accedere all'API di gestione tenant.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.

   a. Dichiarare le variabili necessarie per l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

Per accedere all'API Grid Management, utilizzare 0 AS `TENANTACCOUNTID`.

b. Per ricevere un URL di autenticazione firmato, inviare una richiesta DI POST a. `/api/v3/authorize-saml`E rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per `TENANTACCOUNTID`. I risultati verranno passati a. `python -m json.tool` Per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La risposta per questo esempio include un URL firmato con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salvare `SAMLRequest` dalla risposta per l'utilizzo nei comandi successivi.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Ottenere un URL completo che includa l'ID della richiesta del client da ad FS.

Un'opzione consiste nel richiedere il modulo di accesso utilizzando l'URL della risposta precedente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

La risposta include l'ID della richiesta del client:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salvare l'ID della richiesta del client dalla risposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Inviare le credenziali all'azione del modulo della risposta precedente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS restituisce un reindirizzamento 302, con informazioni aggiuntive nelle intestazioni.

> Se l'autenticazione a più fattori (MFA) è attivata per il sistema SSO, il post del modulo conterrà anche la seconda password o altre credenziali.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Salvare `MSISAuth` cookie dalla risposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Inviare una richiesta GET alla posizione specificata con i cookie del POST di autenticazione.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Le intestazioni delle risposte conterranno le informazioni della sessione di ad FS per un utilizzo successivo della disconnessione e il corpo della risposta conterrà la risposta SAMLin un campo di forma nascosto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Salvare `SAMLResponse` dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizzando il salvato `SAMLResponse`, Creare un StorageGRID`/api/saml-response` Richiesta di generazione di un token di autenticazione StorageGRID.

Per `RelayState`, Utilizzare l'ID account tenant o utilizzare 0 se si desidera accedere all'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La risposta include il token di autenticazione.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salvare il token di autenticazione nella risposta con nome `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi utilizzare `MYTOKEN` Per le altre richieste, in modo simile a come si utilizza l'API se SSO non viene utilizzato.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management.
Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO

A proposito di questa attività

Se necessario, è possibile disconnettersi dall'API StorageGRID disconnettendosi dalla singola pagina di disconnessione dell'organizzazione. In alternativa, è possibile attivare il logout singolo (SLO) da StorageGRID, che richiede un token bearer StorageGRID valido.

Fasi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Salvare l'URL di disconnessione.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione API-only.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Eliminare il token del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se `cookie "sso=true" non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

R `204 No Content` la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```

Utilizzare l'API se è attivato il single sign-on (Azure)

Se lo hai fatto "SSO (Single Sign-on) configurato e abilitato" Inoltre, come provider SSO, Azure consente di utilizzare due script di esempio per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Accedere all'API se Azure Single Sign-on è attivato

Queste istruzioni sono valide se si utilizza Azure come provider di identità SSO

Prima di iniziare

- Si conoscono l'indirizzo e-mail SSO e la password di un utente federato che appartiene a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare i seguenti script di esempio:

- Il `storagegrid-ssoauth-azure.py` Script Python
- Il `storagegrid-ssoauth-azure.js` Script node.js

Entrambi gli script si trovano nella directory dei file di installazione di StorageGRID (`./rpms` Per Red Hat Enterprise Linux, `./debs` Per Ubuntu o Debian, e. `./vsphere` Per VMware).

Per scrivere la propria integrazione API con Azure, vedere `storagegrid-ssoauth-azure.py` script. Lo script Python effettua due richieste direttamente a StorageGRID (prima per ottenere la SAMLRequest e poi per ottenere il token di autorizzazione) e chiama anche lo script Node.js per interagire con Azure per eseguire le operazioni SSO.

Le operazioni SSO possono essere eseguite utilizzando una serie di richieste API, ma non è semplice. Il modulo Puppeteer Node.js viene utilizzato per scrapare l'interfaccia SSO di Azure.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: `Unsupported SAML version`.

Fasi

1. Installare le dipendenze richieste, come indicato di seguito:

a. Installare Node.js (vedere "https://nodejs.org/en/download/").

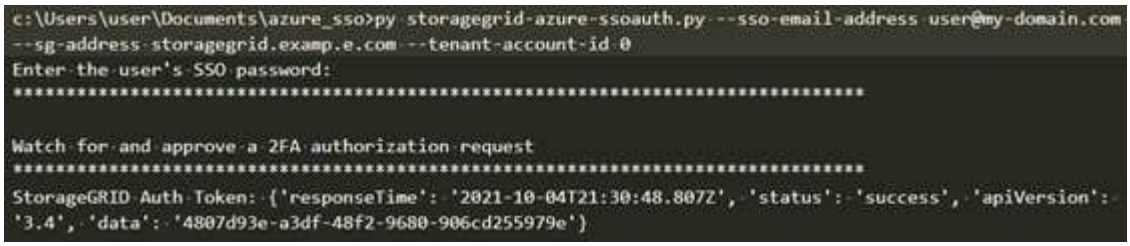
b. Installare i moduli Node.js richiesti (puppeteer e jsdom):

```
npm install -g <module>
```

2. Passare lo script Python all'interprete Python per eseguirlo.

   Lo script Python chiamerà quindi lo script Node.js corrispondente per eseguire le interazioni SSO di Azure.

3. Quando richiesto, immettere i valori per i seguenti argomenti (o passarli utilizzando i parametri):
   - Indirizzo e-mail SSO utilizzato per accedere ad Azure
   - L'indirizzo per StorageGRID
   - L'ID account tenant, se si desidera accedere all'API di gestione tenant
4. Quando richiesto, inserire la password e prepararsi a fornire un'autorizzazione MFA ad Azure, se richiesto.



> Lo script presuppone che l'autenticazione MFA venga eseguita utilizzando Microsoft Authenticator. Potrebbe essere necessario modificare lo script per supportare altre forme di MFA (ad esempio l'immissione di un codice ricevuto in un messaggio di testo).

Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

Utilizzare l'API se è attivato il Single Sign-on (PingFederate)

Se lo hai fatto "SSO (Single Sign-on) configurato e abilitato" E si utilizza PingFederate come provider SSO, è necessario emettere una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Accedere all'API se è attivato il Single Sign-on

Queste istruzioni sono valide se si utilizza PingFederate come provider di identità SSO

Prima di iniziare

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare uno dei seguenti esempi:

- Il `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione di StorageGRID (`./rpms` Per Red Hat Enterprise Linux, `./debs` Per Ubuntu o Debian, e. `./vsphere` Per

VMware).

- Un esempio di workflow di richieste di curl.

  Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: `A valid SubjectConfirmation was not found on this Response`.

  L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

  Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: `Unsupported SAML version`.

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
   - Utilizzare `storagegrid-ssoauth.py` Script Python. Andare alla fase 2.
   - USA richieste di curl. Passare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` Passare lo script all'interprete Python ed eseguirlo.

   Quando richiesto, inserire i valori per i seguenti argomenti:

   - Il metodo SSO. È possibile inserire qualsiasi variazione di "pingfederate" (PINGFEDERATE, pingfederate e così via).
   - Il nome utente SSO
   - Il dominio in cui è installato StorageGRID. Questo campo non viene utilizzato per PingFederate. È possibile lasciare vuoto il campo o inserire un valore qualsiasi.
   - L'indirizzo per StorageGRID
   - L'ID account tenant, se si desidera accedere all'API di gestione tenant.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.

   a. Dichiarare le variabili necessarie per l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

Per accedere all'API Grid Management, utilizzare 0 AS `TENANTACCOUNTID`.

b. Per ricevere un URL di autenticazione firmato, inviare una richiesta DI POST a. `/api/v3/authorize-saml`E rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per TENANTACCOUNTID. I risultati verranno passati a python -m json.tool per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La risposta per questo esempio include un URL firmato con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salvare `SAMLRequest` dalla risposta per l'utilizzo nei comandi successivi.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Esportare la risposta e il cookie e visualizzare la risposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Esportare il valore 'pf.adapterId' e visualizzare la risposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Esportare il valore 'href' (rimuovere la barra finale /) e visualizzare la risposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Esportare il valore "azione":

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Invia cookie con credenziali:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Salvare `SAMLResponse` dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizzando il salvato `SAMLResponse`, Creare un StorageGRID `/api/saml-response` Richiesta di generazione di un token di autenticazione StorageGRID.

Per `RelayState`, Utilizzare l'ID account tenant o utilizzare 0 se si desidera accedere all'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La risposta include il token di autenticazione.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salvare il token di autenticazione nella risposta con nome `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi utilizzare `MYTOKEN` Per le altre richieste, in modo simile a come si utilizza l'API se SSO non viene utilizzato.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management.
Queste istruzioni sono valide se si utilizza PingFederate come provider di identità SSO

A proposito di questa attività

Se necessario, è possibile disconnettersi dall'API StorageGRID disconnettendosi dalla singola pagina di disconnessione dell'organizzazione. In alternativa, è possibile attivare il logout singolo (SLO) da StorageGRID, che richiede un token bearer StorageGRID valido.

Fasi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Salvare l'URL di disconnessione.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione API-only.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Eliminare il token del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se `cookie "sso=true" non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

R `204 No Content` la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```

Disattivare le funzioni con l'API

È possibile utilizzare l'API di gestione griglia per disattivare completamente alcune funzionalità nel sistema StorageGRID. Quando una funzione viene disattivata, non è possibile assegnare a nessuno le autorizzazioni per eseguire le attività correlate a tale funzione.

A proposito di questa attività

Il sistema Disattivato consente di impedire l'accesso a determinate funzioni del sistema StorageGRID. La disattivazione di una funzione è l'unico modo per impedire all'utente root o agli utenti appartenenti a gruppi di amministratori con autorizzazione **Root Access** di utilizzare tale funzione.

Per comprendere come questa funzionalità potrebbe essere utile, considerare il seguente scenario:

L'azienda A è un provider di servizi che affitta la capacità di storage del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei titolari di leasing, la Società A desidera garantire che i propri dipendenti non possano mai accedere a alcun account tenant dopo l'implementazione dell'account.

*L'azienda A è in grado di raggiungere questo obiettivo utilizzando il sistema Deactivate Features nell'API Grid Management. Disattivando completamente la funzione **Cambia password root tenant** in Grid Manager (sia l'interfaccia utente che l'API), la società A può garantire che nessun utente Admin, incluso l'utente root e gli utenti appartenenti a gruppi con l'autorizzazione **Root access**, possa modificare la password per qualsiasi utente root dell'account tenant.*

Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia. Vedere "Utilizzare l'API Grid Management".
2. Individuare l'endpoint Deactivate Features.
3. Per disattivare una funzione, ad esempio Modifica password root tenant, inviare un corpo all'API come segue:

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Al termine della richiesta, la funzione Modifica password root tenant viene disattivata. L'autorizzazione di gestione **Modifica password principale tenant** non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password principale per un tenant non riesce con "403 Proibito".

Riattivare le funzioni disattivate

Per impostazione predefinita, è possibile utilizzare l'API Grid Management per riattivare una funzione disattivata. Tuttavia, se si desidera evitare che le funzioni disattivate vengano riattivate, è possibile disattivare la funzione **ActivateFeatures**.

> Impossibile riattivare la funzione **ActivateCaratures**. Se decidi di disattivare questa funzione, tieni presente che perderai in modo permanente la possibilità di riattivare qualsiasi altra funzione disattivata. È necessario contattare il supporto tecnico per ripristinare eventuali funzionalità perse.

Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia.

2. Individuare l'endpoint Deactivate Features.
3. Per riattivare tutte le funzioni, inviare un corpo all'API come segue:

```
{ "grid": null }
```

Una volta completata la richiesta, tutte le funzioni, inclusa la funzione Change tenant root password, vengono riattivate. L'autorizzazione di gestione **Change tenant root password** viene ora visualizzata nell'interfaccia utente e tutte le richieste API che tentano di modificare la password root per un tenant avranno esito positivo, presupponendo che l'utente disponga dell'autorizzazione di gestione **Root access** o **Change tenant root password**.

> L'esempio precedente causa la riattivazione di *tutte* le funzioni disattivate. Se sono state disattivate altre funzioni che devono rimanere disattivate, è necessario specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzione Modifica password root tenant e continuare a disattivare la funzione di riconoscimento allarme, inviare la seguente richiesta PUT:
>
> ```
> { "grid": { "alarmAcknowledgment": true } }
> ```

Controllo dell'accesso a StorageGRID

Control StorageGRID access: Panoramica

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.

Utilizzo di "federazione delle identità" rende la configurazione "gruppi" e. "utenti" Più veloce 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 diverse "permessi" 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). Dopo di lei "Configurare e abilitare SSO", 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.

Modificare la passphrase di provisioning

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 la passphrase" secondo necessità.

Modificare le password della console dei nodi

Ciascun nodo della griglia dispone di una password univoca per la console del nodo, che deve essere utilizzata per accedere al nodo come "admin" utilizzando SSH o all'utente root con una connessione VM/console fisica. In base alle esigenze, è possibile "modificare la password della console del nodo" per ogni nodo.

Modificare la passphrase di provisioning

Utilizzare questa procedura per modificare la passphrase di provisioning StorageGRID. La passphrase è necessaria per le procedure di ripristino, espansione e manutenzione. La passphrase è necessaria anche per scaricare i backup del pacchetto di ripristino che includono le informazioni sulla topologia della griglia, le password della console del nodo della griglia e le chiavi di crittografia per il sistema StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone delle autorizzazioni di accesso Maintenance o Root.
- Si dispone della passphrase di provisioning corrente.

A proposito di questa attività

La passphrase di provisioning è necessaria per molte procedure di installazione e manutenzione e per "Download del pacchetto di ripristino". La passphrase di provisioning non è elencata in `Passwords.txt` file. Assicurarsi di documentare la passphrase di provisioning e conservarla in una posizione sicura.

Fasi

1. Selezionare **CONFIGURATION** > **Access control**> **Grid passwords**.
2. In **Cambia passphrase di provisioning**, selezionare **effettua una modifica**
3. Inserire la passphrase di provisioning corrente.
4. Inserire la nuova passphrase. La passphrase deve contenere almeno 8 e non più di 32 caratteri. Le passphrase sono sensibili al maiuscolo/minuscolo.
5. Memorizzare la nuova passphrase di provisioning in una posizione sicura. È necessario per le procedure di installazione, espansione e manutenzione.
6. Immettere nuovamente la nuova passphrase e selezionare **Save** (Salva).

   Al termine della modifica della passphrase di provisioning, il sistema visualizza un banner verde di successo.

7. Selezionare **Recovery Package** (pacchetto di ripristino).
8. Inserire la nuova passphrase di provisioning per scaricare il nuovo Recovery Package.

> Dopo aver modificato la passphrase di provisioning, è necessario scaricare immediatamente un nuovo pacchetto di ripristino. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

Modificare le password della console dei nodi

Ogni nodo della griglia dispone di una password univoca per la console del nodo, che è necessario accedere al nodo. Seguire questa procedura per modificare ogni password univoca della console dei nodi per ciascun nodo della griglia.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning corrente.

A proposito di questa attività

Utilizzare la password della console del nodo per accedere a un nodo come "admin" utilizzando SSH o all'utente root su una connessione VM/console fisica. Il processo di modifica della password della console dei nodi crea nuove password per ciascun nodo della griglia e le memorizza in un aggiornato `Passwords.txt` nel pacchetto di ripristino. Le password sono elencate nella colonna Password del file Passwords.txt.

> Esistono password di accesso SSH separate per le chiavi SSH utilizzate per la comunicazione tra i nodi. Questa procedura non modifica le password di accesso SSH.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Grid passwords**.
2. In **Cambia password console nodo**, selezionare **effettua una modifica**.

Inserire la passphrase di provisioning

Fasi

1. Inserire la passphrase di provisioning per la griglia.
2. Selezionare **continua**.

Scarica il pacchetto di ripristino corrente

Prima di modificare le password della console dei nodi, scaricare il pacchetto di ripristino corrente. È possibile utilizzare le password in questo file se il processo di modifica della password non riesce per qualsiasi nodo.

Fasi

1. Selezionare **Download recovery package** (Scarica pacchetto di ripristino).

2. Copiare il file del pacchetto di ripristino (`.zip`) in due posizioni 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.

3. Selezionare **continua**.
4. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Yes** (Sì) se si desidera iniziare a modificare le password della console del nodo.

   Non puoi annullare questo processo dopo l'avvio.

Modificare le password della console dei nodi

All'avvio del processo di password della console dei nodi, viene generato un nuovo pacchetto di ripristino che include le nuove password. Quindi, le password vengono aggiornate su ciascun nodo.

Fasi

1. Attendere che venga generato il nuovo pacchetto di ripristino, che potrebbe richiedere alcuni minuti.
2. Selezionare **Scarica nuovo pacchetto di ripristino**.
3. Al termine del download:

   a. Aprire `.zip` file.

   b. Verificare che sia possibile accedere ai contenuti, incluso il `Passwords.txt` che contiene le nuove password della console dei nodi.

   c. Copiare il nuovo file del pacchetto di ripristino (`.zip`) in due posizioni sicure e separate.

      > Non sovrascrivere il vecchio pacchetto di ripristino.

   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.

4. Selezionare la casella di controllo per indicare che il nuovo pacchetto di ripristino è stato scaricato e che il contenuto è stato verificato.
5. Selezionare **Change node console passwords** (Modifica password console nodi) e attendere che tutti i nodi vengano aggiornati con le nuove password. L'operazione potrebbe richiedere alcuni minuti.

   Se le password vengono modificate per tutti i nodi, viene visualizzato un banner verde di successo. Passare alla fase successiva.

   Se si verifica un errore durante il processo di aggiornamento, un messaggio di intestazione indica il numero di nodi che non sono riusciti a modificare le password. Il sistema riprova automaticamente il processo su qualsiasi nodo che non ha modificato la password. Se il processo termina con alcuni nodi che non hanno ancora una password modificata, viene visualizzato il pulsante **Riprova**.

   Se l'aggiornamento della password non è riuscito per uno o più nodi:

   a. Esaminare i messaggi di errore elencati nella tabella.

   b. Risolvere i problemi.

   c. Selezionare **Riprova**.

Il nuovo tentativo modifica solo le password della console dei nodi sui nodi che non sono riusciti durante i precedenti tentativi di modifica della password.

6. Una volta modificate le password della console del nodo per tutti i nodi, eliminare primo pacchetto di ripristino scaricato.
7. Facoltativamente, utilizzare il collegamento **Recovery package** per scaricare una copia aggiuntiva del nuovo pacchetto di ripristino.

USA la federazione delle identità

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.

Configurare la federazione delle identità per Grid Manager

È possibile configurare la federazione delle identità in Grid Manager se si desidera che i gruppi amministrativi e gli utenti vengano gestiti in un altro sistema, ad esempio Active Directory, Azure Active Directory (Azure ad), OpenLDAP o Oracle Directory Server.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Si utilizza Active Directory, Azure ad, OpenLDAP o Oracle Directory Server come provider di identità.

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

- Se si intende utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere Linee guida per la configurazione di un server OpenLDAP.
- Se si prevede di attivare il Single Sign-on (SSO), è stata esaminata la "requisiti e considerazioni per il single sign-on".
- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità utilizza TLS 1.2 o 1.3. Vedere "Crittografia supportata per le connessioni TLS in uscita".

A proposito di questa attività

È possibile configurare un'origine identità per Grid Manager se si desidera importare gruppi da un altro sistema, ad esempio Active Directory, Azure ad, OpenLDAP o Oracle Directory Server. È possibile importare i seguenti tipi di gruppi:

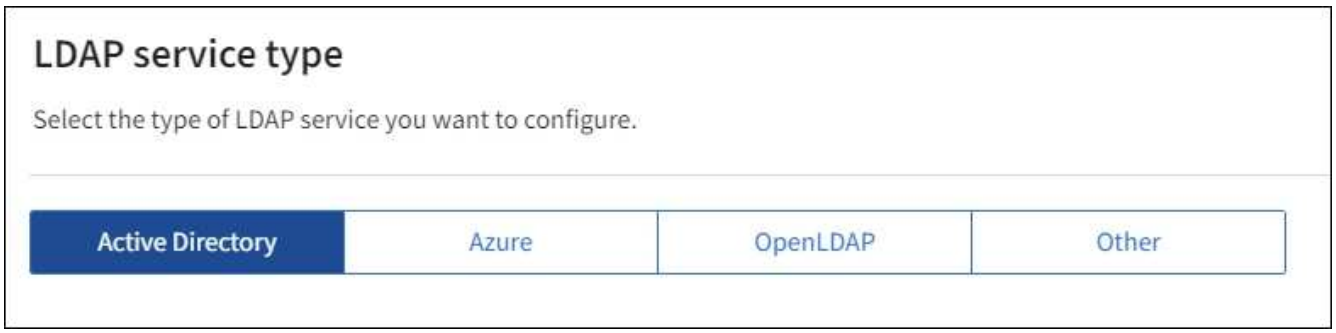
- Gruppi di amministratori. Gli utenti dei gruppi di amministrazione possono accedere a Grid Manager ed eseguire attività in base alle autorizzazioni di gestione assegnate al gruppo.
- Gruppi di utenti tenant per tenant che non utilizzano la propria origine di identità. Gli utenti dei gruppi di tenant possono accedere al tenant manager ed eseguire le attività in base alle autorizzazioni assegnate al gruppo nel tenant manager. Vedere "Creare un account tenant" e. "Utilizzare un account tenant" per ulteriori informazioni.

Inserire la configurazione

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Identity Federation**.

2. Selezionare **Enable Identity Federation** (attiva federazione identità).
3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.



   Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP. In caso contrario, passare alla fase successiva.
   - **User Unique Name** (Nome univoco utente): Il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a. `sAMAccountName` Per Active Directory e. `uid` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
   - **UUID utente**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a. `objectGUID` Per Active Directory e. `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Ogni valore dell'utente per l'attributo specificato deve essere un numero esadecimale a 32 cifre in formato a 16 byte o stringa, dove i trattini vengono ignorati.
   - **Group Unique Name** (Nome univoco gruppo): Il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a. `sAMAccountName` Per Active Directory e. `cn` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
   - **UUID gruppo**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a. `objectGUID` Per Active Directory e. `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale a 32 cifre nel formato a 16 byte o stringa, dove i trattini vengono ignorati.
5. Per tutti i tipi di servizio LDAP, inserire le informazioni richieste relative al server LDAP e alla connessione di rete nella sezione Configura server LDAP.
   - **Nome host**: Il nome di dominio completo (FQDN) o l'indirizzo IP del server LDAP.
   - **Port** (porta): Porta utilizzata per la connessione al server LDAP.

     La porta predefinita per STARTTLS è 389 e la porta predefinita per LDAPS è 636. Tuttavia, è possibile utilizzare qualsiasi porta purché il firewall sia configurato correttamente.

   - **Username**: Percorso completo del nome distinto (DN) per l'utente che si connette al server LDAP.

     Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome principale dell'utente.

     L'utente specificato deve disporre dell'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

- `sAMAccountName` oppure `uid`
- `objectGUID`, `entryUUID`, o. `nsuniqueid`
- `cn`
- `memberOf` oppure `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, e. `userPrincipalName`
- **Azure**: `accountEnabled` e. `userPrincipalName`

◦ **Password**: La password associata al nome utente.

> Se si modifica la password in futuro, è necessario aggiornarla in questa pagina.

◦ **DN base gruppo**: Il percorso completo del nome distinto (DN) per una sottostruttura LDAP che si desidera cercare gruppi. Nell'esempio di Active Directory (riportato di seguito), tutti i gruppi il cui nome distinto è relativo al DN di base (DC=storagegrid,DC=example,DC=com) possono essere utilizzati come gruppi federati.

> I valori **Group unique name** devono essere univoci all'interno del **Group base DN** a cui appartengono.

◦ **User base DN**: Percorso completo del nome distinto (DN) di una sottostruttura LDAP che si desidera cercare gli utenti.

> I valori **Nome univoco utente** devono essere univoci all'interno del **DN base utente** a cui appartengono.

◦ **Bind username format** (opzionale): Il modello di nome utente predefinito che StorageGRID deve utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il formato **bind username** perché può consentire agli utenti di accedere se StorageGRID non è in grado di collegarsi con l'account del servizio.

Immettere uno di questi modelli:

- **Modello UserPrincipalName (Active Directory e Azure)**: `[USERNAME]@*example*.com`
- **Modello di nome di accesso di livello inferiore (Active Directory e Azure)**: `*example*\[USERNAME]`
- **Modello nome distinto**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Includi **[NOME UTENTE]** esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), selezionare un'impostazione di protezione.
   ◦ **Usa STARTTLS**: Utilizza STARTTLS per proteggere le comunicazioni con il server LDAP. Si tratta dell'opzione consigliata per Active Directory, OpenLDAP o altro, ma questa opzione non è supportata per Azure.
   ◦ **Usa LDAPS**: L'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. Selezionare questa opzione per Azure.

- **Non utilizzare TLS**: Il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Azure.

> L'utilizzo dell'opzione **non utilizzare TLS** non è supportato se il server Active Directory applica la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

7. Se si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.
   - **Usa certificato CA del sistema operativo**: Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
   - **Usa certificato CA personalizzato**: Utilizza un certificato di protezione personalizzato.

     Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

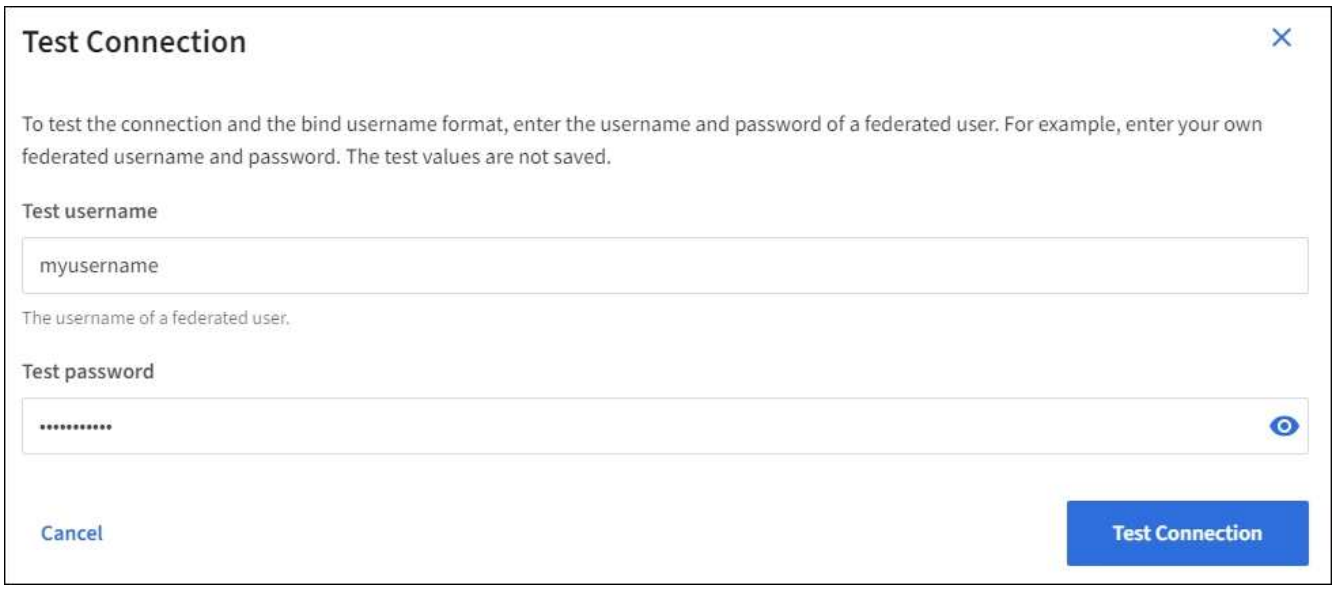
Verificare la connessione e salvare la configurazione

Dopo aver inserito tutti i valori, è necessario verificare la connessione prima di salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente BIND, se fornito.

Fasi

1. Selezionare **Test di connessione**.
2. Se non è stato fornito un formato nome utente BIND:
   - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.
   - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". Selezionare **Chiudi**. Quindi, risolvere eventuali problemi e verificare nuovamente la connessione.
3. Se è stato fornito un formato BIND Username, inserire il nome utente e la password di un utente federato valido.

   Ad esempio, inserire il proprio nome utente e la propria password. Non includere caratteri speciali nel nome utente, ad esempio @ o /.



- Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.
- Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente BIND o il nome utente e la password di prova non sono validi. Risolvere eventuali problemi e verificare nuovamente la connessione.

Forzare la sincronizzazione con l'origine dell'identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dall'origine dell'identità. È possibile forzare l'avvio della sincronizzazione se si desidera attivare o limitare le autorizzazioni utente il più rapidamente possibile.

Fasi

1. Vai alla pagina Identity Federation.
2. Selezionare **Sync server** nella parte superiore della pagina.

   Il processo di sincronizzazione potrebbe richiedere del tempo a seconda dell'ambiente in uso.

   L'avviso **errore di sincronizzazione federazione identità** viene attivato se si verifica un problema durante la sincronizzazione di utenti e gruppi federati dall'origine dell'identità.

Disattiva la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione di identità per gruppi e utenti. Quando la federazione delle identità è disattivata, non vi è alcuna comunicazione tra StorageGRID e l'origine delle identità. Tuttavia, tutte le impostazioni configurate vengono conservate, consentendo di riabilitare facilmente la federazione delle identità in futuro.

A proposito di questa attività

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non viene eseguita e non vengono generati avvisi o allarmi per gli account che non sono stati sincronizzati.
- La casella di controllo **Enable Identity Federation** (attiva federazione identità) è disattivata se Single Sign-on (SSO) è impostato su **Enabled** o **Sandbox Mode**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabled** prima di poter disattivare la federazione delle identità. Vedere "Disattiva single sign-on".

Fasi

1. Vai alla pagina Identity Federation.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).

Linee guida per la configurazione di un server OpenLDAP

Se si desidera utilizzare un server OpenLDAP per la federazione delle identità, è necessario configurare impostazioni specifiche sul server OpenLDAP.

Per le fonti di identità che non sono Active Directory o Azure, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare eventuali chiavi S3 per l'utente o rimuovere l'utente da tutti i gruppi.

MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo in "Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4".

Indicizzazione

È necessario configurare i seguenti attributi OpenLDAP con le parole chiave di indice specificate:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Inoltre, assicurarsi che i campi indicati nella guida per Nome utente siano indicizzati per ottenere prestazioni ottimali.

Consultare le informazioni relative alla manutenzione dell'appartenenza al gruppo inverso nella sezione "Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4".

Gestire i gruppi di amministratori

È possibile creare gruppi di amministratori per gestire le autorizzazioni di sicurezza per uno o più utenti amministratori. Gli utenti devono appartenere a un gruppo per poter accedere al sistema StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Se si intende importare un gruppo federated, la federazione delle identità è stata configurata e il gruppo federated esiste già nell'origine delle identità configurata.

Creare un gruppo di amministratori

I gruppi di amministratori consentono di determinare quali utenti possono accedere a quali funzionalità e operazioni in Grid Manager e nell'API Grid Management.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Admin groups**.
2. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federated.

- Creare un gruppo locale se si desidera assegnare le autorizzazioni agli utenti locali.
- Creare un gruppo federated per importare gli utenti dall'origine dell'identità.

Gruppo locale

Fasi

1. Selezionare **Gruppo locale**.
2. Inserire un nome visualizzato per il gruppo, che sarà possibile aggiornare in seguito secondo necessità. Ad esempio, "Maintenance Users" (manutenzione utenti) o "ILM Administrators" (amministratori ILM).
3. Immettere un nome univoco per il gruppo, che non è possibile aggiornare in seguito.
4. Selezionare **continua**.

Gruppo federated

Fasi

1. Selezionare **Federated group**.
2. Immettere il nome del gruppo che si desidera importare, esattamente come appare nell'origine identità configurata.
   - Per Active Directory e Azure, utilizzare sAMAccountName.
   - Per OpenLDAP, utilizzare il CN (Common Name).
   - Per un altro LDAP, utilizzare il nome univoco appropriato per il server LDAP.
3. Selezionare **continua**.

Gestire le autorizzazioni di gruppo

Fasi

1. Per la modalità **Access**, selezionare se gli utenti del gruppo possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nell'API Grid Management o se possono visualizzare solo impostazioni e funzionalità.
   - **Read-write** (valore predefinito): Gli utenti possono modificare le impostazioni ed eseguire le operazioni consentite dalle autorizzazioni di gestione.
   - **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API Grid Manager o Grid Management. Gli utenti locali di sola lettura possono modificare le proprie password.

     Se un utente appartiene a più gruppi e un gruppo è impostato su **sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Selezionare una o più opzioni "autorizzazioni del gruppo di amministrazione".

   È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti al gruppo non potranno accedere a StorageGRID.

3. Se si sta creando un gruppo locale, selezionare **continua**. Se si sta creando un gruppo federated, selezionare **Crea gruppo** e **fine**.

Aggiunta di utenti (solo gruppi locali)

Fasi

1. Facoltativamente, selezionare uno o più utenti locali per questo gruppo.

   Se non sono ancora stati creati utenti locali, è possibile salvare il gruppo senza aggiungere utenti. È possibile aggiungere questo gruppo all'utente nella pagina utenti. Vedere "Gestire gli utenti" per ulteriori informazioni.

2. Selezionare **Crea gruppo** e **fine**.

Visualizzare e modificare i gruppi di amministratori

È possibile visualizzare i dettagli dei gruppi esistenti, modificare un gruppo o duplicare un gruppo.

- Per visualizzare le informazioni di base per tutti i gruppi, consultare la tabella nella pagina gruppi.
- Per visualizzare tutti i dettagli di un gruppo specifico o per modificarlo, utilizzare il menu **azioni** o la pagina dei dettagli.

Attività	Menu delle azioni	Pagina dei dettagli
Visualizzare i dettagli del gruppo	a. Selezionare la casella di controllo del gruppo. b. Selezionare **azioni** > **Visualizza dettagli gruppo**.	Selezionare il nome del gruppo nella tabella.
Modifica nome visualizzato (solo gruppi locali)	a. Selezionare la casella di controllo del gruppo. b. Selezionare **azioni** > **Modifica nome gruppo**. c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome del gruppo per visualizzare i dettagli. b. Selezionare l'icona di modifica . c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).
Modificare la modalità di accesso o le autorizzazioni	a. Selezionare la casella di controllo del gruppo. b. Selezionare **azioni** > **Visualizza dettagli gruppo**. c. In alternativa, modificare la modalità di accesso del gruppo. d. Facoltativamente, selezionare o deselezionare "autorizzazioni del gruppo di amministrazione". e. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome del gruppo per visualizzare i dettagli. b. In alternativa, modificare la modalità di accesso del gruppo. c. Facoltativamente, selezionare o deselezionare "autorizzazioni del gruppo di amministrazione". d. Selezionare **Save Changes** (Salva modifiche).

Duplicare un gruppo

Fasi

1. Selezionare la casella di controllo del gruppo.
2. Selezionare **azioni** > **Duplica gruppo**.
3. Completare la procedura guidata Duplica gruppo.

Eliminare un gruppo

È possibile eliminare un gruppo di amministratori quando si desidera rimuovere il gruppo dal sistema e rimuovere tutte le autorizzazioni associate al gruppo. L'eliminazione di un gruppo di amministratori rimuove gli utenti dal gruppo, ma non li elimina.

Fasi

1. Dalla pagina Groups (gruppi), selezionare la casella di controllo per ciascun gruppo che si desidera rimuovere.
2. Selezionare **azioni** > **Elimina gruppo**.
3. Selezionare **Elimina gruppi**.

Autorizzazioni del gruppo di amministrazione

Quando si creano gruppi di utenti admin, si selezionano una o più autorizzazioni per controllare l'accesso a funzionalità specifiche di Grid Manager. È quindi possibile assegnare ciascun utente a uno o più di questi gruppi di amministratori per determinare quali attività possono essere eseguite dall'utente.

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti a tale gruppo non potranno accedere a Grid Manager o all'API Grid Management.

Per impostazione predefinita, qualsiasi utente appartenente a un gruppo che dispone di almeno un'autorizzazione può eseguire le seguenti attività:

- Accedi a Grid Manager
- Visualizza la dashboard
- Visualizzare le pagine dei nodi
- Monitorare la topologia della griglia
- Visualizzare gli avvisi correnti e risolti
- Visualizzazione degli allarmi correnti e storici (sistema legacy)
- Modifica della propria password (solo utenti locali)
- Visualizzare alcune informazioni fornite nelle pagine Configurazione e manutenzione

Interazione tra permessi e modalità di accesso

Per tutte le autorizzazioni, l'impostazione **modalità di accesso** del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni o se possono visualizzare solo le relative impostazioni e funzionalità. Se un utente appartiene a più gruppi e un gruppo è impostato su **sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

Le sezioni seguenti descrivono le autorizzazioni che è possibile assegnare durante la creazione o la modifica

di un gruppo amministrativo. Qualsiasi funzionalità non esplicitamente menzionata richiede l'autorizzazione **Root access**.

Accesso root

Questa autorizzazione consente di accedere a tutte le funzioni di amministrazione della griglia.

Riconoscere gli allarmi (legacy)

Questa autorizzazione consente di riconoscere e rispondere agli allarmi (sistema legacy). Tutti gli utenti che hanno effettuato l'accesso possono visualizzare gli allarmi correnti e storici.

Se si desidera che un utente monitori la topologia della griglia e riconosca solo gli allarmi, è necessario assegnare questa autorizzazione.

Modificare la password root del tenant

Questa autorizzazione consente di accedere all'opzione **Modifica password root** nella pagina tenant, consentendo di controllare chi può modificare la password per l'utente root locale del tenant. Questa autorizzazione viene utilizzata anche per la migrazione delle chiavi S3 quando è attivata la funzione di importazione delle chiavi S3. Gli utenti che non dispongono di questa autorizzazione non possono visualizzare l'opzione **Modifica password root**.

> Per consentire l'accesso alla pagina dei tenant, che contiene l'opzione **Modifica password root**, assegnare anche l'autorizzazione **account tenant**.

Configurazione della pagina della topologia della griglia

Questa autorizzazione consente di accedere alle schede di configurazione nella pagina **SUPPORTO** > **Strumenti** > **topologia griglia**.

ILM

Questa autorizzazione consente di accedere alle seguenti opzioni del menu **ILM**:

- Regole
- Policy
- Erasure coding
- Regioni
- Pool di storage

> Gli utenti devono disporre delle autorizzazioni **altra configurazione griglia** e **Configurazione della pagina topologia griglia** per gestire i gradi di storage.

Manutenzione

Gli utenti devono disporre dell'autorizzazione Maintenance per utilizzare queste opzioni:

- **CONFIGURAZIONE** > **controllo degli accessi**:
  - Password di rete
- **CONFIGURAZIONE** > **rete**:

    - Nomi di dominio degli endpoint S3
- **MANUTENZIONE** > **attività**:
    - Decommissionare
    - Espansione
    - Controllo dell'esistenza dell'oggetto
    - Recovery (recupero)
- **MANUTENZIONE** > **sistema**:
    - Pacchetto di recovery
    - Aggiornamento del software
- **SUPPORTO** > **Strumenti**:
    - Registri

Gli utenti che non dispongono dell'autorizzazione Maintenance possono visualizzare, ma non modificare, le seguenti pagine:

- **MANUTENZIONE** > **rete**:
    - Server DNS
    - Grid Network
    - Server NTP
- **MANUTENZIONE** > **sistema**:
    - Licenza
- **CONFIGURAZIONE** > **rete**:
    - Nomi di dominio degli endpoint S3
- **CONFIGURAZIONE** > **sicurezza**:
    - Certificati
- **CONFIGURAZIONE** > **monitoraggio**:
    - Server syslog e audit

Gestire gli avvisi

Questa autorizzazione consente di accedere alle opzioni per la gestione degli avvisi. Gli utenti devono disporre di questa autorizzazione per gestire silenzi, notifiche di avviso e regole di avviso.

Query sulle metriche

Questa autorizzazione consente di accedere a:

- **SUPPORTO** > **Strumenti** > pagina **metriche**
- Query di metriche Prometheus personalizzate utilizzando la sezione **metriche** dell'API Grid Management
- Schede dashboard di Grid Manager che contengono metriche

Ricerca dei metadati degli oggetti

Questa autorizzazione consente di accedere alla pagina **ILM** > **Object metadata lookup**.

Altra configurazione della griglia

Questa autorizzazione consente di accedere a ulteriori opzioni di configurazione della griglia.

> Per visualizzare queste opzioni aggiuntive, gli utenti devono anche disporre dell'autorizzazione **Grid topology page Configuration** (Configurazione pagina topologia griglia).

- **ILM**:
  - Gradi di storage
- **CONFIGURAZIONE** > **sistema**:
  - Opzioni di storage
- **SUPPORTO** > **Allarmi (legacy)**:
  - Eventi personalizzati
  - Allarmi globali
  - Configurazione della posta elettronica legacy
- **SUPPORTO** > **altro**:
  - Costo del collegamento

Amministratore dell'appliance di storage

Questa autorizzazione fornisce:

- Accesso al System Manager di e-Series SANtricity sulle appliance di storage tramite il Grid Manager.
- La possibilità di eseguire attività di troubleshooting e manutenzione nella scheda Manage drives (Gestione dischi) per le appliance che supportano queste operazioni.

Account tenant

Questa autorizzazione consente di:

- Accedere alla pagina tenant, in cui è possibile creare, modificare e rimuovere gli account tenant
- Visualizzare le policy di classificazione del traffico esistenti
- Visualizza le schede dashboard di Grid Manager che contengono i dettagli del tenant

Gestire gli utenti

È possibile visualizzare utenti locali e federati. È inoltre possibile creare utenti locali e assegnarli a gruppi di amministratori locali per determinare a quali funzioni di Grid Manager possono accedere questi utenti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Creare un utente locale

È possibile creare uno o più utenti locali e assegnare ciascun utente a uno o più gruppi locali. Le autorizzazioni del gruppo controllano a quali funzioni dell'API Grid Manager e Grid Management l'utente può accedere.

È possibile creare solo utenti locali. Utilizzare l'origine dell'identità esterna per gestire utenti e gruppi federati.

Grid Manager include un utente locale predefinito, denominato "root". Non puoi rimuovere l'utente root.

Se è attivato il Single Sign-on (SSO), gli utenti locali non possono accedere a StorageGRID.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Admin users**.
2. Selezionare **Crea utente**.

Immettere le credenziali dell'utente

Fasi

1. Immettere il nome completo dell'utente, un nome utente univoco e una password.
2. Se si desidera, selezionare **Sì** se l'utente non deve avere accesso all'API Grid Manager o Grid Management.
3. Selezionare **continua**.

Assegnare ai gruppi

Fasi

1. Facoltativamente, assegnare l'utente a uno o più gruppi per determinare le autorizzazioni dell'utente.

   Se non sono ancora stati creati gruppi, è possibile salvare l'utente senza selezionare i gruppi. È possibile aggiungere questo utente a un gruppo nella pagina gruppi.

   Se un utente appartiene a più gruppi, le autorizzazioni sono cumulative. Vedere "Gestire i gruppi di amministratori" per ulteriori informazioni.

2. Selezionare **Crea utente** e selezionare **fine**.

Visualizzare e modificare gli utenti locali

È possibile visualizzare i dettagli degli utenti locali e federati esistenti. È possibile modificare un utente locale per modificare il nome completo, la password o l'appartenenza al gruppo dell'utente. È inoltre possibile impedire temporaneamente a un utente di accedere a Grid Manager e all'API Grid Management.

È possibile modificare solo gli utenti locali. Utilizzare l'origine dell'identità esterna per gestire gli utenti federati.

- Per visualizzare le informazioni di base per tutti gli utenti locali e federati, consultare la tabella nella pagina utenti.
- Per visualizzare tutti i dettagli di un utente specifico, modificare un utente locale o modificare la password di un utente locale, utilizzare il menu **azioni** o la pagina dei dettagli.

  Tutte le modifiche vengono applicate alla successiva disconnessione dell'utente e all'accesso a Grid Manager.

  Gli utenti locali possono modificare le proprie password utilizzando l'opzione **Change password** (Modifica password) nel banner Grid Manager.

Attività	Menu delle azioni	Pagina dei dettagli
Visualizzare i dettagli dell'utente	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**.	Selezionare il nome dell'utente nella tabella.
Modifica nome completo (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Modifica nome completo**. c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare l'icona di modifica . c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).
Negare o consentire l'accesso a StorageGRID	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**. c. Selezionare la scheda Access (accesso). d. Selezionare **Sì** per impedire all'utente di accedere a Grid Manager o all'API Grid Management oppure selezionare **No** per consentire all'utente di accedere. e. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda Access (accesso). c. Selezionare **Sì** per impedire all'utente di accedere a Grid Manager o all'API Grid Management oppure selezionare **No** per consentire all'utente di accedere. d. Selezionare **Save Changes** (Salva modifiche).
Modifica della password (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**. c. Selezionare la scheda Password. d. Inserire una nuova password. e. Selezionare **Cambia password**.	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda Password. c. Inserire una nuova password. d. Selezionare **Cambia password**.

Attività	Menu delle azioni	Pagina dei dettagli
Modifica dei gruppi (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**. c. Selezionare la scheda gruppi. d. Se si desidera, selezionare il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. e. Selezionare **Edit groups** (Modifica gruppi) per selezionare diversi gruppi. f. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda gruppi. c. Se si desidera, selezionare il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. d. Selezionare **Edit groups** (Modifica gruppi) per selezionare diversi gruppi. e. Selezionare **Save Changes** (Salva modifiche).

Duplicare un utente

È possibile duplicare un utente esistente per creare un nuovo utente con le stesse autorizzazioni.

Fasi

1. Selezionare la casella di controllo dell'utente.
2. Selezionare **azioni** > **utente duplicato**.
3. Completare la procedura guidata Duplica utente.

Eliminare un utente

È possibile eliminare un utente locale per rimuoverlo definitivamente dal sistema.

Impossibile eliminare l'utente root.

Fasi

1. Nella pagina utenti, selezionare la casella di controllo per ciascun utente che si desidera rimuovere.
2. Selezionare **azioni** > **Elimina utente**.
3. Selezionare **Delete user** (Elimina utente).

Utilizzo di SSO (Single Sign-on)

Configurare il single sign-on

Quando è attivato il Single Sign-on (SSO), gli utenti possono accedere a Grid Manager, Tenant Manager, Grid Management API o tenant Management API solo se le loro credenziali sono autorizzate utilizzando il processo di accesso SSO implementato dall'organizzazione. Gli utenti locali non possono accedere a StorageGRID.

Come funziona il single sign-on

Il sistema StorageGRID supporta SSO (Single Sign-on) utilizzando lo standard SAML 2.0 (Security Assertion Markup Language 2.0).

Prima di attivare SSO (Single Sign-on), esaminare in che modo i processi di accesso e disconnessione di StorageGRID vengono influenzati quando SSO è attivato.

Effettuare l'accesso quando SSO è attivato

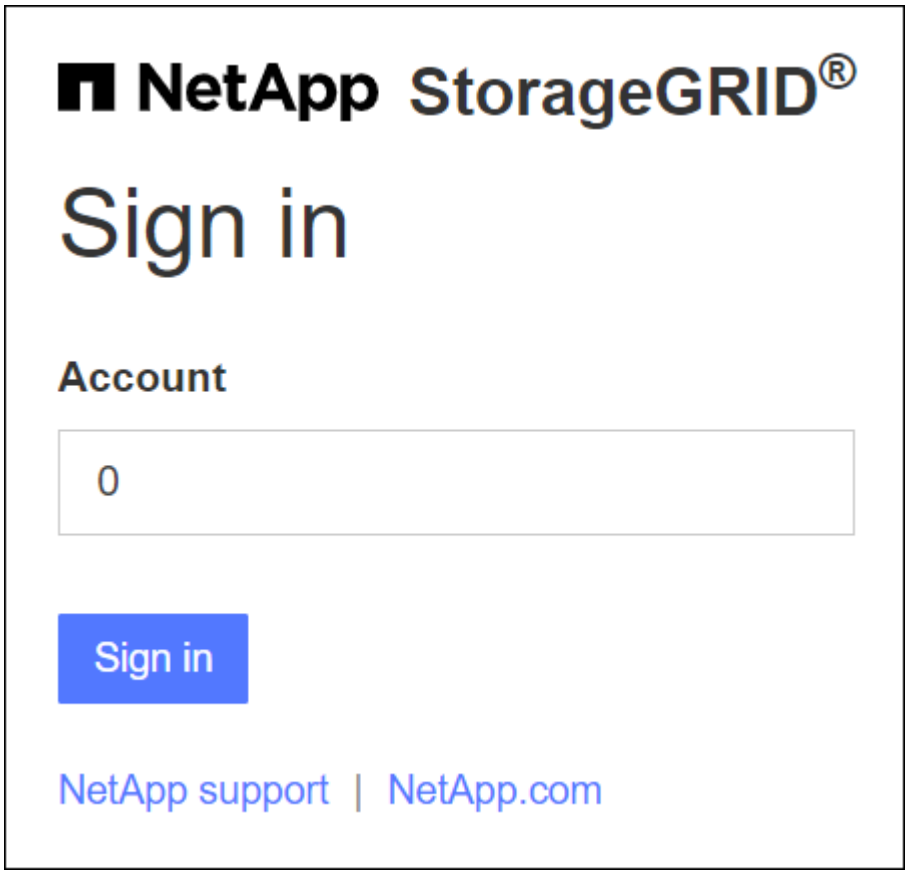
Quando SSO è attivato e si accede a StorageGRID, si viene reindirizzati alla pagina SSO dell'organizzazione per convalidare le credenziali.

Fasi

1. Immettere il nome di dominio completo o l'indirizzo IP di qualsiasi nodo di amministrazione StorageGRID in un browser Web.

   Viene visualizzata la pagina di accesso a StorageGRID.

   - Se si accede per la prima volta all'URL del browser, viene richiesto di inserire un ID account:

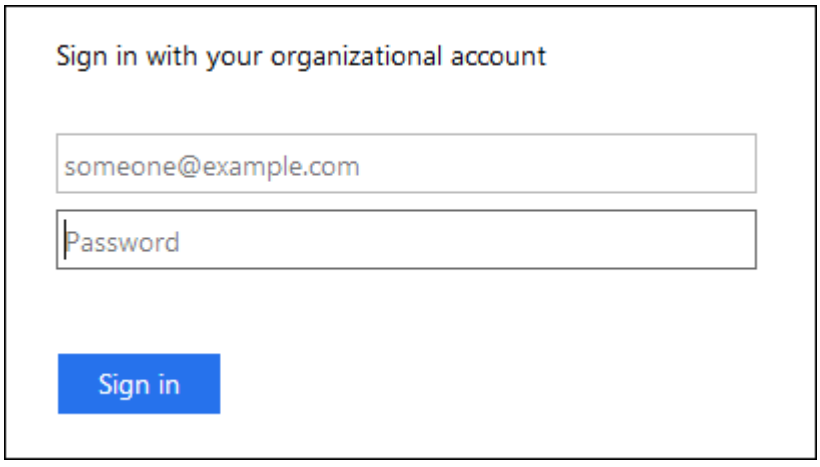


   - Se in precedenza hai effettuato l'accesso a Grid Manager o al Tenant Manager, ti verrà richiesto di selezionare un account recente o di inserire un ID account:

La pagina di accesso a StorageGRID non viene visualizzata quando si inserisce l'URL completo di un account tenant (ovvero un nome di dominio completo o un indirizzo IP seguito da) `/?accountId=20-digit-account-id`). Al contrario, si viene immediatamente reindirizzati alla pagina di accesso SSO dell'organizzazione, dove è possibile Accedi con le tue credenziali SSO.

2. Indicare se si desidera accedere a Grid Manager o al tenant Manager:
   - Per accedere a Grid Manager, lasciare vuoto il campo **ID account**, inserire **0** come ID account o selezionare **Grid Manager** se compare nell'elenco degli account recenti.
   - Per accedere al tenant Manager, inserire l'ID account tenant di 20 cifre o selezionare un tenant in base al nome, se visualizzato nell'elenco degli account recenti.
3. Selezionare **Accedi**

   StorageGRID reindirizza l'utente alla pagina di accesso SSO della propria organizzazione. Ad esempio:



4. Accedi con le tue credenziali SSO.

Se le credenziali SSO sono corrette:

a. Il provider di identità (IdP) fornisce una risposta di autenticazione a StorageGRID.
b. StorageGRID convalida la risposta di autenticazione.
c. Se la risposta è valida e l'utente appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID, l'utente ha effettuato l'accesso a Gestione griglia o a Gestione tenant, a seconda dell'account selezionato.

> Se l'account del servizio non è accessibile, è comunque possibile effettuare l'accesso, purché si sia un utente esistente che appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID.

5. Se si dispone di autorizzazioni adeguate, è possibile accedere ad altri nodi di amministrazione o a Grid Manager o Tenant Manager.

   Non è necessario immettere nuovamente le credenziali SSO.

Disconnettersi quando SSO è attivato

Quando SSO è abilitato per StorageGRID, ciò che accade quando si effettua la disconnessione dipende da ciò che si effettua l'accesso e da dove si effettua la disconnessione.

Fasi

1. Individuare il collegamento **Disconnetti** nell'angolo in alto a destra dell'interfaccia utente.
2. Selezionare **Disconnetti**.

   Viene visualizzata la pagina di accesso a StorageGRID. Il menu a discesa **Recent Accounts** (account recenti) viene aggiornato per includere **Grid Manager** o il nome del tenant, in modo da poter accedere a queste interfacce utente più rapidamente in futuro.

Se hai effettuato l'accesso a…	E ti disconnetterai da…	Sei disconnesso da…
Grid Manager su uno o più nodi di amministrazione	Grid Manager su qualsiasi nodo di amministrazione	Grid Manager su tutti i nodi di amministrazione **Nota:** se si utilizza Azure per SSO, la disconnessione da tutti i nodi Admin potrebbe richiedere alcuni minuti.
Tenant Manager su uno o più nodi di amministrazione	Tenant Manager su qualsiasi nodo di amministrazione	Tenant Manager su tutti i nodi di amministrazione
Sia Grid Manager che tenant Manager	Grid Manager	Solo Grid Manager. Per disconnettersi da SSO, devi anche disconnetterti da Tenant Manager.

La tabella riassume ciò che accade quando si effettua la disconnessione se si utilizza una singola sessione del browser. Se hai effettuato l'accesso a StorageGRID in più sessioni del browser, devi disconnetterti separatamente da tutte le sessioni del browser.

Requisiti e considerazioni per il single sign-on

Prima di abilitare il single sign-on (SSO) per un sistema StorageGRID, esaminare i requisiti e le considerazioni.

Requisiti del provider di identità

StorageGRID supporta i seguenti provider di identità SSO (IdP):

- Active Directory Federation Service (ad FS)
- Azure Active Directory (Azure ad)
- PingFederate

È necessario configurare la federazione delle identità per il sistema StorageGRID prima di poter configurare un provider di identità SSO. Il tipo di servizio LDAP utilizzato per i controlli di federazione delle identità che consentono di implementare il tipo di SSO.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Requisiti AD FS

È possibile utilizzare una delle seguenti versioni di ad FS:

- Windows Server 2022 ad FS
- Windows Server 2019 ad FS
- Windows Server 2016 ad FS

Windows Server 2016 dovrebbe utilizzare "Aggiornamento KB3201845", o superiore.

Requisiti aggiuntivi

- Transport Layer Security (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versione 3.5.1 o successiva

Considerazioni per Azure

Se si utilizza Azure come tipo SSO e gli utenti dispongono di nomi principali che non utilizzano il nome sAMAccountName come prefisso, possono verificarsi problemi di accesso se StorageGRID perde la

connessione con il server LDAP. Per consentire agli utenti di accedere, è necessario ripristinare la connessione al server LDAP.

Requisiti dei certificati del server

Per impostazione predefinita, StorageGRID utilizza un certificato di interfaccia di gestione su ciascun nodo di amministrazione per garantire l'accesso al gestore di griglia, al gestore del tenant, all'API di gestione del grid e all'API di gestione del tenant. Quando si configurano i trust delle parti di base (ad FS), le applicazioni aziendali (Azure) o le connessioni del provider di servizi (PingFederate) per StorageGRID, il certificato del server viene utilizzato come certificato di firma per le richieste StorageGRID.

Se non lo hai già fatto "ha configurato un certificato personalizzato per l'interfaccia di gestione", dovresti farlo ora. Quando si installa un certificato server personalizzato, viene utilizzato per tutti i nodi di amministrazione e può essere utilizzato in tutti i trust, le applicazioni aziendali o le connessioni SP di StorageGRID.

> Si sconsiglia di utilizzare il certificato server predefinito di un nodo di amministrazione in una connessione SP, un'applicazione aziendale o un trust di parte attiva. Se il nodo si guasta e viene ripristinato, viene generato un nuovo certificato server predefinito. Prima di poter accedere al nodo recuperato, è necessario aggiornare il trust della parte che si basa, l'applicazione aziendale o la connessione SP con il nuovo certificato.

È possibile accedere al certificato del server di un nodo amministratore accedendo alla shell dei comandi del nodo e accedendo a. `/var/local/mgmt-api` directory. Viene assegnato un nome a un certificato server personalizzato `custom-server.crt`. Il certificato server predefinito del nodo viene denominato `server.crt`.

Requisiti delle porte

Single Sign-on (SSO) non è disponibile sulle porte limitate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443). Vedere "Controllare l'accesso al firewall esterno".

Confermare che gli utenti federati possono accedere

Prima di attivare il Single Sign-on (SSO), è necessario confermare che almeno un utente federato possa accedere a Grid Manager e a Tenant Manager per qualsiasi account tenant esistente.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- La federazione delle identità è già stata configurata.

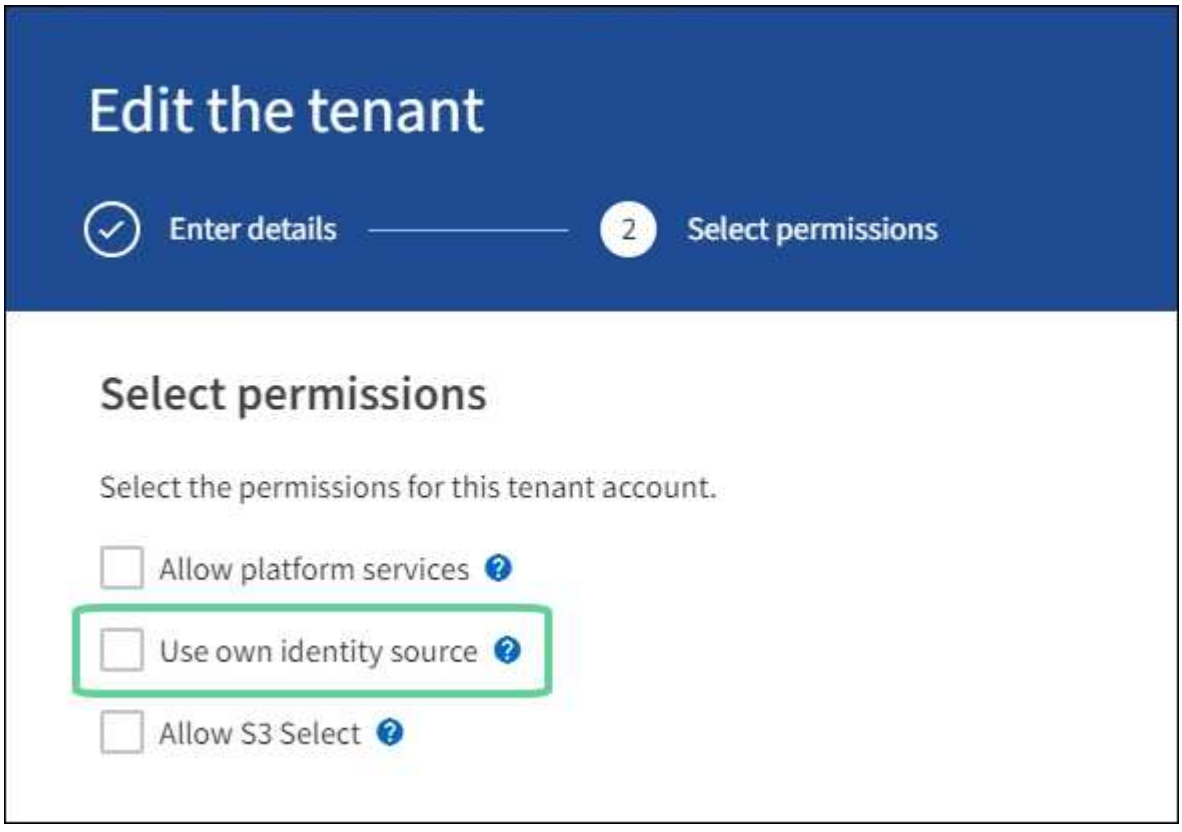
Fasi

1. Se esistono account tenant, verificare che nessuno dei tenant utilizzi la propria origine di identità.

> Quando si attiva SSO, un'origine identità configurata in Tenant Manager viene ignorata dall'origine identità configurata in Grid Manager. Gli utenti che appartengono all'origine dell'identità del tenant non potranno più accedere a meno che non dispongano di un account con l'origine dell'identità di Grid Manager.

a. Accedi al tenant manager per ogni account tenant.
b. Selezionare **ACCESS MANAGEMENT** > **Identity Federation**.
c. Verificare che la casella di controllo **Enable Identity Federation** (Abilita federazione identità) non sia selezionata.
d. In tal caso, verificare che i gruppi federati che potrebbero essere in uso per questo account tenant non siano più necessari, deselezionare la casella di controllo e selezionare **Salva**.

2. Verificare che un utente federated possa accedere a Grid Manager:
   a. Da Grid Manager, selezionare **CONFIGURATION** > **Access control** > **Admin groups**.
   b. Assicurarsi che almeno un gruppo federated sia stato importato dall'origine dell'identità di Active Directory e che sia stata assegnata l'autorizzazione di accesso root.
   c. Disconnettersi.
   d. Confermare che è possibile accedere nuovamente a Grid Manager come utente nel gruppo federated.
3. Se sono presenti account tenant, verificare che un utente federated che dispone dell'autorizzazione di accesso root possa effettuare l'accesso:
   a. In Grid Manager, selezionare **TENANT**.
   b. Selezionare l'account tenant e selezionare **azioni** > **Modifica**.
   c. Nella scheda Immetti dettagli, selezionare **continua**.
   d. Se la casella di controllo **Usa origine identità propria** è selezionata, deselezionare la casella e selezionare **Salva**.



Viene visualizzata la pagina del tenant.

   a. Selezionare l'account tenant, selezionare **Accedi** e accedere all'account tenant come utente root

locale.

b. Da Tenant Manager, selezionare **ACCESS MANAGEMENT** > **Groups**.

c. Assicurarsi che almeno un gruppo federated di Grid Manager sia stato assegnato all'autorizzazione di accesso root per questo tenant.

d. Disconnettersi.

e. Confermare che è possibile accedere nuovamente al tenant come utente nel gruppo federated.

Informazioni correlate

- "Requisiti e considerazioni per il single sign-on"
- "Gestire i gruppi di amministratori"
- "Utilizzare un account tenant"

USA la modalità sandbox

È possibile utilizzare la modalità sandbox per configurare e testare SSO (Single Sign-on) prima di attivarla per tutti gli utenti StorageGRID. Una volta attivato SSO, è possibile tornare alla modalità sandbox ogni volta che è necessario modificare o ripetere il test della configurazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Hai configurato la federazione delle identità per il tuo sistema StorageGRID.
- Per la federazione di identità **tipo di servizio LDAP**, è stato selezionato Active Directory o Azure, in base al provider di identità SSO che si intende utilizzare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

A proposito di questa attività

Quando SSO è attivato e un utente tenta di accedere a un nodo amministratore, StorageGRID invia una richiesta di autenticazione al provider di identità SSO. A sua volta, il provider di identità SSO invia una risposta di autenticazione a StorageGRID, indicando se la richiesta di autenticazione ha avuto esito positivo. Per le richieste riuscite:

- La risposta di Active Directory o PingFederate include un UUID (Universally Unique Identifier) per l'utente.
- La risposta di Azure include un User Principal Name (UPN).

Per consentire a StorageGRID (il provider di servizi) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione dell'utente, è necessario configurare alcune impostazioni in StorageGRID. Quindi, è necessario utilizzare il software del provider di identità SSO per creare un trust di parte (ad FS),

un'applicazione aziendale (Azure) o un provider di servizi (PingFederate) per ciascun nodo di amministrazione. Infine, è necessario tornare a StorageGRID per attivare SSO.

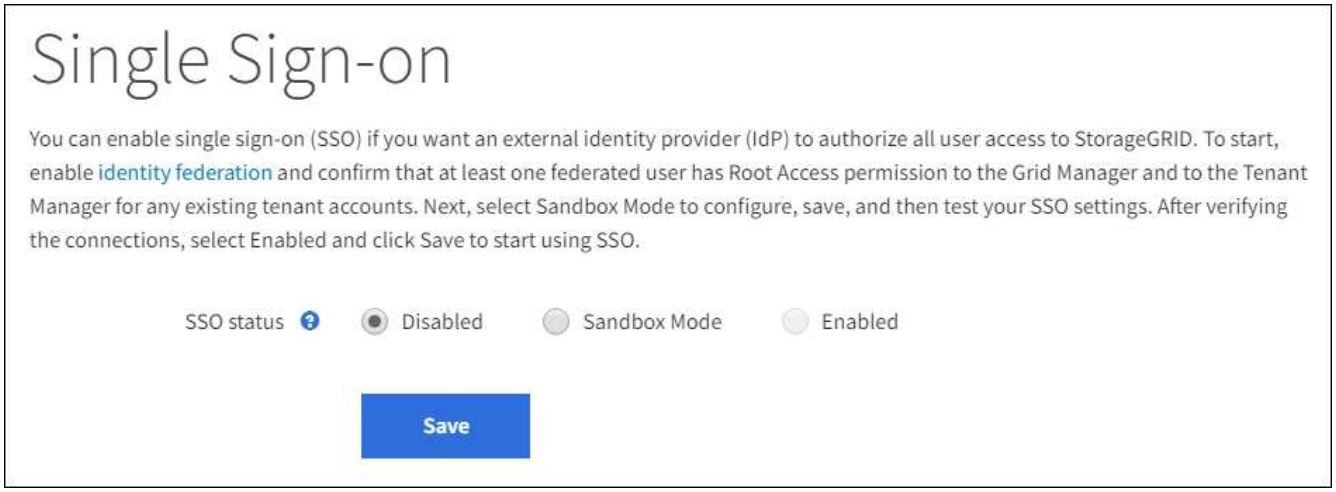
La modalità sandbox semplifica l'esecuzione di questa configurazione e il test di tutte le impostazioni prima di attivare SSO. Quando si utilizza la modalità sandbox, gli utenti non possono accedere utilizzando SSO.

Accedere alla modalità sandbox

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.

   Viene visualizzata la pagina Single Sign-on (accesso singolo), con l'opzione **Disabled** (Disattivato) selezionata.



   Se le opzioni di stato SSO non vengono visualizzate, verificare di aver configurato il provider di identità come origine dell'identità federata. Vedere "Requisiti e considerazioni per il single sign-on".

2. Selezionare **Sandbox Mode**.

   Viene visualizzata la sezione Identity Provider (Provider di identità).

Inserire i dettagli del provider di identità

Fasi

1. Selezionare **tipo SSO** dall'elenco a discesa.
2. Compilare i campi nella sezione Identity Provider (Provider di identità) in base al tipo di SSO selezionato.

Active Directory

1. Inserire il nome del servizio Federazione* del provider di identità, esattamente come appare in Active Directory Federation Service (ad FS).

   Per individuare il nome del servizio federativo, accedere a Gestione server Windows. Selezionare **Tools** > **ad FS Management**. Dal menu Action (azione), selezionare **Edit Federation Service Properties** (Modifica proprietà servizio federazione). Il nome del servizio della federazione viene visualizzato nel secondo campo.

2. Specificare il certificato TLS da utilizzare per proteggere la connessione quando il provider di identità invia le informazioni di configurazione SSO in risposta alle richieste StorageGRID.
   - **Usa certificato CA del sistema operativo**: Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
   - **Usa certificato CA personalizzato**: Utilizza un certificato CA personalizzato per proteggere la connessione.

     Se si seleziona questa impostazione, copiare il testo del certificato personalizzato e incollarlo nella casella di testo **certificato CA**.

   - **Non utilizzare TLS**: Non utilizzare un certificato TLS per proteggere la connessione.

     Se si modifica immediatamente il certificato CA "Riavviare il servizio Mgmt-api sui nodi Admin" E testare un SSO di successo in Grid Manager.

3. Nella sezione parte che si basa, specificare il **identificativo della parte che si basa** per StorageGRID. Questo valore controlla il nome utilizzato per ciascun trust di parte che si basa in ad FS.
   - Ad esempio, se la griglia dispone di un solo nodo di amministrazione e non si prevede di aggiungere altri nodi di amministrazione in futuro, immettere `SG` oppure `StorageGRID`.
   - Se la griglia include più di un nodo di amministrazione, includere la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. In questo modo viene generata una tabella che mostra l'identificativo del componente di base per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.

   È necessario creare un trust per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

4. Selezionare **Salva**.

   Sul pulsante **Save** viene visualizzato un segno di spunta verde per alcuni secondi.

Azure

1. Specificare il certificato TLS da utilizzare per proteggere la connessione quando il provider di identità

invia le informazioni di configurazione SSO in risposta alle richieste StorageGRID.

- **Usa certificato CA del sistema operativo**: Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Usa certificato CA personalizzato**: Utilizza un certificato CA personalizzato per proteggere la connessione.

  Se si seleziona questa impostazione, copiare il testo del certificato personalizzato e incollarlo nella casella di testo **certificato CA**.

- **Non utilizzare TLS**: Non utilizzare un certificato TLS per proteggere la connessione.

> Se si modifica immediatamente il certificato CA "Riavviare il servizio Mgmt-api sui nodi Admin" E testare un SSO di successo in Grid Manager.

2. Nella sezione applicazione aziendale, specificare **Nome applicazione aziendale** per StorageGRID. Questo valore controlla il nome utilizzato per ogni applicazione aziendale in Azure ad.

   - Ad esempio, se la griglia dispone di un solo nodo di amministrazione e non si prevede di aggiungere altri nodi di amministrazione in futuro, immettere `SG` oppure `StorageGRID`.
   - Se la griglia include più di un nodo di amministrazione, includere la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. In questo modo viene generata una tabella che mostra il nome di un'applicazione aziendale per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.

> È necessario creare un'applicazione aziendale per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un'applicazione aziendale per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

3. Seguire la procedura descritta in "Creare applicazioni aziendali in Azure ad" Per creare un'applicazione aziendale per ciascun nodo amministratore elencato nella tabella.
4. Da Azure ad, copiare l'URL dei metadati della federazione per ciascuna applicazione aziendale. Quindi, incolla questo URL nel corrispondente campo **URL metadati federazione** in StorageGRID.
5. Dopo aver copiato e incollato un URL dei metadati della federazione per tutti i nodi di amministrazione, selezionare **Salva**.

   Sul pulsante **Save** viene visualizzato un segno di spunta verde per alcuni secondi.

PingFederate

1. Specificare il certificato TLS da utilizzare per proteggere la connessione quando il provider di identità invia le informazioni di configurazione SSO in risposta alle richieste StorageGRID.
   - **Usa certificato CA del sistema operativo**: Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
   - **Usa certificato CA personalizzato**: Utilizza un certificato CA personalizzato per proteggere la connessione.

Se si seleziona questa impostazione, copiare il testo del certificato personalizzato e incollarlo nella casella di testo **certificato CA**.

- **Non utilizzare TLS**: Non utilizzare un certificato TLS per proteggere la connessione.

> Se si modifica immediatamente il certificato CA "Riavviare il servizio Mgmt-api sui nodi Admin" E testare un SSO di successo in Grid Manager.

2. Nella sezione Provider di servizi (SP), specificare **ID connessione SP** per StorageGRID. Questo valore controlla il nome utilizzato per ogni connessione SP in PingFederate.
   - Ad esempio, se la griglia dispone di un solo nodo di amministrazione e non si prevede di aggiungere altri nodi di amministrazione in futuro, immettere `SG` oppure `StorageGRID`.
   - Se la griglia include più di un nodo di amministrazione, includere la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. In questo modo viene generata una tabella che mostra l'ID di connessione SP per ciascun nodo amministratore del sistema, in base al nome host del nodo.

> È necessario creare una connessione SP per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di una connessione SP per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

3. Specificare l'URL dei metadati della federazione per ciascun nodo amministratore nel campo **URL metadati federazione**.

   Utilizzare il seguente formato:

```
https://<Federation Service Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection ID>
```

4. Selezionare **Salva**.

   Sul pulsante **Save** viene visualizzato un segno di spunta verde per alcuni secondi.

Configurare i trust, le applicazioni aziendali o le connessioni SP della parte che si basa

Una volta salvata la configurazione, viene visualizzato l'avviso di conferma della modalità Sandbox. Questo avviso conferma che la modalità sandbox è ora attivata e fornisce istruzioni generali.

StorageGRID può rimanere in modalità sandbox per tutto il tempo necessario. Tuttavia, quando si seleziona **modalità sandbox** nella pagina Single Sign-on (accesso singolo), SSO viene disattivato per tutti gli utenti StorageGRID. Solo gli utenti locali possono effettuare l'accesso.

Attenersi alla procedura descritta di seguito per configurare i trust (Active Directory), le applicazioni aziendali

complete (Azure) o le connessioni SP (PingFederate).

Active Directory

Fasi

1. Accedere a Active Directory Federation Services (ad FS).
2. Creare uno o più trust di parti di supporto per StorageGRID, utilizzando ciascun identificatore di parte di supporto mostrato nella tabella della pagina di accesso singolo di StorageGRID.

   È necessario creare un trust per ciascun nodo di amministrazione mostrato nella tabella.

   Per istruzioni, visitare il sito Web all'indirizzo "Creazione di trust di parti di base in ad FS".

Azure

Fasi

1. Dalla pagina Single Sign-on (accesso singolo) per il nodo di amministrazione a cui si è attualmente connessi, selezionare il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi di amministrazione della griglia, ripetere questi passaggi:
   a. Accedere al nodo.
   b. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
   c. Scaricare e salvare i metadati SAML per quel nodo.
3. Accedere al portale Azure.
4. Seguire la procedura descritta in "Creare applicazioni aziendali in Azure ad" Per caricare il file di metadati SAML per ciascun nodo di amministrazione nella relativa applicazione aziendale Azure corrispondente.

PingFederate

Fasi

1. Dalla pagina Single Sign-on (accesso singolo) per il nodo di amministrazione a cui si è attualmente connessi, selezionare il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi di amministrazione della griglia, ripetere questi passaggi:
   a. Accedere al nodo.
   b. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
   c. Scaricare e salvare i metadati SAML per quel nodo.
3. Accedere a PingFederate.
4. "Creare una o più connessioni del provider di servizi (SP) per StorageGRID". Utilizzare l'ID connessione SP per ciascun nodo amministratore (mostrato nella tabella della pagina accesso singolo StorageGRID) e i metadati SAML scaricati per tale nodo amministratore.

   È necessario creare una connessione SP per ciascun nodo di amministrazione mostrato nella tabella.

Verificare le connessioni SSO

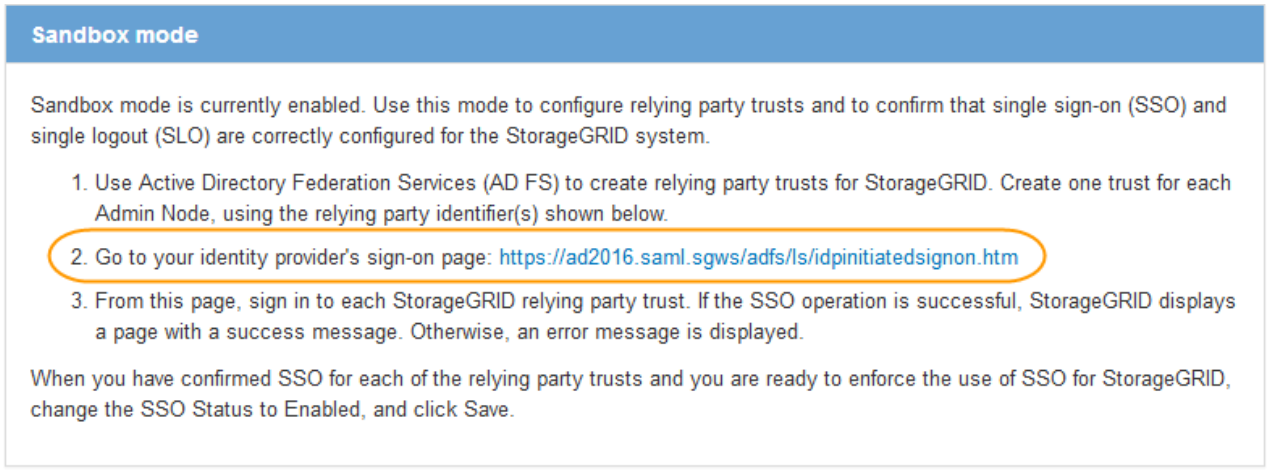
Prima di imporre l'utilizzo del single sign-on per l'intero sistema StorageGRID, è necessario confermare che il single sign-on e il singolo logout sono configurati correttamente per ciascun nodo di amministrazione.

Active Directory

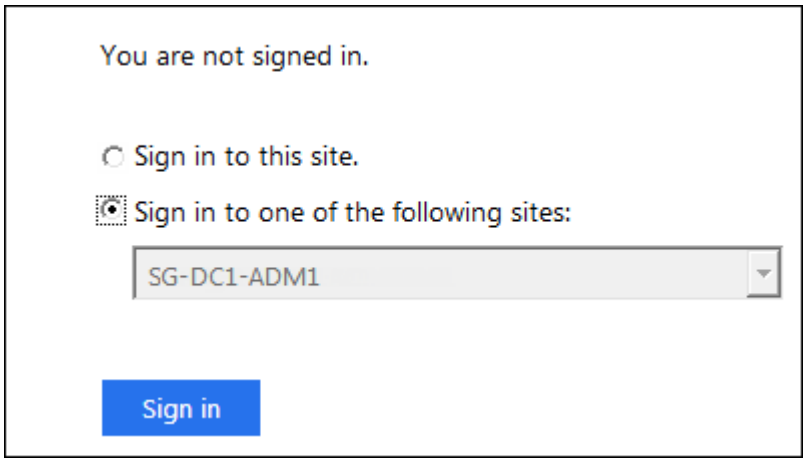
Fasi

1. Dalla pagina Single Sign-on di StorageGRID, individuare il collegamento nel messaggio in modalità sandbox.

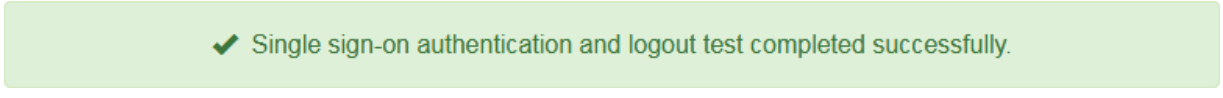
   L'URL deriva dal valore immesso nel campo **Federation service name**.



2. Selezionare il collegamento oppure copiare e incollare l'URL in un browser per accedere alla pagina di accesso del provider di identità.
3. Per confermare che è possibile utilizzare SSO per accedere a StorageGRID, selezionare **Accedi a uno dei seguenti siti**, selezionare l'identificativo della parte di base per il nodo di amministrazione principale e selezionare **Accedi**.



4. Immettere il nome utente e la password federated.
   - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.



   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
5. Ripetere questa procedura per verificare la connessione SSO per ciascun nodo di amministrazione

nella griglia.

Azure

Fasi

1. Vai alla pagina Single Sign-on nel portale Azure.
2. Selezionare **Test dell'applicazione**.
3. Immettere le credenziali di un utente federated.
   - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.

     ✔ Single sign-on authentication and logout test completed successfully.

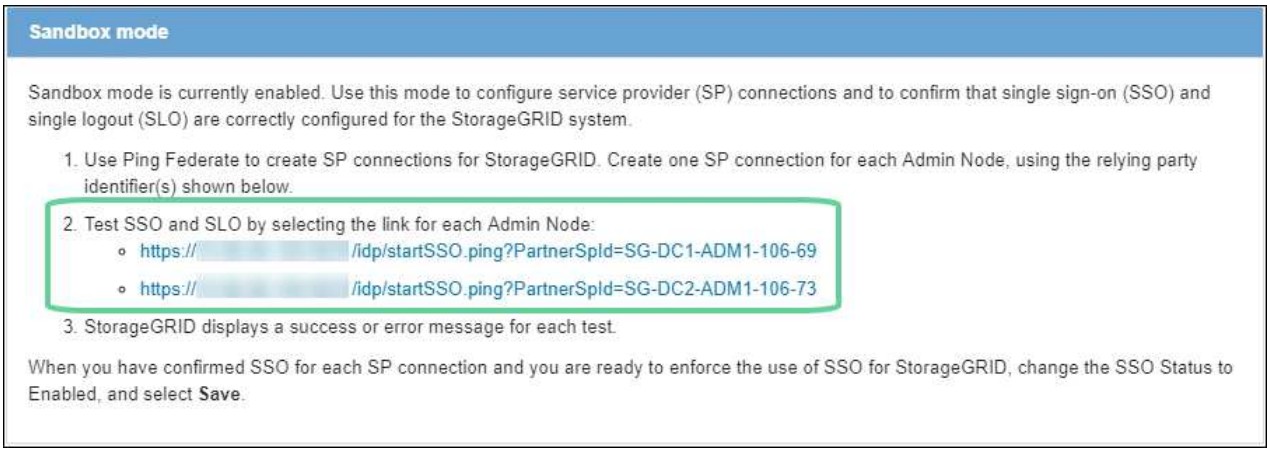
   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
4. Ripetere questa procedura per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

PingFederate

Fasi

1. Dalla pagina accesso singolo StorageGRID, selezionare il primo collegamento nel messaggio in modalità sandbox.

   Selezionare e verificare un collegamento alla volta.



2. Immettere le credenziali di un utente federated.
   - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
3. Selezionare il collegamento successivo per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

Se viene visualizzato un messaggio Page Expired (pagina scaduta), selezionare il pulsante **Back** (Indietro) nel browser e inviare nuovamente le credenziali.

Attiva single sign-on

Una volta confermata la possibilità di utilizzare SSO per accedere a ciascun nodo amministrativo, è possibile attivare SSO per l'intero sistema StorageGRID.

Quando SSO è attivato, tutti gli utenti devono utilizzare SSO per accedere a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Gli utenti locali non possono più accedere a StorageGRID.

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
2. Impostare lo stato SSO su **Enabled**.
3. Selezionare **Salva**.
4. Esaminare il messaggio di avviso e selezionare **OK**.

   Il Single Sign-on è ora attivato.

Se si utilizza il portale Azure e si accede a StorageGRID dallo stesso computer utilizzato per accedere ad Azure, assicurarsi che l'utente sia anche un utente StorageGRID autorizzato (un utente di un gruppo federato importato in StorageGRID) Oppure disconnettersi dal portale Azure prima di tentare di accedere a StorageGRID.

Creazione di trust di parti di base in ad FS

È necessario utilizzare Active Directory Federation Services (ad FS) per creare un trust di parte per ciascun nodo di amministrazione nel sistema. È possibile creare trust di parti che utilizzano i comandi PowerShell, importando metadati SAML da StorageGRID o immettendo i dati manualmente.

Prima di iniziare

- È stato configurato Single Sign-on per StorageGRID ed è stato selezionato **ad FS** come tipo di SSO.
- **La modalità Sandbox** è selezionata nella pagina Single Sign-on di Grid Manager. Vedere "USA la modalità sandbox".
- Si conoscono il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte di base per ciascun nodo di amministrazione nel sistema. Questi valori sono disponibili nella tabella dei dettagli dei nodi di amministrazione nella pagina accesso singolo StorageGRID.

  È necessario creare un trust per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Si dispone di esperienza nella creazione di trust di parti di supporto in ad FS o si dispone dell'accesso alla documentazione di Microsoft ad FS.
- Si sta utilizzando lo snap-in di gestione di ad FS e si appartiene al gruppo Administrators.

- Se si crea manualmente l'attendibilità del componente di base, si dispone del certificato personalizzato caricato per l'interfaccia di gestione di StorageGRID oppure si sa come accedere a un nodo di amministrazione dalla shell dei comandi.

A proposito di questa attività

Queste istruzioni si applicano a Windows Server 2016 ad FS. Se si utilizza una versione diversa di ad FS, si noteranno lievi differenze nella procedura. In caso di domande, consultare la documentazione di Microsoft ad FS.

Creare un trust di parte con Windows PowerShell

È possibile utilizzare Windows PowerShell per creare rapidamente uno o più trust di parti.

Fasi

1. Dal menu Start di Windows, selezionare con il pulsante destro del mouse l'icona PowerShell e selezionare **Esegui come amministratore**.
2. Al prompt dei comandi di PowerShell, immettere il seguente comando:

   `Add-AdfsRelyingPartyTrust -Name "Admin_Node_identifer" -MetadataURL "https://Admin_Node_FQDN/api/saml-metadata"

   - Per *`Admin_Node_Identifier`*, Immettere l'identificativo della parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, `SG-DC1-ADM1`.
   - Per *`Admin_Node_FQDN`*, Immettere il nome di dominio completo per lo stesso nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).
3. Da Gestione server Windows, selezionare **Strumenti** > **Gestione di ad FS**.

   Viene visualizzato lo strumento di gestione di ad FS.

4. Selezionare **ad FS** > **Trust di parte**.

   Viene visualizzato l'elenco dei trust della parte che si basa.

5. Aggiungere un criterio di controllo degli accessi al trust della parte di base appena creato:
   a. Individuare la fiducia della parte di base appena creata.
   b. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit Access Control Policy** (Modifica policy di controllo degli accessi).
   c. Selezionare un criterio di controllo degli accessi.
   d. Selezionare **Applica** e **OK**
6. Aggiungere una policy di emissione delle richieste di rimborso al nuovo Trust della parte di base creato:
   a. Individuare la fiducia della parte di base appena creata.
   b. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
   c. Selezionare **Aggiungi regola**.
   d. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).

e. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

   Ad esempio, **objectGUID a ID nome** o **UPN a ID nome**.

f. Per l'archivio attributi, selezionare **Active Directory**.

g. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.

h. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.

i. Selezionare **fine**, quindi **OK**.

7. Verificare che i metadati siano stati importati correttamente.

   a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.

   b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.

      Se i metadati non sono presenti, verificare che l'indirizzo dei metadati della federazione sia corretto oppure inserire i valori manualmente.

8. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.

9. Una volta completata l'operazione, tornare a StorageGRID e verificare tutti i trust delle parti di base per verificare che siano configurati correttamente. Vedere "Utilizzare la modalità Sandbox" per istruzioni.

Creare un trust per la parte che si basa importando i metadati della federazione

È possibile importare i valori per ciascun trust di parte che si basa accedendo ai metadati SAML per ciascun nodo di amministrazione.

Fasi

1. In Gestione server Windows, selezionare **Strumenti**, quindi selezionare **Gestione di ad FS**.
2. In azioni, selezionare **Aggiungi fiducia parte di base**.
3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e selezionare **Avvia**.
4. Selezionare **Importa dati relativi alla parte che si basa pubblicati online o su una rete locale**.
5. In **Federation metadata address (nome host o URL)**, digitare la posizione dei metadati SAML per questo nodo di amministrazione:

   `https://Admin_Node_FQDN/api/saml-metadata`

   Per *`Admin_Node_FQDN`*, Immettere il nome di dominio completo per lo stesso nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

6. Completare la procedura guidata Trust Party, salvare il trust della parte che si basa e chiudere la procedura guidata.

   Quando si immette il nome visualizzato, utilizzare l'identificativo parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, `SG-DC1-ADM1`.

7. Aggiungere una regola di richiesta di rimborso:
   a. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
   b. Selezionare **Aggiungi regola**:
   c. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).
   d. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

      Ad esempio, **objectGUID a ID nome** o **UPN a ID nome**.

   e. Per l'archivio attributi, selezionare **Active Directory**.
   f. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
   g. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
   h. Selezionare **fine**, quindi **OK**.
8. Verificare che i metadati siano stati importati correttamente.
   a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
   b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.

      Se i metadati non sono presenti, verificare che l'indirizzo dei metadati della federazione sia corretto oppure inserire i valori manualmente.

9. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
10. Una volta completata l'operazione, tornare a StorageGRID e verificare tutti i trust delle parti di base per verificare che siano configurati correttamente. Vedere "Utilizzare la modalità Sandbox" per istruzioni.

Creare manualmente un trust per la parte che si basa

Se si sceglie di non importare i dati per i trust della parte di base, è possibile inserire i valori manualmente.

Fasi

1. In Gestione server Windows, selezionare **Strumenti**, quindi selezionare **Gestione di ad FS**.
2. In azioni, selezionare **Aggiungi fiducia parte di base**.
3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e selezionare **Avvia**.
4. Selezionare **inserire manualmente i dati relativi alla parte di base** e selezionare **Avanti**.
5. Completare la procedura guidata Trust Party:
   a. Immettere un nome visualizzato per questo nodo di amministrazione.

      Per coerenza, utilizzare l'identificativo parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, `SG-DC1-ADM1`.

   b. Saltare il passaggio per configurare un certificato di crittografia token opzionale.
   c. Nella pagina Configure URL (Configura URL), selezionare la casella di controllo **Enable support for**

the SAML 2.0 WebSSO Protocol (attiva supporto per il protocollo SAML WebSSO).

d. Digitare l'URL dell'endpoint del servizio SAML per il nodo di amministrazione:

`https://Admin_Node_FQDN/api/saml-response`

Per *Admin_Node_FQDN*, Immettere il nome di dominio completo per il nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

e. Nella pagina Configure Identifier (Configura identificatori), specificare l'identificativo della parte di base per lo stesso nodo di amministrazione:

Admin_Node_Identifier

Per *Admin_Node_Identifier*, Immettere l'identificativo della parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, `SG-DC1-ADM1`.

f. Rivedere le impostazioni, salvare l'attendibilità della parte che si basa e chiudere la procedura guidata.

Viene visualizzata la finestra di dialogo Edit Claim Issuance Policy (Modifica policy di emissione richieste di

> Se la finestra di dialogo non viene visualizzata, fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).

6. Per avviare la procedura guidata Claim Rule, selezionare **Add Rule**:
   a. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).
   b. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

      Ad esempio, **objectGUID a ID nome** o **UPN a ID nome**.

   c. Per l'archivio attributi, selezionare **Active Directory**.
   d. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
   e. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
   f. Selezionare **fine**, quindi **OK**.
7. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
8. Nella scheda **Endpoint**, configurare l'endpoint per la disconnessione singola (SLO):
   a. Selezionare **Add SAML** (Aggiungi SAML).
   b. Selezionare **Endpoint Type** > **SAML Logout**.
   c. Selezionare **binding** > **Redirect**.
   d. Nel campo **Trusted URL**, immettere l'URL utilizzato per la disconnessione singola (SLO) da questo nodo di amministrazione:

      `https://Admin_Node_FQDN/api/saml-logout`

Per *Admin_Node_FQDN*, Immettere il nome di dominio completo del nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

a. Selezionare **OK**.

9. Nella scheda **Firma**, specificare il certificato di firma per il trust della parte che si basa:

   a. Aggiungere il certificato personalizzato:

      - Se si dispone del certificato di gestione personalizzato caricato su StorageGRID, selezionare il certificato.
      - Se non si dispone del certificato personalizzato, accedere al nodo di amministrazione, quindi passare a. `/var/local/mgmt-api` Della directory Admin Node e aggiungere `custom-server.crt` file di certificato.

        Nota: utilizzando il certificato predefinito del nodo di amministrazione (`server.crt`) non è consigliato. Se il nodo Admin non riesce, il certificato predefinito viene rigenerato quando si ripristina il nodo ed è necessario aggiornare il trust della parte che si basa.

   b. Selezionare **Applica** e **OK**.

      Le proprietà della parte di base vengono salvate e chiuse.

10. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
11. Una volta completata l'operazione, tornare a StorageGRID e verificare tutti i trust delle parti di base per verificare che siano configurati correttamente. Vedere "USA la modalità sandbox" per istruzioni.

Creare applicazioni aziendali in Azure ad

Azure ad consente di creare un'applicazione aziendale per ciascun nodo di amministrazione del sistema.

Prima di iniziare

- È stata avviata la configurazione del single sign-on per StorageGRID ed è stato selezionato **Azure** come tipo di SSO.
- **La modalità Sandbox** è selezionata nella pagina Single Sign-on di Grid Manager. Vedere "USA la modalità sandbox".
- Si dispone del nome dell'applicazione aziendale* per ciascun nodo di amministrazione nel sistema. È possibile copiare questi valori dalla tabella Dettagli nodo amministratore nella pagina accesso singolo StorageGRID.

> È necessario creare un'applicazione aziendale per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un'applicazione aziendale per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Hai esperienza nella creazione di applicazioni aziendali in Azure Active Directory.
- Hai un account Azure con un abbonamento attivo.
- Nell'account Azure hai uno dei seguenti ruoli: Amministratore globale, amministratore dell'applicazione cloud, amministratore dell'applicazione o proprietario del service principal.

Accedere ad Azure ad

Fasi

1. Accedere a. "Portale Azure".
2. Selezionare "Azure Active Directory".
3. Selezionare "Applicazioni aziendali".

Creare applicazioni aziendali e salvare la configurazione SSO di StorageGRID

Per salvare la configurazione SSO per Azure in StorageGRID, è necessario utilizzare Azure per creare un'applicazione aziendale per ciascun nodo di amministrazione. Copiare gli URL dei metadati della federazione da Azure e incollarli nei corrispondenti campi **URL metadati federazione** nella pagina di accesso singolo di StorageGRID.

Fasi

1. Ripetere i passaggi seguenti per ciascun nodo di amministrazione.
   a. Nel riquadro Azure Enterprise Applications (applicazioni aziendali Azure), selezionare **New application** (Nuova applicazione).
   b. Selezionare **Crea la tua applicazione**.
   c. Per il nome, inserire il nome dell'applicazione aziendale copiato dalla tabella dei dettagli del nodo amministrativo nella pagina accesso singolo StorageGRID.
   d. Lasciare selezionato il pulsante di opzione **integra qualsiasi altra applicazione che non trovi nella galleria (non-gallery)**.
   e. Selezionare **Crea**.
   f. Selezionare il collegamento **Get Started** nel campo **2. Impostare la casella Single Sign on** (accesso singolo) oppure selezionare il collegamento **Single Sign-on** (accesso singolo) nel margine sinistro.
   g. Selezionare la casella **SAML**.
   h. Copiare l'URL * dei metadati dell'App Federation, disponibile nella sezione **fase 3 certificato di firma SAML**.
   i. Accedere alla pagina Single Sign-on di StorageGRID e incollare l'URL nel campo **Federation metadata URL** che corrisponde al **nome dell'applicazione aziendale** utilizzato.
2. Dopo aver incollato un URL dei metadati della federazione per ciascun nodo amministratore e aver apportato tutte le altre modifiche necessarie alla configurazione SSO, selezionare **Salva** nella pagina accesso singolo StorageGRID.

Scarica i metadati SAML per ogni nodo di amministrazione

Una volta salvata la configurazione SSO, è possibile scaricare un file di metadati SAML per ciascun nodo amministratore nel sistema StorageGRID.

Fasi

1. Ripetere questi passaggi per ciascun nodo di amministrazione.
   a. Accedere a StorageGRID dal nodo di amministrazione.
   b. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
   c. Selezionare il pulsante per scaricare i metadati SAML per il nodo di amministrazione.
   d. Salvare il file che verrà caricato in Azure ad.

Carica i metadati SAML in ogni applicazione aziendale

Dopo aver scaricato un file di metadati SAML per ciascun nodo amministrativo StorageGRID, eseguire la seguente procedura in Azure ad:

Fasi

1. Tornare al portale Azure.
2. Ripetere questi passaggi per ogni applicazione aziendale:

   > Potrebbe essere necessario aggiornare la pagina Enterprise Applications (applicazioni aziendali) per visualizzare le applicazioni aggiunte in precedenza nell'elenco.

   a. Accedere alla pagina Proprietà dell'applicazione aziendale.
   b. Impostare **assegnazione richiesta** su **No** (a meno che non si desideri configurare separatamente le assegnazioni).
   c. Vai alla pagina Single Sign-on.
   d. Completare la configurazione SAML.
   e. Selezionare il pulsante **carica file di metadati** e selezionare il file di metadati SAML scaricato per il nodo di amministrazione corrispondente.
   f. Una volta caricato il file, selezionare **Salva**, quindi selezionare **X** per chiudere il riquadro. Viene visualizzata nuovamente la pagina Set up Single Sign-on with SAML (Configura Single Sign-on con SAML).
3. Seguire la procedura descritta in "USA la modalità sandbox" per testare ogni applicazione.

Creare connessioni SP (service provider) in PingFederate

Utilizzare PingFederate per creare una connessione SP (Service Provider) per ciascun nodo amministratore del sistema. Per accelerare il processo, importare i metadati SAML da StorageGRID.

Prima di iniziare

- È stato configurato Single Sign-on per StorageGRID ed è stato selezionato **Ping Federate** come tipo di SSO.
- **La modalità Sandbox** è selezionata nella pagina Single Sign-on di Grid Manager. Vedere "USA la modalità sandbox".
- Si dispone dell'ID di connessione **SP** per ciascun nodo amministratore del sistema. Questi valori sono disponibili nella tabella dei dettagli dei nodi di amministrazione nella pagina accesso singolo StorageGRID.
- Sono stati scaricati i **metadati SAML** per ciascun nodo di amministrazione nel sistema.
- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Hai il "Guida di riferimento per l'amministratore" Per PingFederate Server. La documentazione di PingFederate fornisce istruzioni dettagliate e spiegazioni dettagliate.
- Hai il "Autorizzazione amministratore" Per PingFederate Server.

A proposito di questa attività

Queste istruzioni riepilogano come configurare PingFederate Server versione 10.3 come provider SSO per StorageGRID. Se si utilizza un'altra versione di PingFederate, potrebbe essere necessario adattare queste

istruzioni. Per istruzioni dettagliate sulla release, consultare la documentazione di PingFederate Server.

Completare i prerequisiti in PingFederate

Prima di poter creare le connessioni SP da utilizzare per StorageGRID, è necessario completare le attività dei prerequisiti in PingFederate. Quando si configurano le connessioni SP, verranno utilizzate le informazioni di questi prerequisiti.

Creare un archivio di dati

Se non lo si è già fatto, creare un archivio dati per connettere PingFederate al server LDAP di ad FS. Utilizzare i valori utilizzati quando "configurazione della federazione delle identità" In StorageGRID.

- **Tipo**: Directory (LDAP)
- **LDAP Type**: Active Directory
- **Binary Attribute Name** (Nome attributo binario): Inserire **objectGUID** nella scheda LDAP Binary Attributes (attributi binari LDAP) esattamente come mostrato.

Crea validatore credenziale password

Se non l'hai ancora fatto, crea una convalida delle credenziali per la password.

- **Type**: LDAP Username Password Credential Validator
- **Data store**: Selezionare il data store creato.
- **Base di ricerca**: Immettere le informazioni da LDAP (ad esempio, DC=saml,DC=sgws).
- **Filtro di ricerca**: SAMAccountName={nomeutente}
- **Scopo**: Sottostruttura

Crea istanza dell'adattatore IdP

Se non lo si è già fatto, creare un'istanza dell'adattatore IdP.

Fasi

1. Accedere a **Authentication** > **Integration** > **IdP Adapter**.
2. Selezionare **Crea nuova istanza**.
3. Nella scheda tipo, selezionare **HTML Form IdP Adapter**.
4. Nella scheda IdP Adapter, selezionare **Aggiungi una nuova riga a "Credential Validators"**.
5. Selezionare validatore delle credenziali per la password creato.
6. Nella scheda attributi adattatore, selezionare l'attributo **nome utente** per **pseudonimo**.
7. Selezionare **Salva**.

Creare o importare un certificato di firma

Se non lo si è già fatto, creare o importare il certificato di firma.

Fasi

1. Accedere a **sicurezza** > **chiavi e certificati di firma e decrittografia**.
2. Creare o importare il certificato di firma.

Creare una connessione SP in PingFederate

Quando si crea una connessione SP in PingFederate, si importano i metadati SAML scaricati da StorageGRID per il nodo di amministrazione. Il file di metadati contiene molti dei valori specifici necessari.

È necessario creare una connessione SP per ciascun nodo amministratore nel sistema StorageGRID, in modo che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo. Seguire queste istruzioni per creare la prima connessione SP. Quindi, passare a. Creare ulteriori connessioni SP per creare eventuali connessioni aggiuntive necessarie.

Scegliere il tipo di connessione SP

Fasi

1. Accedere a **applicazioni** > **integrazione** > **connessioni SP**.
2. Selezionare **Crea connessione**.
3. Selezionare **non utilizzare un modello per questa connessione**.
4. Selezionare **browser SSO Profiles** (profili SSO browser) e **SAML 2.0** come protocollo.

Importare metadati SP

Fasi

1. Nella scheda Importa metadati, selezionare **file**.
2. Scegliere il file di metadati SAML scaricato dalla pagina di accesso singolo StorageGRID per il nodo di amministrazione.
3. Esaminare il riepilogo dei metadati e le informazioni fornite nella scheda General Info (informazioni generali).

   L'ID dell'entità del partner e il nome della connessione sono impostati sull'ID della connessione StorageGRID SP. (Ad esempio, 10.96.105.200-DC1-ADM1-105-200). L'URL di base è l'IP del nodo di amministrazione StorageGRID.

4. Selezionare **Avanti**.

Configurare IdP browser SSO

Fasi

1. Dalla scheda SSO del browser, selezionare **Configure browser SSO** (Configura SSO browser).
2. Nella scheda SAML profiles (profili SAML), selezionare le opzioni **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selezionare **Avanti**.
4. Nella scheda Assertion Lifetime (durata asserzione), non apportare modifiche.
5. Nella scheda Assertion Creation (creazione asserzione), selezionare **Configure Assertion Creation (Configura creazione asserzione)**.
   a. Nella scheda Identity Mapping (mappatura identità), selezionare **Standard**.
   b. Nella scheda Contratto attributo, utilizzare **SAML_SUBJECT** come Contratto attributo e il formato del nome non specificato importato.
6. Per estendere il contratto, selezionare **Elimina** per rimuovere `urn:oid`, che non viene utilizzato.

Istanza dell'adattatore di mappatura

Fasi

1. Nella scheda Authentication Source Mapping (mappatura origine autenticazione), selezionare **Map New Adapter Instance** (mappatura nuova istanza adattatore).
2. Nella scheda Adapter instance (istanza adattatore), selezionare istanza dell'adattatore creato.
3. Nella scheda Mapping Method (metodo di mappatura), selezionare **Recupera attributi aggiuntivi da un archivio dati**.
4. Nella scheda origine attributo e Ricerca utente, selezionare **Aggiungi origine attributo**.
5. Nella scheda Data Store (Archivio dati), fornire una descrizione e selezionare archivio di dati hai aggiunto.
6. Nella scheda LDAP Directory Search (Ricerca directory LDAP):
   - Inserire il **DN di base**, che deve corrispondere esattamente al valore immesso in StorageGRID per il server LDAP.
   - Per l'ambito di ricerca, selezionare **sottostruttura**.
   - Per la classe di oggetti Root, cercare e aggiungere uno dei seguenti attributi: **ObjectGUID** o **userPrincipalName**.
7. Nella scheda LDAP Binary Attribute Encoding Types (tipi di codifica attributi binari LDAP), selezionare **Base64** come attributo **objectGUID**.
8. Nella scheda filtro LDAP, immettere **sAMAccountName={nome utente}**.
9. Nella scheda adempimento contratto attributo, selezionare **LDAP (attributo)** dall'elenco a discesa origine e selezionare **objectGUID** o **userPrincipalName** dall'elenco a discesa valore.
10. Esaminare e salvare l'origine dell'attributo.
11. Nella scheda origine attributo failsaved, selezionare **Interrompi transazione SSO**.
12. Esaminare il riepilogo e selezionare **fine**.
13. Selezionare **fine**.

Configurare le impostazioni del protocollo

Fasi

1. Nella scheda **connessione SP** > **SSO browser** > **Impostazioni protocollo**, selezionare **Configura impostazioni protocollo**.
2. Nella scheda URL servizio clienti asserzione, accettare i valori predefiniti, che sono stati importati dai metadati SAML di StorageGRID (**POST** per il binding e. `/api/saml-response` Per URL endpoint).
3. Nella scheda URL servizio SLO, accettare i valori predefiniti, importati dai metadati SAML di StorageGRID (**REDIRECT** per l'associazione e. `/api/saml-logout` Per URL endpoint.
4. Nella scheda Allowable SAML Bindings (Binding SAML autorizzati), deselezionare **ARTEFATTO** e **SOAP**. Sono richiesti solo **POST** e **REDIRECT**.
5. Nella scheda Firma Policy, lasciare selezionate le caselle di controllo **Richiedi la firma delle richieste Authn** e **Firma sempre asserzione**.
6. Nella scheda Encryption Policy (Criteri di crittografia), selezionare **None** (Nessuno).
7. Esaminare il riepilogo e selezionare **Done** (fine) per salvare le impostazioni del protocollo.
8. Esaminare il riepilogo e selezionare **fine** per salvare le impostazioni SSO del browser.

Configurare le credenziali

Fasi

1. Dalla scheda connessione SP, selezionare **credenziali**.
2. Dalla scheda credenziali, selezionare **Configura credenziali**.
3. Selezionare firma del certificato creato o importato.
4. Selezionare **Avanti** per accedere a **Gestisci impostazioni di verifica della firma**.
   a. Nella scheda Trust Model (modello di attendibilità), selezionare **Unancored** (non ancorato).
   b. Nella scheda certificato di verifica della firma, esaminare le informazioni del certificato di firma importate dai metadati SAML di StorageGRID.
5. Esaminare le schermate di riepilogo e selezionare **Save** (Salva) per salvare la connessione SP.

Creare ulteriori connessioni SP

È possibile copiare la prima connessione SP per creare le connessioni SP necessarie per ciascun nodo di amministrazione nella griglia. Vengono caricati nuovi metadati per ogni copia.

> Le connessioni SP per diversi nodi di amministrazione utilizzano impostazioni identiche, ad eccezione di ID entità del partner, URL di base, ID connessione, nome connessione, verifica firma, E SLO Response URL.

Fasi

1. Selezionare **Action** > **Copy** per creare una copia della connessione SP iniziale per ogni nodo Admin aggiuntivo.
2. Immettere l'ID connessione e il nome connessione per la copia, quindi selezionare **Salva**.
3. Scegliere il file di metadati corrispondente al nodo di amministrazione:
   a. Selezionare **azione** > **Aggiorna con metadati**.
   b. Selezionare **Scegli file** e caricare i metadati.
   c. Selezionare **Avanti**.
   d. Selezionare **Salva**.
4. Risolvere l'errore dovuto all'attributo inutilizzato:
   a. Selezionare la nuova connessione.
   b. Selezionare **Configure browser SSO > Configure Assertion Creation > Attribute Contract**.
   c. Elimina la voce per **urn:oid**.
   d. Selezionare **Salva**.

Disattiva single sign-on

È possibile disattivare SSO (Single Sign-on) se non si desidera più utilizzare questa funzionalità. È necessario disattivare il Single Sign-on prima di poter disattivare la federazione delle identità.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.

   Viene visualizzata la pagina Single Sign-on (accesso singolo).

2. Selezionare l'opzione **Disabled**.
3. Selezionare **Salva**.

   Viene visualizzato un messaggio di avviso che indica che gli utenti locali potranno accedere.

4. Selezionare **OK**.

   Al successivo accesso a StorageGRID, viene visualizzata la pagina di accesso a StorageGRID e sono necessari il nome utente e la password di un utente StorageGRID locale o federato.

Disattivare e riabilitare temporaneamente il Single Sign-on per un nodo di amministrazione

Se il sistema SSO (Single Sign-on) non funziona, potrebbe non essere possibile accedere a Grid Manager. In questo caso, è possibile disattivare e riabilitare temporaneamente SSO per un nodo di amministrazione. Per disattivare e riabilitare SSO, è necessario accedere alla shell dei comandi del nodo.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai il `Passwords.txt` file.
- Si conosce la password dell'utente root locale.

A proposito di questa attività

Dopo aver disattivato SSO per un nodo di amministrazione, è possibile accedere a Grid Manager come utente root locale. Per proteggere il sistema StorageGRID, è necessario utilizzare la shell dei comandi del nodo per riabilitare SSO sul nodo di amministrazione non appena si effettua la disconnessione.

> La disattivazione di SSO per un nodo di amministrazione non influisce sulle impostazioni SSO per qualsiasi altro nodo di amministrazione nella griglia. La casella di controllo **Enable SSO** (attiva SSO) nella pagina Single Sign-on (accesso singolo) di Grid Manager rimane selezionata e tutte le impostazioni SSO esistenti vengono mantenute, a meno che non vengano aggiornate.

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Eseguire il seguente comando:`disable-saml`

   Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

3. Confermare che si desidera disattivare SSO.

   Un messaggio indica che l'accesso singolo è disattivato sul nodo.

4. Da un browser Web, accedere a Grid Manager sullo stesso nodo di amministrazione.

   Viene visualizzata la pagina di accesso di Grid Manager perché SSO è stato disattivato.

5. Accedere con il nome utente root e la password dell'utente root locale.
6. Se SSO è stato disattivato temporaneamente perché era necessario correggere la configurazione SSO:
   a. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
   b. Modificare le impostazioni SSO non corrette o non aggiornate.
   c. Selezionare **Salva**.

      Selezionando **Save** (Salva) dalla pagina Single Sign-on (accesso singolo), l'SSO viene riattivato automaticamente per l'intera griglia.

7. Se l'SSO è stato disattivato temporaneamente perché era necessario accedere a Grid Manager per un altro motivo:

   a. Eseguire qualsiasi attività o attività da eseguire.
   b. Selezionare **Disconnetti** e chiudere Grid Manager.
   c. Riabilitare SSO sul nodo di amministrazione. È possibile eseguire una delle seguenti operazioni:

      - Eseguire il seguente comando: `enable-saml`

        Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

      Confermare che si desidera attivare SSO.

   Un messaggio indica che il Single Sign-on è attivato sul nodo.

      - Riavviare il nodo Grid: `reboot`

8. Da un browser Web, accedere a Grid Manager dallo stesso nodo di amministrazione.
9. Verificare che venga visualizzata la pagina di accesso a StorageGRID e che sia necessario immettere le credenziali SSO per accedere a Grid Manager.

USA la federazione di grid

Che cos'è la federazione di griglie?

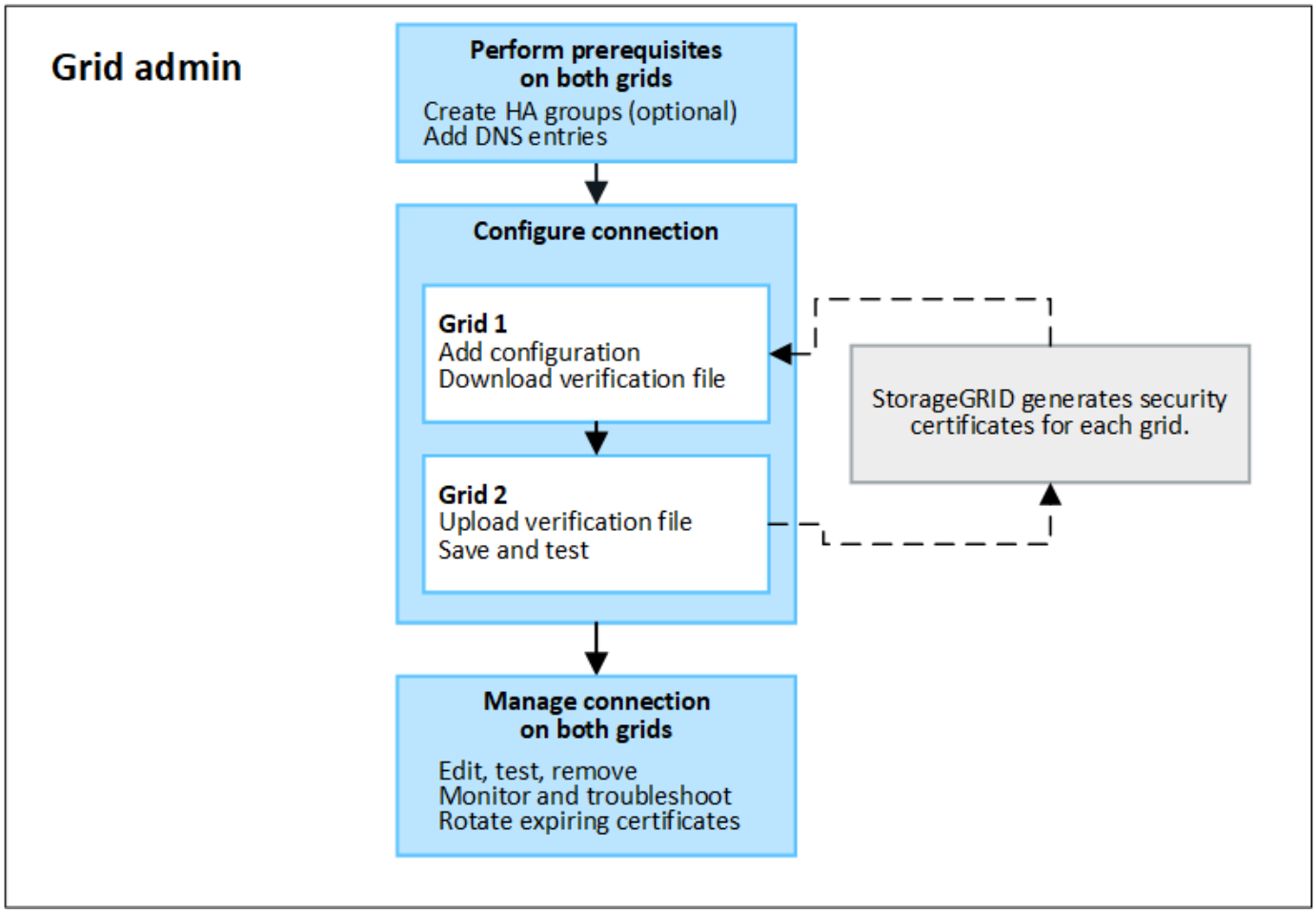
È possibile utilizzare la federazione di grid per clonare i tenant e replicare i loro oggetti tra due sistemi StorageGRID per il disaster recovery.

Che cos'è una connessione a federazione di griglie?

Una connessione a federazione di griglie è una connessione bidirezionale, affidabile e sicura tra i nodi amministratore e gateway in due sistemi StorageGRID.

Workflow per la federazione di grid

Il diagramma del flusso di lavoro riassume i passaggi per la configurazione di una connessione a federazione di griglie tra due griglie.



Considerazioni e requisiti per le connessioni a federazione di griglie

- Entrambe le griglie utilizzate per la federazione delle griglie devono eseguire StorageGRID 11,7 o versioni successive.
- Una griglia può avere una o più connessioni di federazione di griglia ad altre griglie. Ogni connessione a federazione di griglie è indipendente da qualsiasi altra connessione. Ad esempio, se la griglia 1 ha una connessione con la griglia 2 e una seconda connessione con la griglia 3, non esiste alcuna connessione implicita tra la griglia 2 e la griglia 3.
- Le connessioni a federazione di griglie sono bidirezionali. Una volta stabilita la connessione, è possibile monitorare e gestire la connessione da entrambe le griglie.
- Prima di poter utilizzare, deve esistere almeno una connessione di federazione di griglie "clone dell'account" oppure "replica cross-grid".

Requisiti di rete e indirizzo IP

- Le connessioni a federazione di griglie possono avvenire su Grid Network, Admin Network o Client Network.
- Una connessione a federazione di griglie collega una griglia a un'altra griglia. La configurazione per ogni griglia specifica un endpoint della federazione di griglia sull'altro griglia che consiste in nodi di amministrazione, nodi gateway o entrambi.
- La procedura consigliata è quella di connettersi "Gruppi ad alta disponibilità (ha)" Dei nodi Gateway e Admin su ogni griglia. L'utilizzo di gruppi ha consente di garantire che le connessioni a federazione di griglie rimangano online se i nodi non sono più disponibili. Se l'interfaccia attiva in uno dei gruppi ha non riesce, la connessione può utilizzare un'interfaccia di backup.
- Si sconsiglia di creare una connessione a federazione di griglie che utilizzi l'indirizzo IP di un singolo nodo di amministrazione o di un nodo gateway. Se il nodo diventa non disponibile, anche la connessione a federazione di griglie non sarà disponibile.
- "Replica cross-grid" Of Objects (numero di oggetti) richiede che i nodi di storage su ogni griglia siano in grado di accedere ai nodi Admin e Gateway configurati sull'altra griglia. Per ogni griglia, verificare che tutti i nodi di storage dispongano di un percorso a elevata larghezza di banda verso i nodi Admin o Gateway utilizzati per la connessione.

Utilizzare FQDN per bilanciare il carico della connessione

Per un ambiente di produzione, utilizzare FQDN (Fully Qualified Domain Name) per identificare ogni griglia della connessione. Quindi, creare le voci DNS appropriate, come indicato di seguito:

- L'FQDN per la griglia 1 è mappato a uno o più indirizzi IP virtuali (VIP) per i gruppi ha nella griglia 1 o all'indirizzo IP di uno o più nodi Admin o Gateway nella griglia 1.
- L'FQDN per la griglia 2 è mappato a uno o più indirizzi VIP per la griglia 2 o all'indirizzo IP di uno o più nodi Admin o Gateway nella griglia 2.

Quando si utilizzano più voci DNS, le richieste per utilizzare la connessione vengono bilanciate dal carico, come segue:

- Le voci DNS associate agli indirizzi VIP di più gruppi ha vengono bilanciate in base al carico tra i nodi attivi nei gruppi ha.
- Le voci DNS associate agli indirizzi IP di più nodi Admin o Gateway vengono bilanciate in base al carico tra i nodi mappati.

Requisiti delle porte

Quando si crea una connessione a federazione di griglie, è possibile specificare qualsiasi numero di porta inutilizzato compreso tra 23000 e 23999. Entrambe le griglie di questa connessione utilizzeranno la stessa porta.

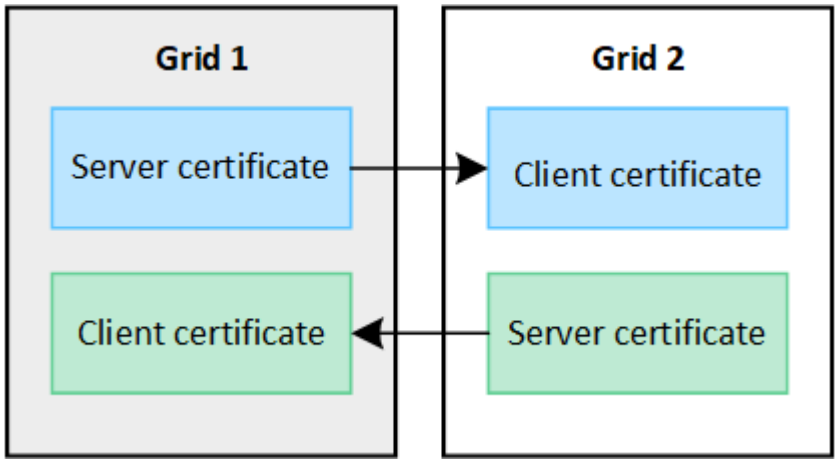
È necessario assicurarsi che nessun nodo di una delle griglie utilizzi questa porta per altre connessioni.

Requisiti del certificato

Quando si configura una connessione a federazione di griglie, StorageGRID genera automaticamente quattro certificati SSL:

- Certificati server e client per autenticare e crittografare le informazioni inviate dalla griglia 1 alla griglia 2

- Certificati server e client per autenticare e crittografare le informazioni inviate dalla griglia 2 alla griglia 1



Per impostazione predefinita, i certificati sono validi per 730 giorni (2 anni). Quando questi certificati sono prossimi alla data di scadenza,
L'avviso **scadenza del certificato di federazione griglia** ricorda di ruotare i certificati, operazione che è possibile eseguire utilizzando Grid Manager.

> Se i certificati a una delle due estremità della connessione scadono, la connessione non funziona più. La replica dei dati sarà in sospeso fino all'aggiornamento dei certificati.

Scopri di più

- "Creare connessioni di federazione di griglie"
- "Gestire le connessioni a federazione di griglie"
- "Risolvere i problemi relativi agli errori di federazione della griglia"

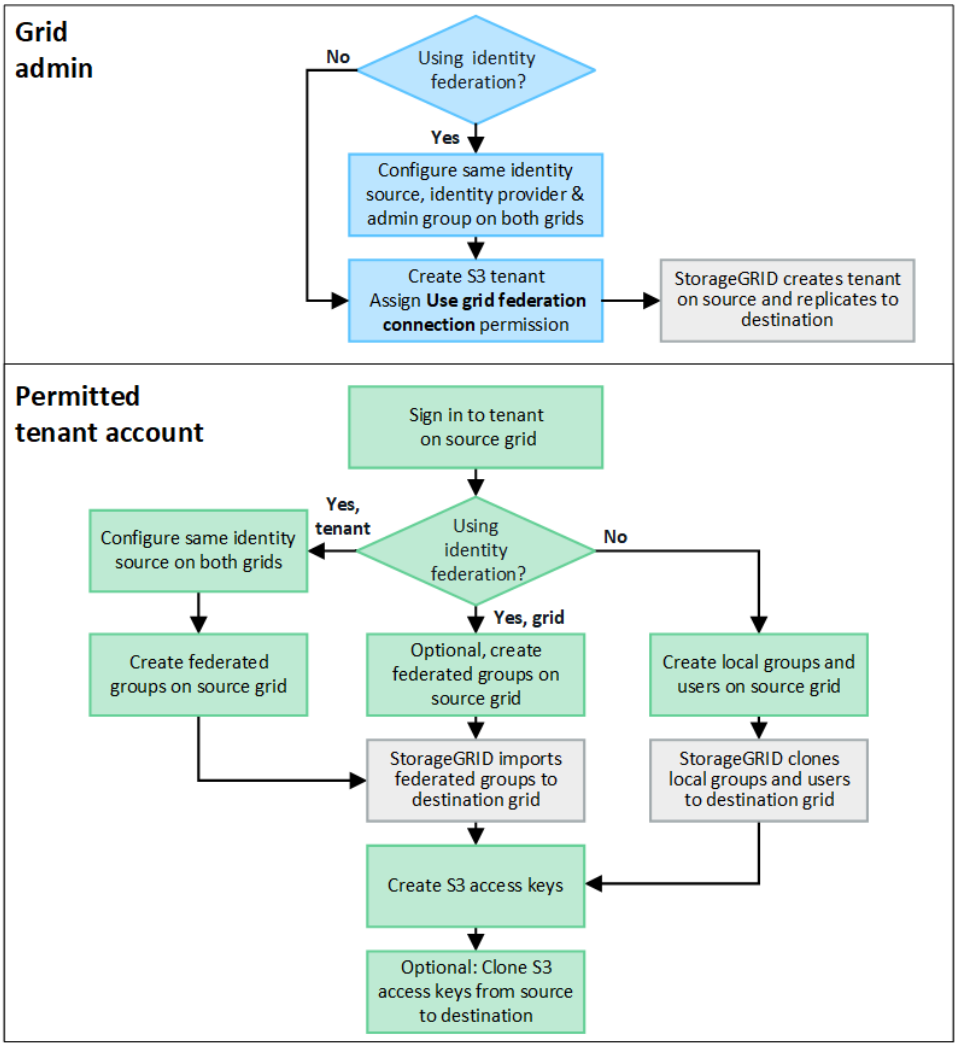
Che cos'è il clone dell'account?

Il clone dell'account è la replica automatica di un account tenant, di gruppi tenant, di utenti tenant e, facoltativamente, S3 access key tra i sistemi StorageGRID in un "connessione a federazione di griglie".

Il clone dell'account è necessario per "replica cross-grid". La clonazione delle informazioni sugli account da un sistema StorageGRID di origine a un sistema StorageGRID di destinazione garantisce che gli utenti e i gruppi tenant possano accedere ai bucket e agli oggetti corrispondenti su entrambe le griglie.

Workflow per il clone dell'account

Il diagramma del flusso di lavoro mostra i passaggi che gli amministratori della griglia e i tenant autorizzati eseguiranno per impostare il clone dell'account. Questi passaggi vengono eseguiti dopo "la connessione a federazione di griglie è configurata".



Workflow di amministrazione della griglia

Le operazioni eseguite dagli amministratori della griglia dipendono dal fatto che i sistemi StorageGRID in siano o meno presenti in "connessione a federazione di griglie" Utilizzare SSO (Single Sign-on) o federazione di identità.

Configura SSO per il clone dell'account (opzionale)

Se uno dei sistemi StorageGRID nella connessione a federazione di griglie utilizza SSO, entrambe le griglie devono utilizzare SSO. Prima di creare gli account tenant per la federazione di griglie, gli amministratori di griglie per le griglie di origine e di destinazione del tenant devono eseguire questi passaggi.

Fasi

1. Configurare la stessa origine di identità per entrambe le griglie. Vedere "USA la federazione delle identità".
2. Configurare lo stesso provider di identità SSO (IdP) per entrambe le griglie. Vedere "Configurare il single sign-on".
3. "Creare lo stesso gruppo di amministratori" su entrambe le griglie importando lo stesso gruppo federated.

   Quando si crea il tenant, si seleziona questo gruppo per disporre dell'autorizzazione di accesso root iniziale per gli account tenant di origine e di destinazione.

Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non viene replicato nella destinazione.

Configura federazione di identità a livello di griglia per il clone dell'account (opzionale)

Se uno dei sistemi StorageGRID utilizza la federazione delle identità senza SSO, entrambe le griglie devono utilizzare la federazione delle identità. Prima di creare gli account tenant per la federazione di griglie, gli amministratori di griglie per le griglie di origine e di destinazione del tenant devono eseguire questi passaggi.

Fasi

1. Configurare la stessa origine di identità per entrambe le griglie. Vedere "USA la federazione delle identità".
2. Facoltativamente, se un gruppo federated disporrà dell'autorizzazione di accesso root iniziale per gli account tenant di origine e di destinazione, "creare lo stesso gruppo di amministratori" su entrambe le griglie importando lo stesso gruppo federated.

   Se si assegna l'autorizzazione di accesso root a un gruppo federated che non esiste su entrambe le griglie, il tenant non viene replicato nella griglia di destinazione.

3. Se non si desidera che un gruppo federated disponga dell'autorizzazione di accesso root iniziale per entrambi gli account, specificare una password per l'utente root locale.

Creare un account tenant S3 consentito

Dopo la configurazione opzionale di SSO o federazione di identità, un amministratore di grid esegue questi passaggi per determinare quali tenant possono replicare gli oggetti bucket in altri sistemi StorageGRID.

Fasi

1. Determinare quale griglia si desidera essere la griglia di origine del tenant per le operazioni di cloni degli account.

   La griglia in cui viene creato il tenant è nota come *griglia di origine* del tenant. La griglia in cui viene replicato il tenant è nota come *griglia di destinazione* del tenant.

2. In tale griglia, creare un nuovo account tenant S3 o modificare un account esistente.
3. Assegnare l'autorizzazione **Usa connessione federazione griglia**.
4. Se l'account tenant gestirà i propri utenti federati, assegnare l'autorizzazione **use own Identity source**.

   Se questa autorizzazione viene assegnata, gli account tenant di origine e di destinazione devono configurare la stessa origine identità prima di creare gruppi federati. I gruppi federati aggiunti al tenant di origine non possono essere clonati nel tenant di destinazione a meno che entrambe le griglie non utilizzino la stessa origine di identità.

5. Selezionare una connessione a federazione di griglie specifica.
6. Salvare il tenant nuovo o modificato.

   Quando viene salvato un nuovo tenant con l'autorizzazione **use grid Federation Connection**, StorageGRID crea automaticamente una replica del tenant sull'altro grid, come segue:

   - Entrambi gli account tenant hanno lo stesso ID account, il nome, la quota di storage e le stesse autorizzazioni assegnate.

- Se è stato selezionato un gruppo federated per disporre dell'autorizzazione di accesso root per il tenant, tale gruppo viene clonato nel tenant di destinazione.
- Se si seleziona un utente locale per disporre dell'autorizzazione di accesso root per il tenant, tale utente viene clonato nel tenant di destinazione. Tuttavia, la password per quell'utente non viene clonata.

Per ulteriori informazioni, vedere
"Gestire i tenant autorizzati per la federazione di grid".

Flusso di lavoro account tenant consentito

Dopo che un tenant con l'autorizzazione **Usa connessione federazione griglia** è stato replicato nella griglia di destinazione, gli account tenant autorizzati possono eseguire queste operazioni per clonare gruppi tenant, utenti e chiavi di accesso S3.

Fasi

1. Accedere all'account tenant sulla griglia di origine del tenant.
2. Se consentito, configurare la federazione di identificazione sugli account tenant di origine e di destinazione.
3. Creare gruppi e utenti nel tenant di origine.

   Quando vengono creati nuovi gruppi o utenti nel tenant di origine, StorageGRID li clonerà automaticamente nel tenant di destinazione, ma non si verificherà alcun cloning dalla destinazione all'origine.

4. Creare chiavi di accesso S3.
5. Facoltativamente, clonare le chiavi di accesso S3 dal tenant di origine al tenant di destinazione.

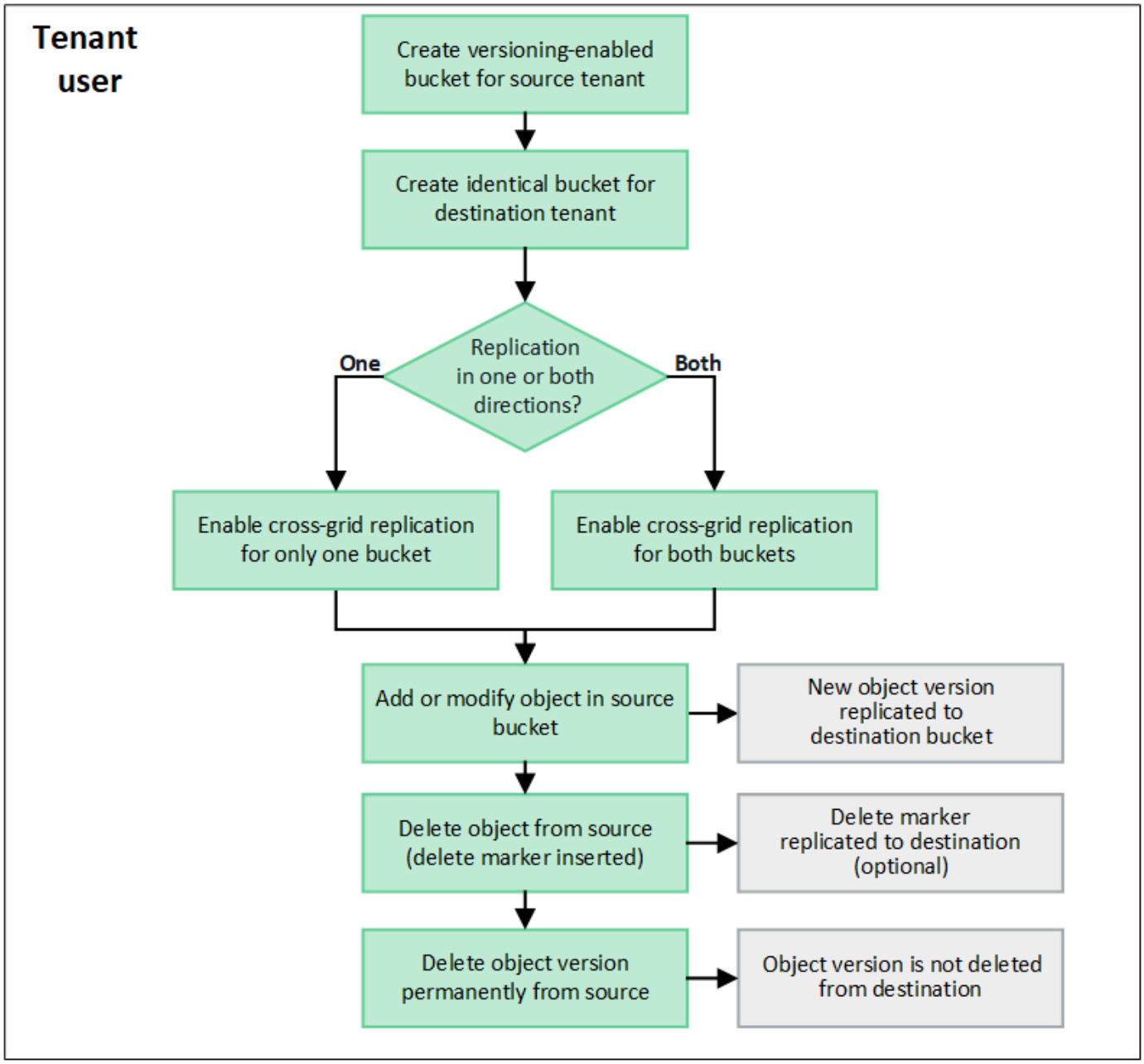
Per ulteriori informazioni sul flusso di lavoro dell'account tenant consentito e su come clonare gruppi, utenti e chiavi di accesso S3, vedere "Clonare utenti e gruppi tenant" e. "Clonare le chiavi di accesso S3 utilizzando l'API".

Che cos'è la replica cross-grid?

La replica cross-grid è la replica automatica degli oggetti tra bucket S3 selezionati in due sistemi StorageGRID collegati in un "connessione a federazione di griglie". "Clone dell'account" è necessario per la replica cross-grid.

Workflow per la replica cross-grid

Il diagramma del flusso di lavoro riassume i passaggi per la configurazione della replica cross-grid tra bucket su due griglie.



Requisiti per la replica cross-grid

Se un account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** per utilizzare uno o più account "connessioni a federazione di griglie", Un utente tenant con autorizzazione di accesso Root può creare bucket identici negli account tenant corrispondenti su ogni griglia. Questi bucket:

- Deve avere lo stesso nome ma possono avere regioni diverse
- È necessario attivare la versione
- È necessario che S3 Object Lock sia disattivato
- Deve essere vuoto

Una volta creati entrambi i bucket, è possibile configurare la replica cross-grid per uno o entrambi i bucket.

Scopri di più

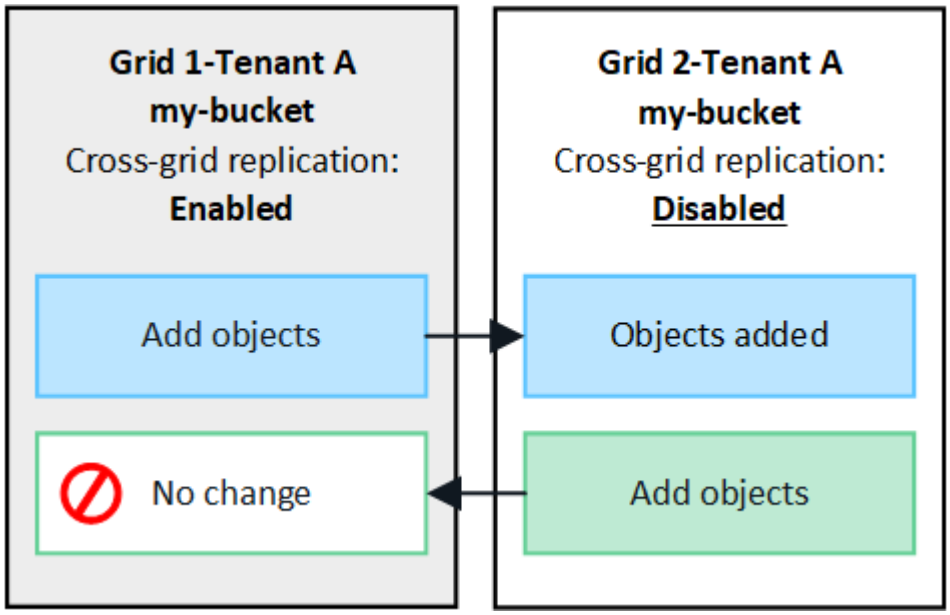
"Gestire la replica cross-grid"

Come funziona la replica cross-grid

È possibile configurare la replica cross-grid in modo che avvenga in una direzione o in entrambe le direzioni.

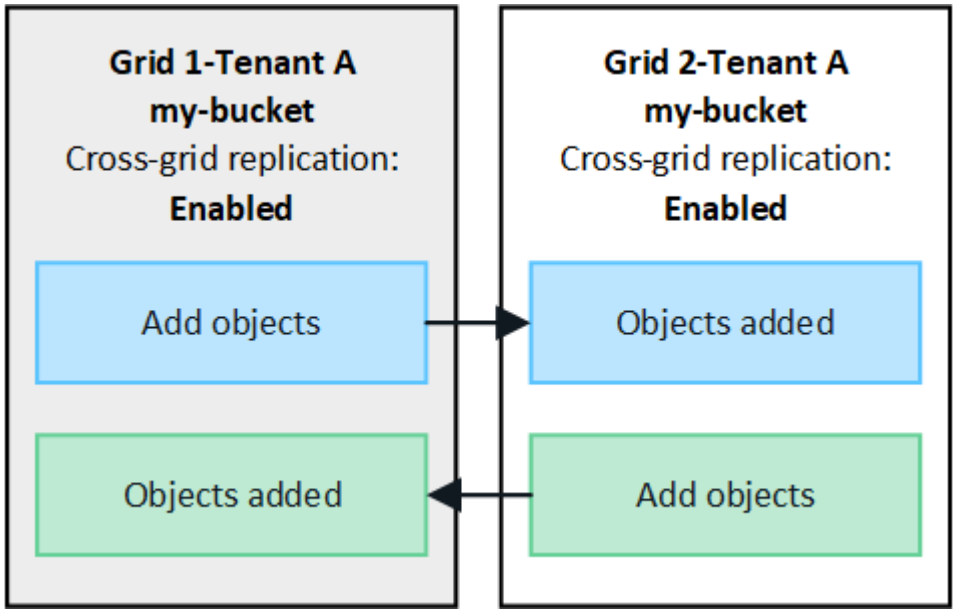
Replica in un'unica direzione

Se si attiva la replica cross-grid per un bucket su una sola griglia, gli oggetti aggiunti a quel bucket (il bucket di origine) vengono replicati nel bucket corrispondente sull'altra griglia (il bucket di destinazione). Tuttavia, gli oggetti aggiunti al bucket di destinazione non vengono replicati di nuovo nell'origine. Nella figura, la replica cross-grid è attivata per `my-bucket` Dalla griglia 1 alla griglia 2, ma non è attivata nell'altra direzione.



Replica in entrambe le direzioni

Se si attiva la replica cross-grid per lo stesso bucket su entrambe le griglie, gli oggetti aggiunti a entrambi i bucket vengono replicati nell'altra griglia. Nella figura, la replica cross-grid è attivata per `my-bucket` in entrambe le direzioni.



Cosa succede quando gli oggetti vengono acquisiti?

Quando un client S3 aggiunge un oggetto a un bucket con replica cross-grid attivata, si verifica quanto segue:

1. StorageGRID replica automaticamente l'oggetto dal bucket di origine al bucket di destinazione. Il tempo necessario per eseguire questa operazione di replica in background dipende da diversi fattori, tra cui il numero di altre operazioni di replica in sospeso.

   Il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta GetObject o HeadObject. La risposta include uno specifico StorageGRID `x-ntap-sg-cgr-replication-status` intestazione della risposta, che avrà uno dei seguenti valori:
   Il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta GetObject o HeadObject. La risposta include uno specifico StorageGRID `x-ntap-sg-cgr-replication-status` intestazione della risposta, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• **SUCCESSO**: La replica è riuscita per tutte le connessioni alla rete. • **PENDING**: L'oggetto non è stato replicato in almeno una connessione di rete. • **GUASTO**: La replica non è in sospeso per nessuna connessione alla rete e almeno una ha avuto esito negativo con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

   > StorageGRID non supporta `x-amz-replication-status` intestazione.

2. StorageGRID utilizza i criteri ILM attivi di ciascuna griglia per gestire gli oggetti, esattamente come per qualsiasi altro oggetto. Ad esempio, l'oggetto A sulla griglia 1 potrebbe essere memorizzato come due copie replicate e conservato per sempre, mentre la copia dell'oggetto A replicata sulla griglia 2 potrebbe essere memorizzata utilizzando la codifica di cancellazione 2+1 ed eliminata dopo tre anni.

Cosa succede quando gli oggetti vengono cancellati?

Come descritto in "Eliminare il flusso di dati", StorageGRID può eliminare un oggetto per uno dei seguenti motivi:

- Il client S3 invia una richiesta di eliminazione.
- Un utente tenant Manager seleziona "Eliminare gli oggetti nel bucket" opzione per rimuovere tutti gli oggetti da un bucket.
- Il bucket ha una configurazione del ciclo di vita che scade.
- L'ultimo periodo di tempo nella regola ILM per l'oggetto termina e non sono stati specificati ulteriori posizionamenti.

Quando StorageGRID elimina un oggetto a causa di un'operazione Delete Objects (Elimina oggetti) nel bucket, della scadenza del ciclo di vita del bucket o della scadenza del posizionamento ILM, l'oggetto replicato non viene mai cancellato dall'altra griglia in una connessione a federazione di griglie. Tuttavia, i marker di eliminazione aggiunti al bucket di origine da S3 client Delete possono essere replicati nel bucket di destinazione.

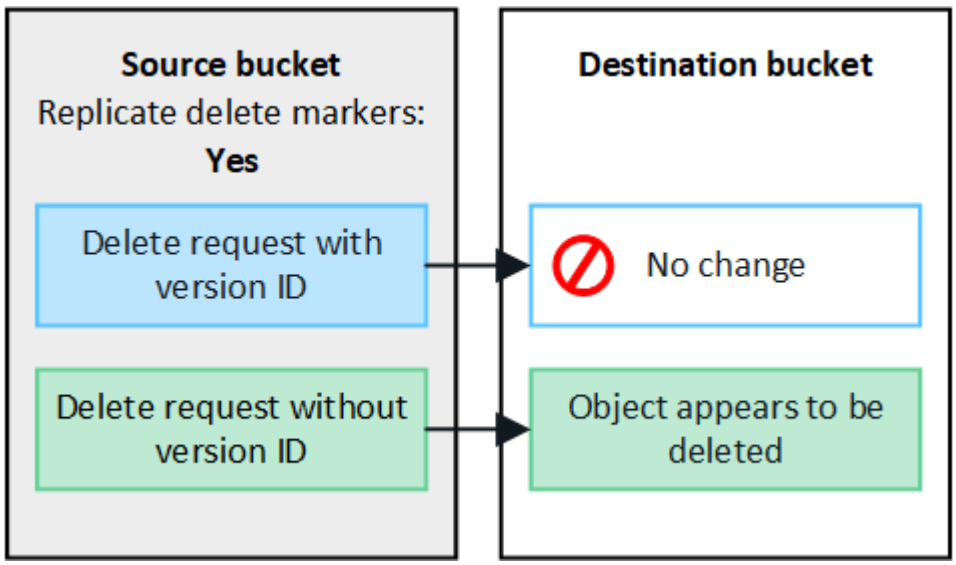
Per capire cosa accade quando un client S3 elimina oggetti da un bucket che ha la replica cross-grid attivata, rivedere come i client S3 eliminano oggetti dai bucket che hanno la versione attivata, come segue:

- Se un client S3 invia una richiesta di eliminazione che include un ID di versione, la versione dell'oggetto viene rimossa in modo permanente. Nessun marker di eliminazione aggiunto al bucket.
- Se un client S3 invia una richiesta di eliminazione che non include un ID di versione, StorageGRID non elimina alcuna versione di oggetto. Al contrario, aggiunge un contrassegno di eliminazione al bucket. Il contrassegno DELETE fa sì che StorageGRID agisca come se l'oggetto fosse stato cancellato:
  - Una richiesta GetObject senza ID versione non riesce con `404 No Object Found`
  - Una richiesta GetObject con un ID di versione valido avrà esito positivo e restituirà la versione dell'oggetto richiesta.

Quando un client S3 elimina un oggetto da un bucket con la replica cross-grid attivata, StorageGRID determina se replicare la richiesta di eliminazione nella destinazione, come segue:

- Se la richiesta di eliminazione include un ID di versione, la versione dell'oggetto viene rimossa in modo permanente dalla griglia di origine. Tuttavia, StorageGRID non replica le richieste di eliminazione che includono un ID di versione, pertanto la stessa versione dell'oggetto non viene eliminata dalla destinazione.
- Se la richiesta di eliminazione non include un ID di versione, StorageGRID può facoltativamente replicare il marker di eliminazione, in base alla configurazione della replica cross-grid per il bucket:
  - Se si sceglie di replicare i marker di eliminazione (impostazione predefinita), un marker di eliminazione viene aggiunto al bucket di origine e replicato nel bucket di destinazione. In effetti, l'oggetto sembra essere cancellato su entrambe le griglie.
  - Se si sceglie di non replicare i marker di eliminazione, un marker di eliminazione viene aggiunto al bucket di origine ma non viene replicato nel bucket di destinazione. In effetti, gli oggetti eliminati nella griglia di origine non vengono cancellati nella griglia di destinazione.

Nella figura, **Replicate delete markers** è stato impostato su **Yes** quando "la replica cross-grid è stata attivata". Le richieste di eliminazione per il bucket di origine che includono un ID di versione non elimineranno gli oggetti dal bucket di destinazione. Le richieste di eliminazione per il bucket di origine che non includono un ID di versione verranno visualizzate per eliminare gli oggetti nel bucket di destinazione.



Se si desidera mantenere le eliminazioni degli oggetti sincronizzate tra le griglie, creare le corrispondenti "Configurazioni del ciclo di vita S3" per i bucket su entrambe le griglie.

Modalità di replica degli oggetti crittografati

Quando si utilizza la replica cross-grid per replicare oggetti tra griglie, è possibile crittografare singoli oggetti, utilizzare la crittografia bucket predefinita o configurare la crittografia a livello di griglia. È possibile aggiungere, modificare o rimuovere le impostazioni di crittografia predefinite del bucket o dell'intera griglia prima o dopo aver attivato la replica cross-grid per un bucket.

Per crittografare singoli oggetti, è possibile utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID) quando si aggiungono gli oggetti al bucket di origine. Utilizzare `x-amz-server-side-encryption` richiedi intestazione e specifica `AES256`. Vedere "Utilizzare la crittografia lato server".

L'utilizzo di SSE-C (crittografia lato server con chiavi fornite dal cliente) non è supportato per la replica cross-grid. L'operazione di acquisizione non riesce.

Per utilizzare la crittografia predefinita per un bucket, utilizzare una richiesta PutBucketEncryption e impostare `SSEAlgorithm` parametro a. `AES256`. La crittografia a livello di bucket si applica a tutti gli oggetti acquisiti senza `x-amz-server-side-encryption` intestazione della richiesta. Vedere "Operazioni sui bucket".

Per utilizzare la crittografia a livello di griglia, impostare l'opzione **Stored Object Encryption** su **AES-256**. La crittografia a livello di griglia si applica a tutti gli oggetti che non sono crittografati a livello di bucket o che sono acquisiti senza `x-amz-server-side-encryption` intestazione della richiesta. Vedere "Configurare le opzioni di rete e degli oggetti".

SSE non supporta AES-128. Se l'opzione **Stored Object Encryption** è attivata per la griglia di origine utilizzando l'opzione **AES-128**, l'utilizzo dell'algoritmo AES-128 non verrà propagato all'oggetto replicato. L'oggetto replicato utilizzerà invece l'impostazione predefinita del bucket o della crittografia a livello di griglia della destinazione, se disponibile.

Quando si determina come crittografare gli oggetti di origine, StorageGRID applica le seguenti regole:

1. Utilizzare `x-amz-server-side-encryption` acquisire l'intestazione, se presente.
2. Se non è presente un'intestazione di acquisizione, utilizzare l'impostazione di crittografia predefinita del bucket, se configurata.
3. Se un'impostazione bucket non è configurata, utilizzare l'impostazione di crittografia a livello di griglia, se configurata.
4. Se non è presente un'impostazione a livello di griglia, non crittografare l'oggetto di origine.

Quando si determina come crittografare gli oggetti replicati, StorageGRID applica queste regole nel seguente ordine:

1. Utilizzare la stessa crittografia dell'oggetto di origine, a meno che tale oggetto non utilizzi la crittografia AES-128.
2. Se l'oggetto di origine non è crittografato o utilizza AES-128, utilizzare l'impostazione di crittografia predefinita del bucket di destinazione, se configurato.
3. Se il bucket di destinazione non dispone di un'impostazione di crittografia, utilizzare l'impostazione di crittografia a livello di griglia della destinazione, se configurata.
4. Se non è presente un'impostazione a livello di griglia, non crittografare l'oggetto di destinazione.

PutObjectTagging e DeleteObjectTagging non sono supportati

Le richieste PutObjectTagging e DeleteObjectTagging non sono supportate per gli oggetti nei bucket in cui è abilitata la replica cross-grid.

Se un client S3 esegue una richiesta PutObjectTagging o DeleteObjectTagging, `501 Not Implemented` viene restituito. Il messaggio è `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`.

Come vengono replicati gli oggetti segmentati

Le dimensioni massime dei segmenti della griglia di origine si applicano agli oggetti replicati nella griglia di destinazione. Quando gli oggetti vengono replicati in un'altra griglia, l'impostazione **Maximum Segment Size** (**CONFIGURATION** > **System** > **Storage options**) della griglia di origine viene utilizzata su entrambe le griglie. Ad esempio, supponiamo che la dimensione massima del segmento per la griglia di origine sia di 1 GB, mentre la dimensione massima del segmento della griglia di destinazione sia di 50 MB. Se si riceve un oggetto da 2 GB nella griglia di origine, tale oggetto viene salvato come due segmenti da 1 GB. Inoltre, verrà replicato nella griglia di destinazione come due segmenti da 1 GB, anche se la dimensione massima del segmento della griglia è di 50 MB.

Confronta la replica cross-grid e la replica CloudMirror

Mentre inizi a utilizzare la federazione di griglie, esamina le analogie e le differenze tra "replica cross-grid" e a. "Servizio di replica di StorageGRID CloudMirror".

	Replica cross-grid	Servizio di replica di CloudMirror
Qual è lo scopo principale?	Un sistema StorageGRID funge da sistema di disaster recovery. Gli oggetti in un bucket possono essere replicati tra le griglie in una o entrambe le direzioni.	Consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). La replica di CloudMirror crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente. Questa copia indipendente non viene utilizzata come backup, ma viene spesso ulteriormente elaborata nel cloud.
Come viene configurato?	1. Configurare una connessione a federazione di griglie tra due griglie. 2. Aggiungere nuovi account tenant, che vengono clonati automaticamente nell'altra griglia. 3. Aggiungere nuovi gruppi di tenant e utenti, che vengono clonati. 4. Creare bucket corrispondenti su ogni griglia e consentire la replica cross-grid in una o entrambe le direzioni.	1. Un utente tenant configura la replica di CloudMirror definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) utilizzando Tenant Manager o l'API S3. 2. Qualsiasi bucket di proprietà dell'account tenant può essere configurato per puntare all'endpoint CloudMirror.

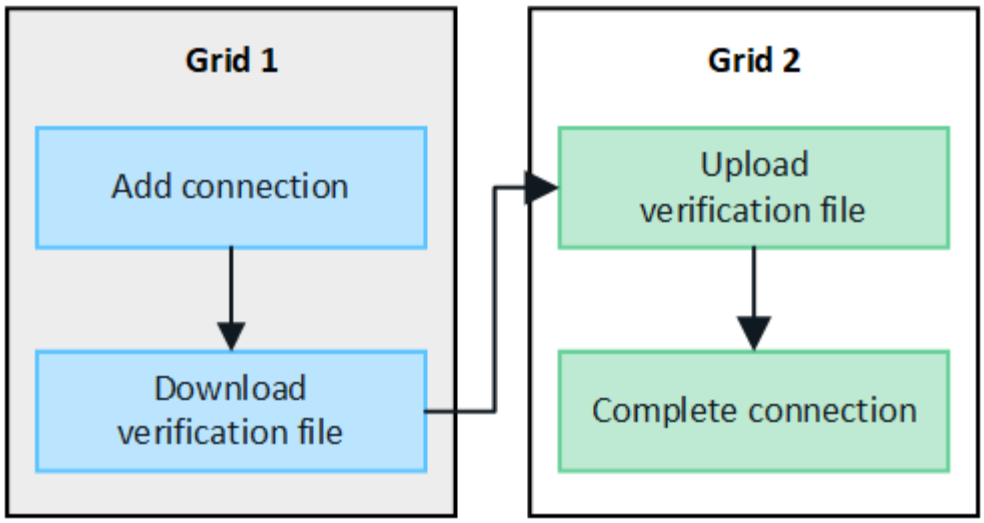
	Replica cross-grid	Servizio di replica di CloudMirror
Chi è responsabile della sua configurazione?	• Un amministratore di grid configura la connessione e i tenant. • Gli utenti tenant configurano gruppi, utenti, chiavi e bucket.	In genere, un utente tenant.
Qual è la destinazione?	Un bucket S3 corrispondente e identico sull'altro sistema StorageGRID nella connessione a federazione di griglia.	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3). • Piattaforma Google Cloud (GCP)
È necessario il controllo della versione degli oggetti?	Sì, sia il bucket di origine che quello di destinazione devono avere attivato la versione degli oggetti.	No, la replica di CloudMirror supporta qualsiasi combinazione di bucket senza versioni e con versioni sia sull'origine che sulla destinazione.
Qual è la causa dello spostamento degli oggetti nella destinazione?	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket con replica cross-grid attivata.	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket configurato con un endpoint CloudMirror. Gli oggetti che esistevano nel bucket di origine prima della configurazione del bucket con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come vengono replicati gli oggetti?	La replica cross-grid crea oggetti con versione e replica l'ID della versione dal bucket di origine al bucket di destinazione. Ciò consente di mantenere l'ordine delle versioni in entrambe le griglie.	La replica di CloudMirror non richiede bucket abilitati per il controllo delle versioni, pertanto CloudMirror può eseguire l'ordine solo per una chiave all'interno di un sito. Non vi sono garanzie che l'ordine venga mantenuto per le richieste a un oggetto in un sito diverso.
Cosa succede se un oggetto non può essere replicato?	L'oggetto viene messo in coda per la replica, in base ai limiti di storage dei metadati.	L'oggetto viene messo in coda per la replica, in base ai limiti dei servizi della piattaforma (vedere "Consigli per l'utilizzo dei servizi della piattaforma").
I metadati di sistema dell'oggetto sono replicati?	Sì, quando un oggetto viene replicato nell'altra griglia, vengono replicati anche i relativi metadati di sistema. I metadati saranno identici su entrambe le griglie.	No, quando un oggetto viene replicato nel bucket esterno, i relativi metadati di sistema vengono aggiornati. I metadati variano in base al tempo di acquisizione e al comportamento dell'infrastruttura S3 indipendente.

	Replica cross-grid	Servizio di replica di CloudMirror
Come vengono recuperati gli oggetti?	Le applicazioni possono recuperare o leggere gli oggetti effettuando una richiesta al bucket su una griglia.	Le applicazioni possono recuperare o leggere oggetti effettuando una richiesta a StorageGRID o alla destinazione S3. Si supponga, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti in un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è necessario utilizzare StorageGRID.
Cosa succede se un oggetto viene cancellato?	• Le richieste di eliminazione che includono un ID di versione non vengono mai replicate nella griglia di destinazione. • Le richieste di eliminazione che non includono un ID di versione aggiungono un contrassegno di eliminazione al bucket di origine, che può essere facoltativamente replicato nella griglia di destinazione. • Se la replica cross-grid è configurata per una sola direzione, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.	I risultati variano in base allo stato di versione dei bucket di origine e di destinazione (che non devono essere identici): • Se entrambi i bucket sono con versione, una richiesta di eliminazione aggiungerà un indicatore di eliminazione in entrambe le posizioni. • Se viene configurato solo il bucket di origine, una richiesta di eliminazione aggiungerà un indicatore di eliminazione all'origine, ma non alla destinazione. • Se nessuno dei bucket è dotato di versione, una richiesta di eliminazione elimina l'oggetto dall'origine ma non dalla destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.

Creare connessioni di federazione di griglie

È possibile creare una connessione a federazione di griglie tra due sistemi StorageGRID se si desidera clonare i dettagli del tenant e replicare i dati degli oggetti.

Come illustrato nella figura, la creazione di una connessione a federazione di griglie include operazioni su entrambe le griglie. La connessione viene aggiunta su una griglia e completata sull'altra. È possibile iniziare da una delle due griglie.



Prima di iniziare

- Hai esaminato il "considerazioni e requisiti" per la configurazione delle connessioni di federazione di griglie.
- Se si intende utilizzare FQDN (Fully Qualified Domain Name) per ogni griglia invece degli indirizzi IP o VIP, si conoscono i nomi da utilizzare e si conferma che il server DNS per ogni griglia dispone delle voci appropriate.
- Si sta utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso root e della passphrase di provisioning per entrambe le griglie.

Aggiungi connessione

Eseguire questa procedura su uno dei due sistemi StorageGRID.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale su una griglia.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare **Aggiungi connessione**.
4. Inserire i dettagli della connessione.

Campo	Descrizione
Nome della connessione	Un nome univoco che consente di riconoscere questa connessione, ad esempio "Grid 1-Grid 2".
FQDN o IP per questa griglia	Una delle seguenti opzioni: • L'FQDN della griglia a cui si è attualmente connessi • Indirizzo VIP di un gruppo ha su questa griglia • Indirizzo IP di un nodo Admin o di un nodo Gateway in questa griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla griglia di destinazione.

Campo	Descrizione
Porta	La porta che si desidera utilizzare per questa connessione. È possibile immettere un numero di porta inutilizzato compreso tra 23000 e 23999. Entrambe le griglie di questa connessione utilizzeranno la stessa porta. È necessario assicurarsi che nessun nodo di una delle griglie utilizzi questa porta per altre connessioni.
Giorni di validità del certificato per questa griglia	Il numero di giorni in cui si desidera che i certificati di protezione per questa griglia nella connessione siano validi. Il valore predefinito è 730 giorni (2 anni), ma è possibile immettere un valore compreso tra 1 e 762 giorni. StorageGRID genera automaticamente certificati client e server per ogni griglia quando si salva la connessione.
Passphrase di provisioning per questa griglia	La passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
FQDN o IP per l'altra griglia	Una delle seguenti opzioni: • L'FQDN della griglia a cui si desidera connettersi • Indirizzo VIP di un gruppo ha sull'altra griglia • Indirizzo IP di un nodo Admin o di un nodo Gateway nell'altra griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla rete di origine.

5. Selezionare **Salva e continua**.
6. Per la fase Download verfica file, selezionare **Download verfica file**.

   Una volta completata la connessione sull'altra griglia, non è più possibile scaricare il file di verifica da nessuna griglia.

7. Individuare il file scaricato (*`connection-name`*`.grid-federation`) e salvarlo in una posizione sicura.

   > Questo file contiene segreti (mascherati come *****) e altri dettagli sensibili e devono essere memorizzati e trasmessi in modo sicuro.

8. Selezionare **Close** (Chiudi) per tornare alla pagina Grid Federation (federazione griglia).
9. Verificare che sia visualizzata la nuova connessione e che il relativo **stato della connessione** sia **in attesa di connessione**.
10. Fornire il *`connection-name`*`.grid-federation` all'amministratore della griglia per l'altra griglia.

Connessione completa

Eseguire questa procedura sul sistema StorageGRID a cui si sta effettuando la connessione (l'altra griglia).

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare **carica file di verifica** per accedere alla pagina carica.
4. Selezionare **carica file di verifica**. Quindi, individuare e selezionare il file scaricato dalla prima griglia (*connection-name*`.grid-federation`).

   Vengono visualizzati i dettagli della connessione.

5. Se si desidera, immettere un numero diverso di giorni validi per i certificati di sicurezza per questa griglia. Per impostazione predefinita, la voce **Certificate Valid Days** (giorni validi certificato) corrisponde al valore immesso nella prima griglia, ma ciascuna griglia può utilizzare date di scadenza diverse.

   In generale, utilizzare lo stesso numero di giorni per i certificati su entrambi i lati della connessione.

   > Se i certificati a una delle due estremità della connessione scadono, la connessione smette di funzionare e le repliche saranno in sospeso fino all'aggiornamento dei certificati.

6. Inserire la passphrase di provisioning per la griglia a cui si è attualmente connessi.
7. Selezionare **Save and test** (Salva e verifica).

   I certificati vengono generati e la connessione viene testata. Se la connessione è valida, viene visualizzato un messaggio di esito positivo e la nuova connessione viene elencata nella pagina Grid Federation. Lo stato **Connection** sarà **Connected**.

   Se viene visualizzato un messaggio di errore, risolvere eventuali problemi. Vedere "Risolvere i problemi relativi agli errori di federazione della griglia".

8. Accedere alla pagina Grid Federation (federazione griglia) nella prima griglia e aggiornare il browser. Verificare che lo stato della connessione sia ora **connesso**.
9. Una volta stabilita la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

   Se si modifica questa connessione, viene creato un nuovo file di verifica. Il file originale non può essere riutilizzato.

Al termine

- Esaminare le considerazioni per "gestione dei tenant autorizzati".
- "Creare uno o più nuovi account tenant", Assegnare l'autorizzazione **Usa connessione federazione griglia** e selezionare la nuova connessione.
- "Gestire la connessione" secondo necessità. È possibile modificare i valori di connessione, verificare una connessione, ruotare i certificati di connessione o rimuovere una connessione.
- "Monitorare la connessione" Come parte delle normali attività di monitoraggio StorageGRID.
- "Risolvere i problemi di connessione", inclusa la risoluzione di eventuali avvisi ed errori relativi al clone dell'account e alla replica cross-grid.

Gestire le connessioni a federazione di griglie

La gestione delle connessioni a federazione di griglie tra sistemi StorageGRID include la modifica dei dettagli di connessione, la rotazione dei certificati, la rimozione delle autorizzazioni del tenant e la rimozione delle connessioni inutilizzate.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su una delle griglie utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root" per la griglia a cui si è effettuato l'accesso.

Modifica una connessione a federazione di griglie

È possibile modificare una connessione a federazione di griglie effettuando l'accesso al nodo di amministrazione primario su una delle griglie della connessione. Una volta apportate le modifiche alla prima griglia, è necessario scaricare un nuovo file di verifica e caricarlo nell'altra griglia.

> ⓘ Durante la modifica della connessione, le richieste di replica cross-grid o clone dell'account continueranno a utilizzare le impostazioni di connessione esistenti. Tutte le modifiche apportate alla prima griglia vengono salvate localmente, ma non vengono utilizzate fino a quando non vengono caricate nella seconda griglia, salvate e testate.

Avviare la modifica della connessione

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale su una griglia.
2. Selezionare **NODI** e verificare che tutti gli altri nodi Admin del sistema siano in linea.

   > ⓘ Quando si modifica una connessione a federazione di griglie, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi di amministrazione della prima griglia. Se il file non può essere salvato in tutti i nodi di amministrazione, viene visualizzato un messaggio di avviso quando si seleziona **Salva e test**.

3. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
4. Modificare i dettagli della connessione utilizzando il menu **azioni** della pagina Grid Federation o la pagina dei dettagli per una connessione specifica. Vedere "Creare connessioni di federazione di griglie" per cosa partecipare.

   Menu delle azioni

   a. Selezionare il pulsante di opzione per la connessione.
   b. Selezionare **azioni** > **Modifica**.
   c. Inserire le nuove informazioni.

   Pagina dei dettagli

   a. Selezionare un nome di connessione per visualizzarne i dettagli.
   b. Selezionare **Modifica**.
   c. Inserire le nuove informazioni.

5. Inserire la passphrase di provisioning per la griglia a cui si è connessi.
6. Selezionare **Salva e continua**.

   I nuovi valori vengono salvati, ma non vengono applicati alla connessione fino a quando non si carica il nuovo file di verifica sull'altra griglia.

7. Selezionare **Scarica file di verifica**.

   Per scaricare il file in un secondo momento, accedere alla pagina dei dettagli della connessione.

8. Individuare il file scaricato (*connection-name*`.grid-federation`) e salvarlo in una posizione sicura.

   > Il file di verifica contiene segreti e deve essere memorizzato e trasmesso in modo sicuro.

9. Selezionare **Close** (Chiudi) per tornare alla pagina Grid Federation (federazione griglia).
10. Verificare che lo stato della connessione sia **Pending EDIT** (Modifica in sospeso).

    > Se lo stato della connessione era diverso da **connesso** quando si inizia a modificare la connessione, non verrà modificato in **in attesa di modifica**.

11. Fornire il *connection-name*`.grid-federation` all'amministratore della griglia per l'altra griglia.

Terminare la modifica della connessione

Terminare la modifica della connessione caricando il file di verifica sull'altra griglia.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare **carica file di verifica** per accedere alla pagina di caricamento.
4. Selezionare **carica file di verifica**. Quindi, individuare e selezionare il file scaricato dalla prima griglia.
5. Inserire la passphrase di provisioning per la griglia a cui si è attualmente connessi.
6. Selezionare **Save and test** (Salva e verifica).

   Se è possibile stabilire la connessione utilizzando i valori modificati, viene visualizzato un messaggio di esito positivo. In caso contrario, viene visualizzato un messaggio di errore. Esaminare il messaggio e risolvere eventuali problemi.

7. Chiudere la procedura guidata per tornare alla pagina Grid Federation.
8. Verificare che lo stato della connessione sia **connesso**.
9. Accedere alla pagina Grid Federation (federazione griglia) nella prima griglia e aggiornare il browser. Verificare che lo stato della connessione sia ora **connesso**.
10. Una volta stabilita la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

Test di una connessione a federazione di griglie

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Verificare la connessione utilizzando il menu **azioni** della pagina Grid Federation o la pagina dei dettagli per una connessione specifica.

Menu delle azioni

a. Selezionare il pulsante di opzione per la connessione.
b. Selezionare **azioni** > **Test**.

Pagina dei dettagli

a. Selezionare un nome di connessione per visualizzarne i dettagli.
b. Selezionare **Test di connessione**.

4. Controllare lo stato della connessione:

Stato della connessione	Descrizione
Connesso	Entrambe le griglie sono collegate e comunicano normalmente.
Errore	La connessione si trova in uno stato di errore. Ad esempio, un certificato è scaduto o un valore di configurazione non è più valido.
In attesa di modifica	La connessione su questa griglia è stata modificata, ma la connessione sta ancora utilizzando la configurazione esistente. Per completare la modifica, caricare il nuovo file di verifica nell'altra griglia.
In attesa di connessione	La connessione è stata configurata su questa griglia, ma la connessione non è stata completata sull'altra griglia. Scarica il file di verifica da questa griglia e caricalo nell'altra griglia.
Sconosciuto	La connessione si trova in uno stato sconosciuto, probabilmente a causa di un problema di rete o di un nodo offline.

5. Se lo stato della connessione è **Error**, risolvere eventuali problemi. Quindi, selezionare di nuovo **Test di connessione** per confermare che il problema è stato risolto.

rotazione dei certificati di connessione

Ogni connessione a federazione di griglie utilizza quattro certificati SSL generati automaticamente per proteggere la connessione. Quando i due certificati per ogni griglia si avvicinano alla data di scadenza, l'avviso **scadenza del certificato federazione griglia** ricorda di ruotare i certificati.

> Se i certificati a una delle due estremità della connessione scadono, la connessione smette di funzionare e le repliche saranno in sospeso fino all'aggiornamento dei certificati.

Fasi

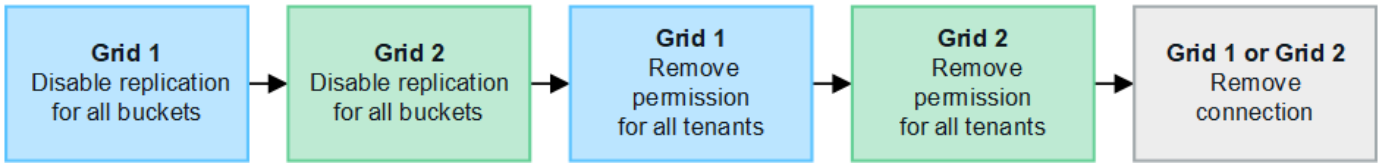
1. Accedere a Grid Manager dal nodo di amministrazione principale su una griglia.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Da una delle schede della pagina Grid Federation, selezionare il nome della connessione per visualizzarne i dettagli.

4. Selezionare la scheda **certificati**.
5. Selezionare **ruota certificati**.
6. Specificare il numero di giorni in cui i nuovi certificati devono essere validi.
7. Inserire la passphrase di provisioning per la griglia a cui si è connessi.
8. Selezionare **ruota certificati**.
9. Se necessario, ripetere questi passaggi sull'altra griglia della connessione.

   In generale, utilizzare lo stesso numero di giorni per i certificati su entrambi i lati della connessione.

Rimuovi una connessione a federazione di griglie

È possibile rimuovere una connessione a federazione di griglia da una delle griglie della connessione. Come illustrato nella figura, è necessario eseguire i passaggi necessari su entrambe le griglie per confermare che la connessione non viene utilizzata da alcun tenant su nessuna griglia.



Prima di rimuovere una connessione, tenere presente quanto segue:

- La rimozione di una connessione non elimina gli elementi già copiati tra le griglie. Ad esempio, gli utenti, i gruppi e gli oggetti del tenant presenti in entrambe le griglie non vengono cancellati da nessuna griglia quando viene rimossa l'autorizzazione del tenant. Se si desidera eliminare questi elementi, è necessario eliminarli manualmente da entrambe le griglie.
- Quando si rimuove una connessione, la replica di tutti gli oggetti in sospeso (acquisiti ma non ancora replicati nell'altra griglia) avrà esito negativo in modo permanente.

Disattiva la replica per tutti i bucket del tenant

Fasi

1. Partendo da una griglia, accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare il nome della connessione per visualizzarne i dettagli.
4. Nella scheda **tenant consentiti**, determinare se la connessione viene utilizzata da qualsiasi tenant.
5. Se sono elencati dei tenant, chiedere a tutti i tenant di "disattiva la replica cross-grid" per tutti i bucket su entrambe le griglie della connessione.

> Non è possibile rimuovere l'autorizzazione **use grid Federation Connection** (Usa connessione federazione griglia) se alcuni bucket tenant hanno attivato la replica cross-grid. Ciascun account tenant deve disattivare la replica cross-grid per i bucket su entrambe le griglie.

Rimuovere i permessi per ciascun tenant

Una volta disattivata la replica cross-grid per tutti i bucket del tenant, rimuovere l'autorizzazione **Usa federazione grid** da tutti i tenant su entrambe le grid.

Fasi

1. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
2. Selezionare il nome della connessione per visualizzarne i dettagli.
3. Per ciascun tenant nella scheda **tenant consentiti**, rimuovere l'autorizzazione **Usa connessione federazione griglia** da ciascun tenant. Vedere "Gestire i tenant autorizzati".
4. Ripetere questi passaggi per i tenant consentiti sull'altra griglia.

Rimuovere la connessione

Fasi

1. Se nessun tenant su una griglia sta utilizzando la connessione, selezionare **Remove** (Rimuovi).
2. Controllare il messaggio di conferma e selezionare **Rimuovi**.
   - Se è possibile rimuovere la connessione, viene visualizzato un messaggio di conferma. La connessione a federazione di griglie viene ora rimossa da entrambe le griglie.
   - Se la connessione non può essere rimossa (ad esempio, è ancora in uso o si è verificato un errore di connessione), viene visualizzato un messaggio di errore. È possibile effettuare una delle seguenti operazioni:
     - Risolvere l'errore (consigliato). Vedere "Risolvere i problemi relativi agli errori di federazione della griglia".
     - Rimuovere la connessione con la forza. Vedere la sezione successiva.

Rimuovi una connessione a federazione di griglie con la forza

Se necessario, è possibile forzare la rimozione di una connessione che non ha lo stato **Connected**.

La rimozione forzata elimina solo la connessione dalla griglia locale. Per rimuovere completamente la connessione, eseguire le stesse operazioni su entrambe le griglie.

Fasi

1. Dalla finestra di dialogo di conferma, selezionare **Force remove** (forza rimozione).

   Viene visualizzato un messaggio di successo. Questa connessione a federazione di griglie non può più essere utilizzata. Tuttavia, i bucket tenant potrebbero avere ancora la replica cross-grid attivata e alcune copie degli oggetti potrebbero essere già state replicate tra le griglie della connessione.

2. Dall'altra griglia della connessione, accedere a Grid Manager dal nodo di amministrazione primario.
3. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
4. Selezionare il nome della connessione per visualizzarne i dettagli.
5. Selezionare **Rimuovi** e **Sì**.
6. Selezionare **forza rimozione** per rimuovere la connessione da questa griglia.

Gestire i tenant consentiti per la federazione di grid

È possibile consentire agli account tenant S3 di utilizzare una connessione di federazione di griglie tra due sistemi StorageGRID. Quando ai tenant viene consentito di utilizzare una connessione, sono necessari passaggi speciali per modificare i dettagli del tenant o per rimuovere in modo permanente l'autorizzazione di un tenant a utilizzare la

connessione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su una delle griglie utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root" per la griglia a cui si è effettuato l'accesso.
- Lo hai fatto "creazione di una connessione a federazione di griglie" tra due griglie.
- Hai esaminato i flussi di lavoro per "clone dell'account" e. "replica cross-grid".
- Come richiesto, è già stato configurato il Single Sign-on (SSO) o l'identificazione della federazione per entrambe le griglie della connessione. Vedere "Cos'è il clone dell'account".

Creare un tenant consentito

Se si desidera consentire a un account tenant nuovo o esistente di utilizzare una connessione di federazione griglia per la clonazione dell'account e la replica cross-grid, seguire le istruzioni generali riportate a. "Creare un nuovo tenant S3" oppure "modificare un account tenant" e prendere nota di quanto segue:

- È possibile creare il tenant da una griglia della connessione. La griglia in cui viene creato un tenant è la griglia di origine del *tenant*.
- Lo stato della connessione deve essere **connesso**.
- Quando il tenant viene creato o modificato per attivare l'autorizzazione **Usa connessione federazione griglia** e quindi salvato nella prima griglia, un tenant identico viene replicato automaticamente nell'altra griglia. La griglia in cui viene replicato il tenant è la griglia di destinazione del *tenant*.
- I tenant di entrambe le griglie avranno lo stesso ID account a 20 cifre, il nome, la descrizione, la quota e le autorizzazioni. In alternativa, è possibile utilizzare il campo **Description** per identificare il tenant di origine e il tenant di destinazione. Ad esempio, questa descrizione per un tenant creato sulla griglia 1 verrà visualizzata anche per il tenant replicato sulla griglia 2: "Questo tenant è stato creato sulla griglia 1".
- Per motivi di sicurezza, la password di un utente root locale non viene copiata nella griglia di destinazione.

> Prima che un utente root locale possa accedere al tenant replicato sulla griglia di destinazione, un amministratore della griglia deve "modificare la password per l'utente root locale".

- Una volta che il tenant nuovo o modificato è disponibile su entrambi i grid, gli utenti tenant possono eseguire queste operazioni:
  - Dalla griglia di origine del tenant, creare gruppi e utenti locali, che vengono clonati automaticamente nella griglia di destinazione del tenant. Vedere "Clonare utenti e gruppi tenant".
  - Creare nuove chiavi di accesso S3, che possono essere eventualmente clonate nella griglia di destinazione del tenant. Vedere "Clonare le chiavi di accesso S3 utilizzando l'API".
  - Creare bucket identici su entrambe le griglie della connessione e abilitare la replica cross-grid in una direzione o in entrambe le direzioni. Vedere "Gestire la replica cross-grid".

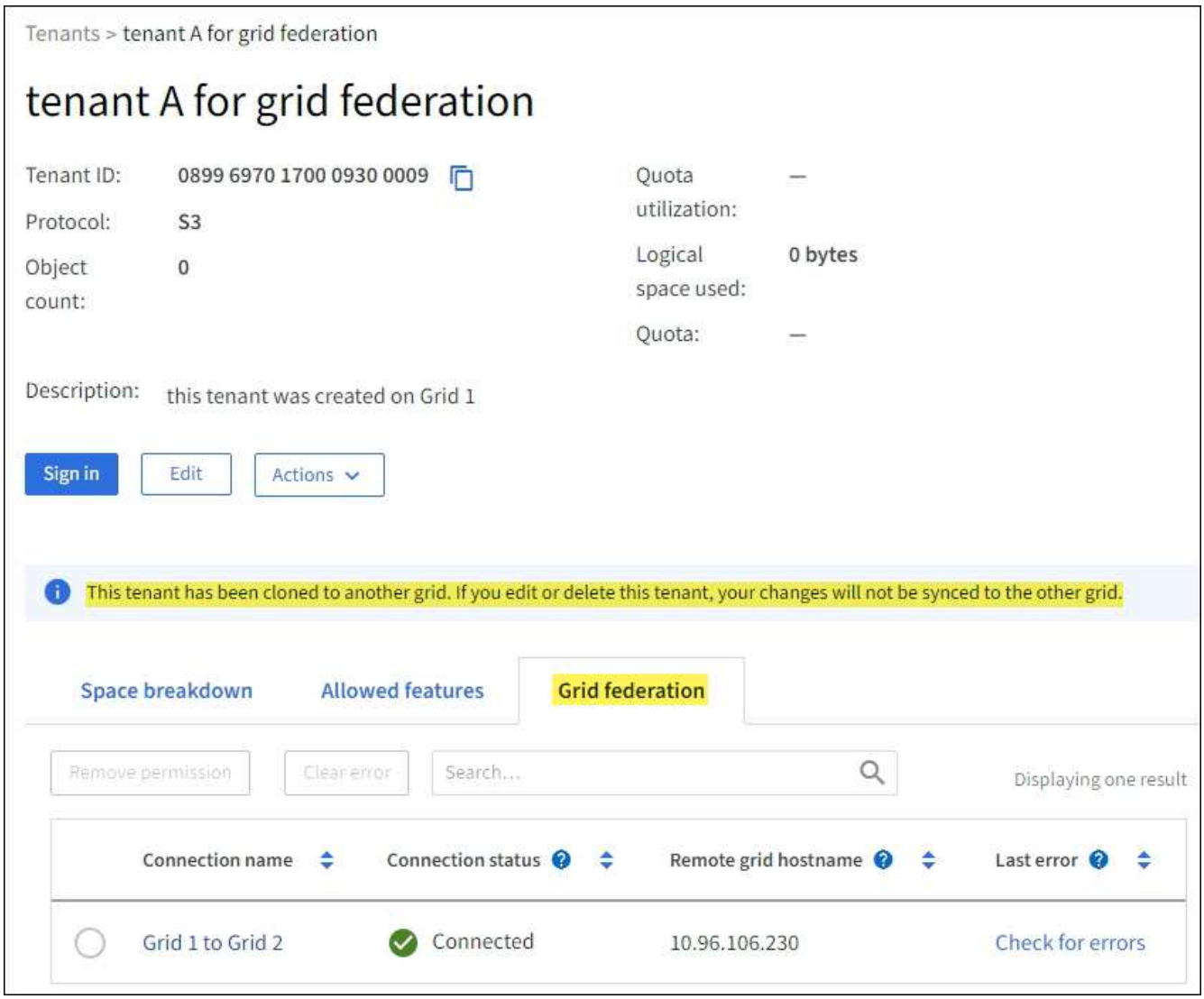
Visualizzare un tenant consentito

È possibile visualizzare i dettagli di un tenant autorizzato a utilizzare una connessione a federazione di griglie.

Fasi

1. Selezionare **TENANT**.
2. Dalla pagina tenant, selezionare il nome del tenant per visualizzare la pagina dei dettagli del tenant.

Se si tratta della griglia di origine del tenant (ovvero, se il tenant è stato creato in questa griglia), viene visualizzato un banner per ricordare che il tenant è stato clonato in un'altra griglia. Se modifichi o elimini questo tenant, le modifiche non verranno sincronizzate con l'altra griglia.



3. Se si desidera, selezionare la scheda **Grid Federation** in "monitorare la connessione alla federazione di griglie".

Modificare un tenant consentito

Se è necessario modificare un tenant con l'autorizzazione **Usa connessione federazione griglia**, seguire le istruzioni generali per "modifica di un account tenant" e prendere nota di quanto segue:

- Se un tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile modificare i dettagli del tenant da una delle griglie della connessione. Tuttavia, qualsiasi modifica apportata non verrà copiata nell'altra griglia. Se si desidera mantenere sincronizzati i dettagli del tenant tra le griglie, è necessario apportare le stesse modifiche su entrambe.
- Non è possibile cancellare l'autorizzazione **Usa connessione federazione griglia** quando si modifica un tenant.
- Non è possibile selezionare una connessione a federazione di griglie diversa quando si modifica un tenant.

Eliminare un tenant consentito

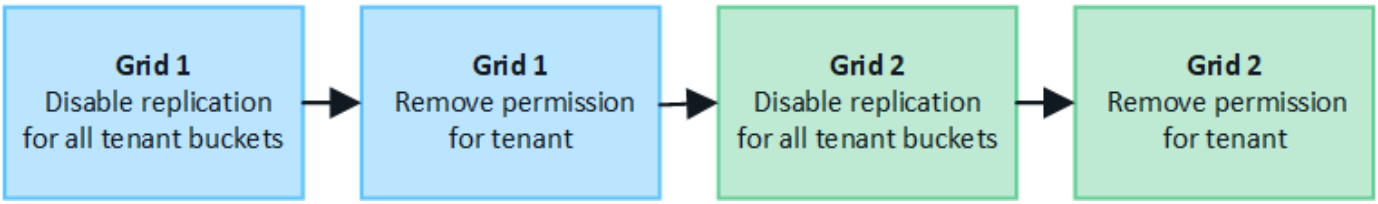
Se è necessario rimuovere un tenant con l'autorizzazione **Usa connessione federazione griglia**, seguire le istruzioni generali per "eliminazione di un account tenant" e prendere nota di quanto segue:

- Prima di rimuovere il tenant originale dalla griglia di origine, è necessario rimuovere tutti i bucket dell'account sulla griglia di origine.
- Prima di poter rimuovere il tenant clonato nella griglia di destinazione, è necessario rimuovere tutti i bucket dell'account nella griglia di destinazione.
- Se si rimuove il tenant originale o clonato, l'account non può più essere utilizzato per la replica cross-grid.
- Se si rimuove il tenant originale dalla griglia di origine, i gruppi di tenant, gli utenti o le chiavi clonati nella griglia di destinazione non verranno influenzati. È possibile eliminare il tenant clonato o consentirne la gestione di gruppi, utenti, chiavi di accesso e bucket.
- Se si rimuove il tenant clonato nella griglia di destinazione, si verificano errori di clonazione se vengono aggiunti nuovi gruppi o utenti al tenant originale.

  Per evitare questi errori, rimuovere l'autorizzazione del tenant per utilizzare la connessione di federazione della griglia prima di eliminare il tenant da questa griglia.

Rimuovi l'autorizzazione Usa connessione federazione griglia

Per impedire a un tenant di utilizzare una connessione a federazione di griglie, è necessario rimuovere l'autorizzazione **Usa connessione a federazione di griglie**.



Prima di rimuovere l'autorizzazione di un tenant a utilizzare una connessione a federazione di griglie, tenere presente quanto segue:

- Non è possibile rimuovere l'autorizzazione **Usa connessione federazione griglia** se uno dei bucket del tenant ha attivato la replica cross-grid. L'account tenant deve prima disattivare la replica cross-grid per tutti i bucket.
- La rimozione dell'autorizzazione **Usa connessione federazione griglia** non elimina gli elementi che sono già stati replicati tra le griglie. Ad esempio, gli utenti, i gruppi e gli oggetti del tenant presenti in entrambe le griglie non vengono cancellati da nessuna griglia quando viene rimossa l'autorizzazione del tenant. Se si desidera eliminare questi elementi, è necessario eliminarli manualmente da entrambe le griglie.
- Se si desidera riattivare questa autorizzazione con la stessa connessione di federazione della griglia, eliminare prima questo tenant sulla griglia di destinazione; in caso contrario, riabilitare questa autorizzazione causerà un errore.

> Riattivando l'autorizzazione **Use grid Federation Connection**, la griglia locale diventa la griglia di origine e attiva la clonazione alla griglia remota specificata dalla connessione di federazione della griglia selezionata. Se l'account tenant è già presente nella griglia remota, la clonazione causerà un errore di conflitto.

Prima di iniziare

- Si sta utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root" per entrambe le griglie.

Disattiva la replica per i bucket tenant

Come primo passo, disattivare la replica cross-grid per tutti i bucket del tenant.

Fasi

1. Partendo da una griglia, accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare il nome della connessione per visualizzarne i dettagli.
4. Nella scheda **tenant consentiti**, determinare se il tenant sta utilizzando la connessione.
5. Se il tenant è presente nell'elenco, chiedere al tenant di farlo "disattiva la replica cross-grid" per tutti i bucket su entrambe le griglie della connessione.

> Non è possibile rimuovere l'autorizzazione **use grid Federation Connection** (Usa connessione federazione griglia) se alcuni bucket tenant hanno attivato la replica cross-grid. Il tenant deve disattivare la replica cross-grid per i bucket su entrambe le griglie.

Rimuovere l'autorizzazione per il tenant

Una volta disattivata la replica cross-grid per i bucket tenant, è possibile rimuovere il permesso del tenant per utilizzare la connessione di federazione grid.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Rimuovere l'autorizzazione dalla pagina Grid Federation o dalla pagina tenant.

Pagina Grid Federation

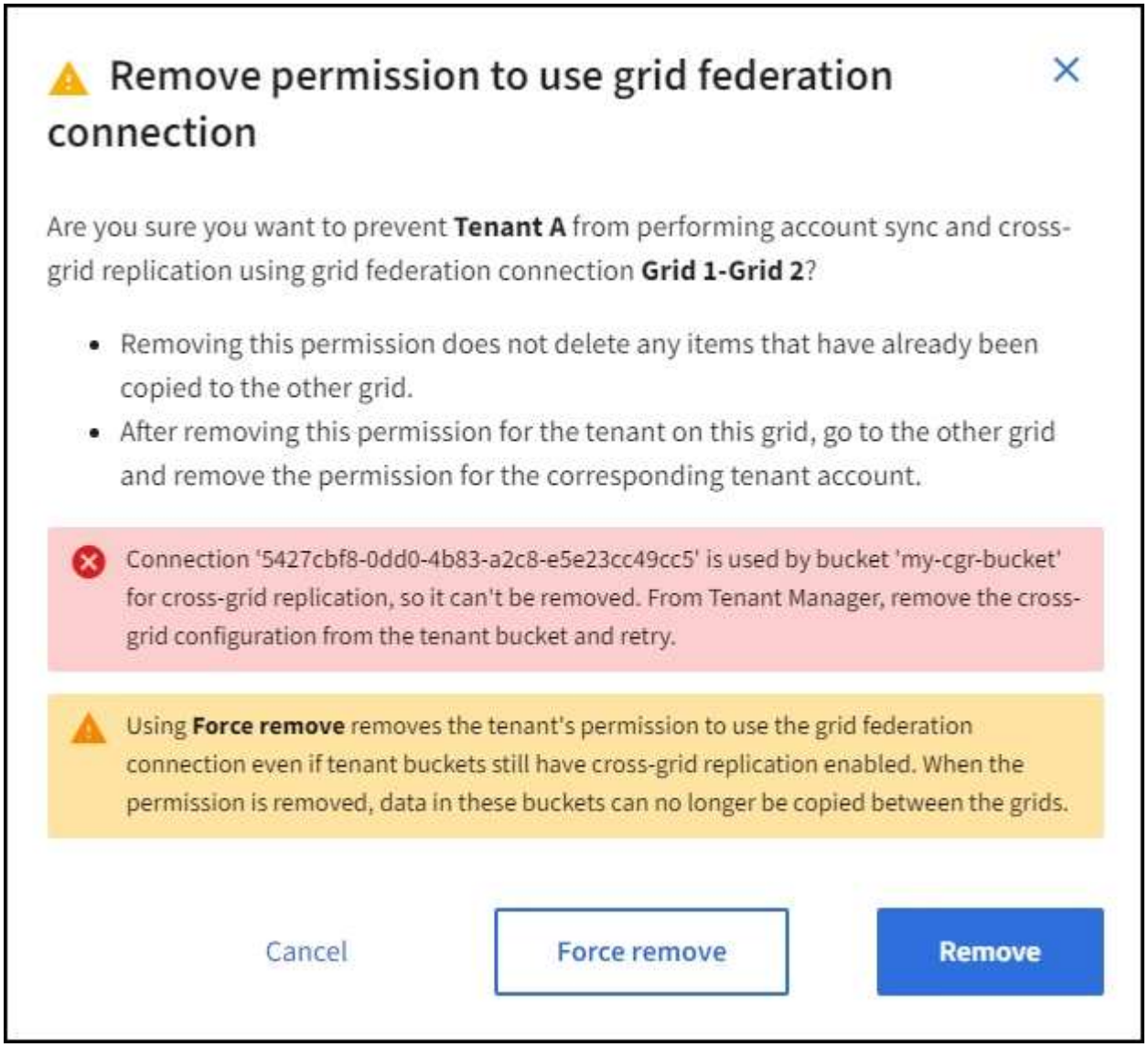
a. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
b. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
c. Nella scheda **tenant consentiti**, selezionare il pulsante di opzione corrispondente al tenant.
d. Selezionare **Rimuovi permesso**.

Pagina tenant

a. Selezionare **TENANT**.
b. Selezionare il nome del tenant per visualizzare la pagina dei dettagli.
c. Nella scheda **Grid Federation**, selezionare il pulsante di opzione per la connessione.
d. Selezionare **Rimuovi permesso**.

3. Esaminare gli avvisi nella finestra di dialogo di conferma e selezionare **Rimuovi**.
   - Se l'autorizzazione può essere rimossa, viene visualizzata nuovamente la pagina dei dettagli e viene visualizzato un messaggio di conferma. Questo tenant non può più utilizzare la connessione a federazione di grid.

◦ Se in uno o più bucket tenant è ancora attivata la replica cross-grid, viene visualizzato un errore.



È possibile effettuare una delle seguenti operazioni:

- (Consigliato). Accedere a Tenant Manager e disattivare la replica per ciascuno dei bucket del tenant. Vedere "Gestire la replica cross-grid". Quindi, ripetere la procedura per rimuovere l'autorizzazione **Usa connessione alla rete**.
- Rimuovere l'autorizzazione forzatamente. Vedere la sezione successiva.

4. Passare all'altra griglia e ripetere questa procedura per rimuovere l'autorizzazione per lo stesso tenant sull'altra griglia.

Rimuovi l'autorizzazione in base alla forza

Se necessario, è possibile forzare la rimozione dell'autorizzazione di un tenant per utilizzare una connessione a federazione di griglia anche se i bucket tenant hanno la replica cross-grid attivata.

Prima di rimuovere il permesso di un tenant per forza, prendere nota delle considerazioni generali per rimozione dell'autorizzazione oltre a queste considerazioni aggiuntive:

- Se si rimuove l'autorizzazione **Usa connessione federazione griglia** per forza, tutti gli oggetti che sono in

attesa di replica nell'altra griglia (acquisiti ma non ancora replicati) continueranno a essere replicati. Per evitare che questi oggetti in-process raggiungano il bucket di destinazione, è necessario rimuovere anche l'autorizzazione del tenant sull'altra griglia.

- Qualsiasi oggetto acquisito nel bucket di origine dopo la rimozione dell'autorizzazione **Usa connessione federazione griglia** non verrà mai replicato nel bucket di destinazione.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
4. Nella scheda **tenant consentiti**, selezionare il pulsante di opzione corrispondente al tenant.
5. Selezionare **Rimuovi permesso**.
6. Rivedere gli avvisi nella finestra di dialogo di conferma e selezionare **forza rimozione**.

   Viene visualizzato un messaggio di successo. Questo tenant non può più utilizzare la connessione a federazione di grid.

7. Se necessario, passare all'altra griglia e ripetere questa procedura per forzare la rimozione dell'autorizzazione per lo stesso account tenant sull'altra griglia. Ad esempio, è necessario ripetere questi passaggi sull'altra griglia per evitare che gli oggetti in-process raggiungano il bucket di destinazione.

Risolvere i problemi relativi agli errori di federazione della griglia

Potrebbe essere necessario risolvere gli avvisi e gli errori relativi alle connessioni di federazione di griglie, al clone dell'account e alla replica cross-grid.

Avvisi ed errori di connessione a Grid Federation

È possibile che si ricevano avvisi o si verifichino errori con le connessioni della federazione di griglie.

Dopo aver apportato qualsiasi modifica per risolvere un problema di connessione, verificare che lo stato della connessione torni a **connesso**. Per istruzioni, vedere "Gestire le connessioni a federazione di griglie".

Avviso di errore di connessione della federazione di griglie

Problema

È stato attivato l'avviso **errore di connessione federazione griglia**.

Dettagli

Questo avviso indica che la connessione a federazione di griglie tra le griglie non funziona.

Azioni consigliate

1. Esaminare le impostazioni della pagina Grid Federation per entrambe le griglie. Verificare che tutti i valori siano corretti. Vedere "Gestire le connessioni a federazione di griglie".
2. Esaminare i certificati utilizzati per la connessione. Assicurarsi che non ci siano avvisi per i certificati di federazione griglia scaduti e che i dettagli di ciascun certificato siano validi. Consultare le istruzioni per la rotazione dei certificati di connessione in "Gestire le connessioni a federazione di griglie".
3. Verificare che tutti i nodi Admin e Gateway in entrambe le griglie siano online e disponibili. Risolvere eventuali avvisi che potrebbero interessare questi nodi e riprovare.

4. Se è stato fornito un nome di dominio completo (FQDN) per la griglia locale o remota, verificare che il server DNS sia in linea e disponibile. Vedere "Che cos'è la federazione di griglie?" Per i requisiti di rete, indirizzo IP e DNS.

Scadenza dell'avviso del certificato di federazione griglia

Problema

È stato attivato l'avviso **scadenza del certificato federazione griglia**.

Dettagli

Questo avviso indica che uno o più certificati di federazione griglia stanno per scadere.

Azioni consigliate

Consultare le istruzioni per la rotazione dei certificati di connessione in "Gestire le connessioni a federazione di griglie".

Errore durante la modifica di una connessione a federazione di griglie

Problema

Quando si modifica una connessione a federazione di griglie, viene visualizzato il seguente messaggio di avviso quando si seleziona **Salva e test**: "Impossibile creare un file di configurazione candidato su uno o più nodi."

Dettagli

Quando si modifica una connessione a federazione di griglie, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi di amministrazione della prima griglia. Viene visualizzato un messaggio di avviso se il file non può essere salvato in tutti i nodi di amministrazione, ad esempio perché un nodo di amministrazione non è in linea.

Azioni consigliate

1. Dalla griglia utilizzata per modificare la connessione, selezionare **NODES** (NODI).
2. Verificare che tutti i nodi Admin per la griglia siano in linea.
3. Se alcuni nodi sono offline, ripristinarli online e provare a modificare nuovamente la connessione.

Errori di cloni dell'account

Impossibile accedere a un account tenant clonato

Problema

Impossibile accedere a un account tenant clonato. Il messaggio di errore nella pagina di accesso di Tenant Manager è "le credenziali per questo account non sono valide. Riprovare."

Dettagli

Per motivi di sicurezza, quando un account tenant viene clonato dalla griglia di origine del tenant alla griglia di destinazione del tenant, la password impostata per l'utente root locale del tenant non viene clonata. Allo stesso modo, quando un tenant crea utenti locali sulla griglia di origine, le password utente locali non vengono clonate nella griglia di destinazione.

Azioni consigliate

Prima che l'utente root possa accedere alla griglia di destinazione del tenant, un amministratore della griglia deve prima "modificare la password per l'utente root locale" sulla griglia di destinazione.

Prima che un utente locale clonato possa accedere alla griglia di destinazione del tenant, l'utente root del tenant clonato deve aggiungere una password per l'utente nella griglia di destinazione. Per istruzioni, vedere "Gestire gli utenti locali" Nelle istruzioni per l'utilizzo di Tenant Manager.

Tenant creato senza un clone

Problema

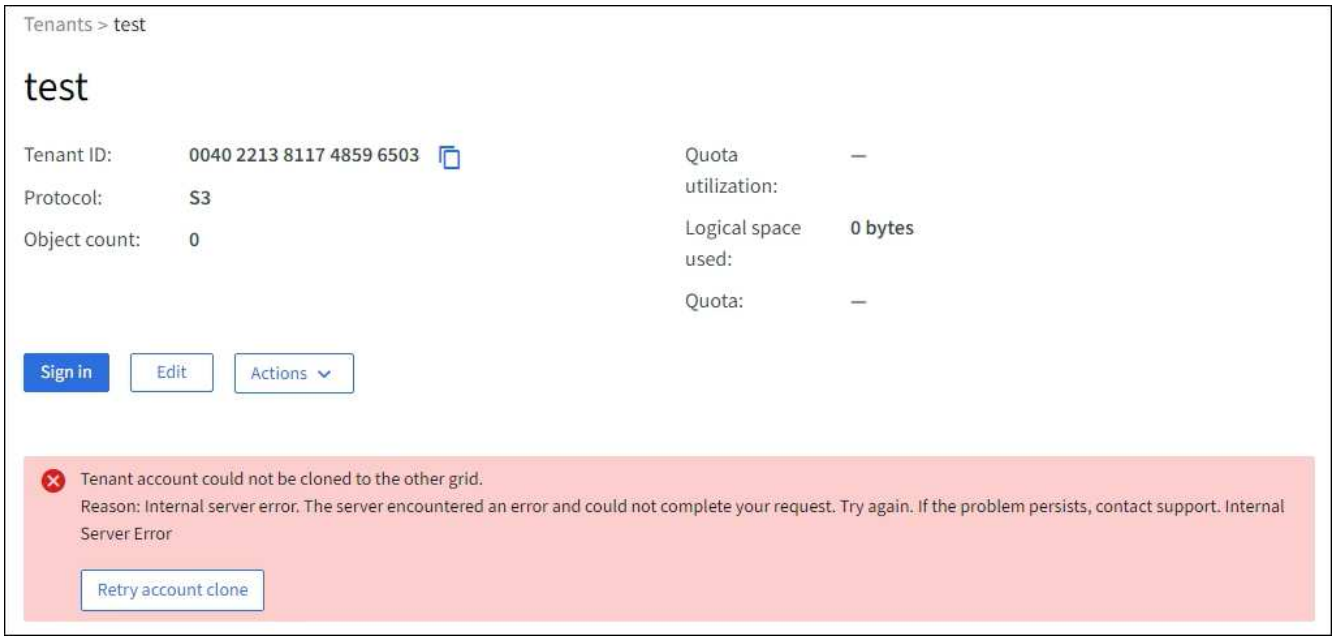
Viene visualizzato il messaggio "tenant creato senza clone" dopo aver creato un nuovo tenant con l'autorizzazione **Usa connessione federazione griglia**.

Dettagli

Questo problema può verificarsi se gli aggiornamenti allo stato della connessione vengono posticipati, causando l'elenco di una connessione non funzionante come **connessa**.

Azioni consigliate

1. Esaminare i motivi elencati nel messaggio di errore e risolvere eventuali problemi di rete o di altro tipo che potrebbero impedire il funzionamento della connessione. Vedere Avvisi ed errori di connessione Grid Federation.
2. Seguire le istruzioni per verificare la connessione a una federazione di griglie in "Gestire le connessioni a federazione di griglie" per confermare che il problema è stato risolto.
3. Dalla griglia di origine del tenant, selezionare **TENANT**.
4. Individuare l'account tenant che non è stato clonato.
5. Selezionare il nome del tenant per visualizzare la pagina dei dettagli.
6. Selezionare **Retry account clone**.



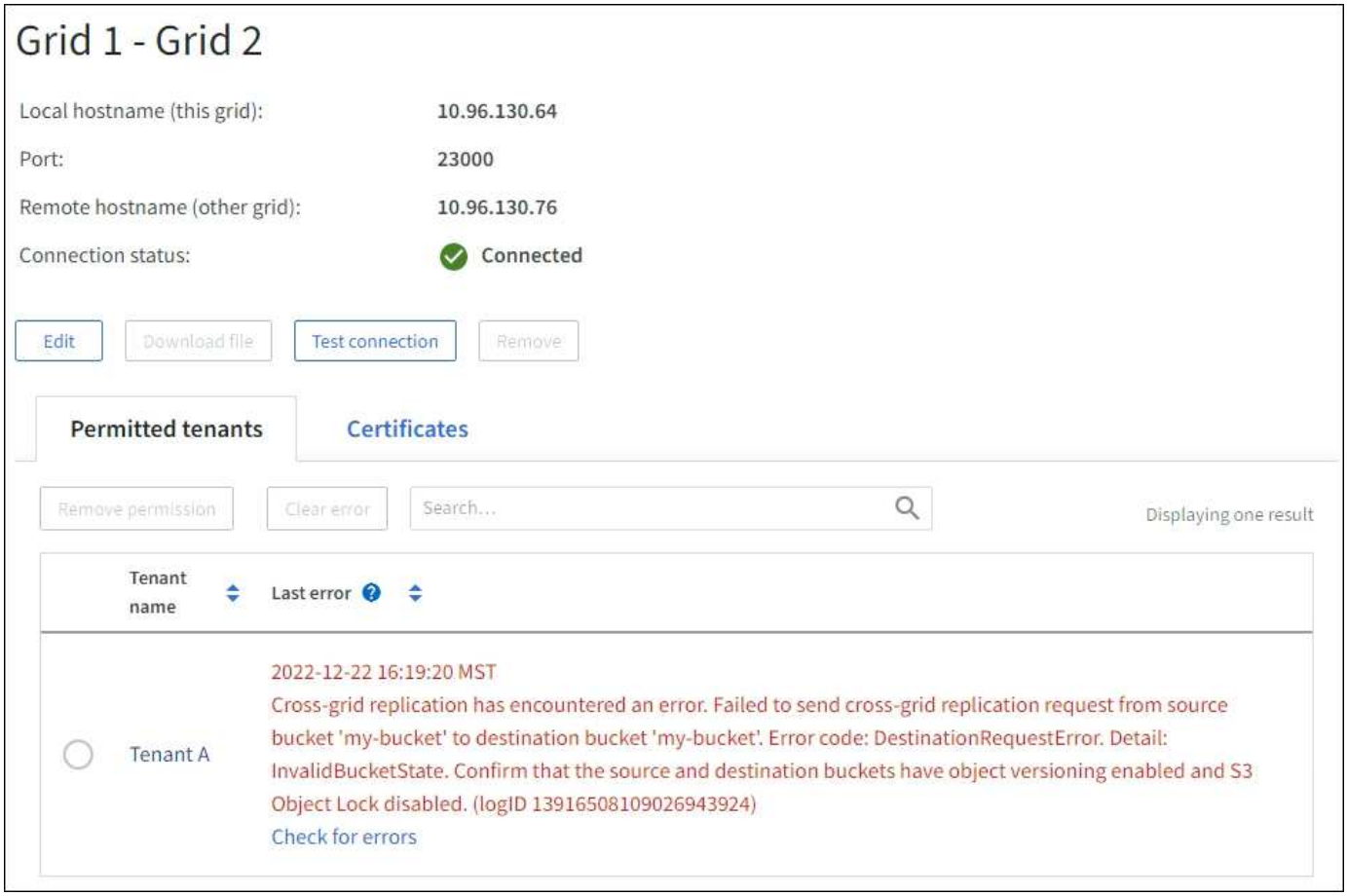
Se l'errore è stato risolto, l'account tenant verrà clonato nell'altra griglia.

Avvisi ed errori di replica cross-grid

Viene visualizzato l'ultimo errore per la connessione o il tenant

Problema

Quando "visualizzazione di una connessione a federazione di griglie" (o quando "gestione dei tenant consentiti" Per una connessione), si verifica un errore nella colonna **ultimo errore** della pagina dei dettagli di connessione. Ad esempio:



Dettagli

Per ogni connessione a federazione di griglie, la colonna **ultimo errore** mostra l'errore più recente che si verifica, se presente, quando i dati di un tenant venivano replicati nell'altro grid. In questa colonna viene visualizzato solo l'ultimo errore di replica tra griglie; gli errori precedenti che potrebbero essere stati rilevati non verranno visualizzati.
In questa colonna potrebbe verificarsi un errore per uno dei seguenti motivi:

- Versione dell'oggetto di origine non trovata.
- Bucket di origine non trovato.
- Il bucket di destinazione è stato cancellato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il bucket di destinazione ha la versione sospesa.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più disponibile.

Azioni consigliate

Se nella colonna **ultimo errore** viene visualizzato un messaggio di errore, attenersi alla seguente procedura:

1. Rivedere il testo del messaggio.
2. Eseguire le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso nel bucket di destinazione per la replica cross-grid, riabilitare il controllo delle versioni per quel bucket.

3. Selezionare la connessione o l'account tenant dalla tabella.
4. Selezionare **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.

   Per assicurarsi che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo l'indicazione dell'ora nel messaggio prima di acquisire un nuovo oggetto.

   Dopo aver corretto l'errore, potrebbe essere visualizzato un nuovo **ultimo errore** se gli oggetti vengono acquisiti in un bucket diverso che presenta anche un errore.

7. Per determinare se non è stato possibile replicare oggetti a causa dell'errore del bucket, vedere "Identificare e riprovare le operazioni di replica non riuscite".

Avviso di errore permanente della replica cross-grid

Problema

È stato attivato l'avviso **errore permanente replica cross-grid**.

Dettagli

Questo avviso indica che gli oggetti tenant non possono essere replicati tra i bucket su due griglie per un motivo che richiede l'intervento dell'utente per la risoluzione. Questo avviso è generalmente causato da una modifica al bucket di origine o di destinazione.

Azioni consigliate

1. Accedere alla griglia in cui è stato attivato l'avviso.
2. Accedere a **CONFIGURATION** > **System** > **Grid Federation** e individuare il nome della connessione elencato nell'avviso.
3. Nella scheda Permitted tenant (tenant consentiti), esaminare la colonna **Last error** (ultimo errore) per determinare quali account tenant presentano errori.
4. Per ulteriori informazioni sull'errore, consultare le istruzioni in "Monitorare le connessioni a federazione di griglie" per rivedere le metriche di replica cross-grid.
5. Per ciascun account tenant interessato:
   a. Consultare le istruzioni in "Monitorare l'attività del tenant" per confermare che il tenant non ha superato la quota sulla griglia di destinazione per la replica cross-grid.
   b. Se necessario, aumentare la quota del tenant sulla griglia di destinazione per consentire il salvataggio di nuovi oggetti.
6. Per ogni tenant interessato, accedi a tenant Manager su entrambe le griglie, in modo da poter confrontare l'elenco dei bucket.
7. Per ogni bucket con replica cross-grid attivata, confermare quanto segue:
   - Esiste un bucket corrispondente per lo stesso tenant sull'altra griglia (deve utilizzare il nome esatto).
   - Entrambi i bucket hanno attivato la versione degli oggetti (la versione non può essere sospesa su nessuna griglia).
   - Entrambi i bucket hanno S3 Object Lock disattivato.

- Nessuno dei due bucket si trova nello stato **Deleting Objects: Read-only**.

8. Per confermare che il problema è stato risolto, consultare le istruzioni in "Monitorare le connessioni a federazione di griglie" per rivedere le metriche di replica cross-grid o eseguire questi passaggi:

   a. Torna alla pagina Grid Federation.
   b. Selezionare il tenant interessato e selezionare **Cancella errore** nella colonna **ultimo errore**.
   c. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
   d. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.

   > Per assicurarsi che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo l'indicazione dell'ora nel messaggio prima di acquisire un nuovo oggetto.

   > Una volta risolto, l'avviso potrebbe richiedere fino a un giorno.

   a. Passare a. "Identificare e riprovare le operazioni di replica non riuscite" per identificare gli oggetti o eliminare i marcatori che non sono riusciti a replicare nell'altra griglia e riprovare la replica secondo necessità.

Avviso di risorsa di replica cross-grid non disponibile

Problema

È stato attivato l'avviso **risorsa di replica cross-grid non disponibile**.

Dettagli

Questo avviso indica che le richieste di replica cross-grid sono in sospeso perché una risorsa non è disponibile. Ad esempio, potrebbe essere presente un errore di rete.

Azioni consigliate

1. Monitorare l'avviso per verificare se il problema si risolve da solo.
2. Se il problema persiste, determinare se una griglia presenta un avviso di errore di connessione * federazione griglia per la stessa connessione o un avviso di errore di comunicazione * con nodo * per un nodo. Questo avviso potrebbe essere risolto quando si risolvono tali avvisi.
3. Per ulteriori informazioni sull'errore, consultare le istruzioni in "Monitorare le connessioni a federazione di griglie" per rivedere le metriche di replica cross-grid.
4. Se non riesci a risolvere l'avviso, contatta il supporto tecnico.

La replica cross-grid procederà normalmente dopo la risoluzione del problema.

Identificare e riprovare le operazioni di replica non riuscite

Dopo aver risolto l'avviso **errore permanente replica cross-grid**, è necessario determinare se non è stato possibile replicare oggetti o marker di eliminazione nell'altra griglia. È quindi possibile recuperare questi oggetti o utilizzare l'API Grid Management per riprovare la replica.

L'avviso **errore permanente di replica cross-grid** indica che gli oggetti tenant non possono essere replicati tra i bucket su due griglie per un motivo che richiede l'intervento dell'utente per la risoluzione. Questo avviso è generalmente causato da una modifica al bucket di origine o di destinazione. Per ulteriori informazioni, vedere

"Risolvere i problemi relativi agli errori di federazione della griglia".

Determinare se non è stato possibile replicare oggetti

Per determinare se gli oggetti o i marker di eliminazione non sono stati replicati nell'altra griglia, è possibile eseguire una ricerca nel registro di controllo "CGRR (Cross-Grid Replication Request)" messaggi. Questo messaggio viene aggiunto al registro quando StorageGRID non riesce a replicare un oggetto, un oggetto multiparte o un indicatore di eliminazione nel bucket di destinazione.

È possibile utilizzare "tool di verifica-spiegazione" per tradurre i risultati in un formato più facile da leggere.

Prima di iniziare

- Si dispone dell'autorizzazione di accesso root.
- Hai il `Passwords.txt` file.
- Si conosce l'indirizzo IP del nodo di amministrazione primario.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Cercare i messaggi CGRR in audit.log e utilizzare lo strumento di spiegazione dell'audit per formattare i risultati.

   Ad esempio, questo comando si grep per tutti i messaggi CGRR negli ultimi 30 minuti e utilizza lo strumento audit-exclaring.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

Il risultato del comando sarà simile a questo esempio, che contiene voci per sei messaggi CGRR. Nell'esempio, tutte le richieste di replica cross-grid hanno restituito un errore generale perché non è stato possibile replicare l'oggetto. I primi tre errori riguardano le operazioni "Replicate Object", mentre gli ultimi tre errori riguardano le operazioni "Replicate delete marker".

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Ciascuna voce contiene le seguenti informazioni:

Campo	Descrizione
Richiesta di replica CGRR Cross-Grid	Il nome della richiesta
tenant	ID account del tenant
connessione	L'ID della connessione a federazione di griglie
operazione	Il tipo di operazione di replica che si stava tentando di eseguire: • oggetto replicate • marker di eliminazione replicato • replica di un oggetto multiparte
bucket	Il nome del bucket
oggetto	Il nome dell'oggetto
versione	L'ID versione dell'oggetto

Campo	Descrizione
errore	Il tipo di errore. Se la replica cross-grid non riesce, l'errore è "General error" (errore generale).

Riprovare a eseguire repliche non riuscite

Dopo aver generato un elenco di oggetti e marker di eliminazione che non sono stati replicati nel bucket di destinazione e aver risolto i problemi sottostanti, è possibile riprovare la replica in due modi:

- Inserire ciascun oggetto nel bucket di origine.
- Utilizzare l'API privata Grid Management, come descritto.

Fasi

1. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.
2. Selezionare **Vai alla documentazione API privata**.

   > Gli endpoint dell'API StorageGRID contrassegnati come "privati" sono soggetti a modifica senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

3. Nella sezione **cross-grid-Replication-Advanced**, selezionare il seguente endpoint:

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Selezionare **Provalo**.
5. Nella casella di testo **body**, sostituire la voce di esempio per **versionID** con un ID di versione di audit.log che corrisponde a una richiesta di replica cross-grid non riuscita.

   Assicurarsi di conservare le virgolette doppie intorno alla stringa.

6. Selezionare **Esegui**.
7. Verificare che il codice di risposta del server sia **204**, a indicare che l'oggetto o il marker di eliminazione è stato contrassegnato come in sospeso per la replica cross-grid sull'altra griglia.

   > In sospeso indica che la richiesta di replica cross-grid è stata aggiunta alla coda interna per l'elaborazione.

Monitorare i tentativi di replica

È necessario monitorare le operazioni di ripetizione della replica per assicurarsi che vengano completate.

> La replica di un oggetto o di un marker di eliminazione nell'altra griglia potrebbe richiedere diverse ore o più.

È possibile monitorare le operazioni di ripetizione in due modi:

- Utilizzare un S3 "HeadObject (oggetto intestazione)" oppure "GetObject" richiesta. La risposta include lo specifico StorageGRID `x-ntap-sg-cgr-replication-status` intestazione della risposta, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• **SUCCESSO**: La replica è riuscita. • **PENDING**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

- Utilizzare l'API privata Grid Management, come descritto.

Fasi

1. Nella sezione **cross-grid-Replication-Advanced** della documentazione dell'API privata, selezionare il seguente endpoint:

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. Selezionare **Provalo**.
3. Nella sezione Parameter (parametro), inserire l'ID versione utilizzato in `cross-grid-replication-retry-failed` richiesta.
4. Selezionare **Esegui**.
5. Verificare che il codice di risposta del server sia **200**.
6. Esaminare lo stato della replica, che sarà uno dei seguenti:
   - **PENDING**: L'oggetto non è stato ancora replicato.
   - **COMPLETATO**: La replica è riuscita.
   - **FAILED**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.

Gestire la sicurezza

Gestione della sicurezza: Panoramica

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

Gestire la crittografia

StorageGRID offre diverse opzioni per la crittografia dei dati. Dovresti "esaminare i metodi di crittografia disponibili" per determinare quali soddisfano i tuoi requisiti di protezione dei dati.

Gestire i certificati

È possibile "configurare e gestire i certificati del server" Utilizzato per le connessioni HTTP o i certificati client utilizzati per autenticare un'identità client o utente nel server.

Configurare i server di gestione delle chiavi

Utilizzando un "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.

Gestire le impostazioni del proxy

Se si utilizzano i servizi della piattaforma S3 o i Cloud Storage Pool, è possibile configurare un "server proxy di archiviazione" Tra i nodi di storage e gli endpoint S3 esterni. Se si inviano pacchetti AutoSupport utilizzando HTTPS o HTTP, è possibile configurare un "admin proxy server (server proxy amministratore)" Tra nodi di amministrazione e supporto tecnico.

Firewall di controllo

Per migliorare la sicurezza del sistema, è possibile controllare l'accesso ai nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche in "firewall esterno". È inoltre possibile controllare l'accesso di rete a ciascun nodo configurandone l'accesso "firewall interno". È possibile impedire l'accesso a tutte le porte, ad eccezione di quelle necessarie per l'implementazione.

Esaminare i metodi di crittografia StorageGRID

StorageGRID offre diverse opzioni per la crittografia dei dati. È necessario esaminare i metodi disponibili per determinare quali metodi soddisfano i requisiti di protezione dei dati.

La tabella fornisce un riepilogo generale dei metodi di crittografia disponibili in StorageGRID.

Opzione di crittografia	Come funziona	Valido per
Server di gestione delle chiavi (KMS) in Grid Manager	Tu "configurare un server di gestione delle chiavi" Per il sito StorageGRID e. "abilitare la crittografia dei nodi per l'appliance". Quindi, un nodo appliance si connette al KMS per richiedere una chiave di crittografia a chiave (KEK). Questa chiave crittografa e decrta la chiave di crittografia dei dati (DEK) su ciascun volume.	Nodi appliance con **Node Encryption** attivato durante l'installazione. Tutti i dati dell'appliance sono protetti da perdite fisiche o rimozione dal data center. **Nota**: La gestione delle chiavi di crittografia con un KMS è supportata solo per i nodi di archiviazione e le appliance di servizi.

Opzione di crittografia	Come funziona	Valido per
Pagina crittografia unità nel programma di installazione dell'appliance StorageGRID	Se l'appliance contiene unità che supportano la crittografia hardware, è possibile impostare una passphrase dell'unità durante l'installazione. Quando si imposta una passphrase di unità, è impossibile per chiunque recuperare dati validi dalle unità rimosse dal sistema, a meno che non conoscano la passphrase. Prima di iniziare l'installazione, andare a **Configure hardware** > **Drive Encryption** per impostare una passphrase di unità che si applica a tutte le unità gestite da StorageGRID con crittografia automatica in un nodo.	Appliance che contengono dischi con crittografia automatica. Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. La crittografia dei dischi non si applica ai dischi gestiti da SANtricity. Se hai un'appliance storage con dischi a crittografia automatica e controller SANtricity, puoi abilitare la sicurezza dei dischi in SANtricity.
Protezione dei dischi in Gestione di sistema SANtricity	Se la funzione di protezione dell'unità è attivata per l'appliance StorageGRID, è possibile utilizzare "Gestore di sistema di SANtricity" per creare e gestire la chiave di protezione. La chiave è necessaria per accedere ai dati sui dischi protetti.	Appliance storage con dischi FDE (Full Disk Encryption) o dischi a crittografia automatica. Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. Non è utilizzabile con alcune appliance di storage o con alcuna appliance di servizi.
Crittografia degli oggetti memorizzati	Attivare il "Crittografia degli oggetti memorizzati" In Grid Manager. Quando questa opzione è attivata, tutti i nuovi oggetti che non sono crittografati a livello di bucket o a livello di oggetto vengono crittografati durante l'acquisizione.	Dati S3 e Swift di recente acquisizione. Gli oggetti memorizzati esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati.
Crittografia bucket S3	Viene inviata una richiesta PutBucketEncryption per abilitare la crittografia per il bucket. Tutti i nuovi oggetti che non sono crittografati a livello di oggetto vengono crittografati durante l'acquisizione.	Solo i dati S3 degli oggetti acquisiti di recente. È necessario specificare la crittografia per il bucket. Gli oggetti bucket esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati. "Operazioni sui bucket"

Opzione di crittografia	Come funziona	Valido per
Crittografia a oggetti lato server (SSE) S3	Viene inviata una richiesta S3 per memorizzare un oggetto e includere `x-amz-server-side-encryption` intestazione della richiesta.	Solo i dati S3 degli oggetti acquisiti di recente. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati. StorageGRID gestisce le chiavi. "Utilizzare la crittografia lato server"
Crittografia a oggetti S3 lato server con chiavi fornite dal cliente (SSE-C)	Viene inviata una richiesta S3 per memorizzare un oggetto e includere tre intestazioni di richiesta. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Solo i dati S3 degli oggetti acquisiti di recente. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati. Le chiavi vengono gestite al di fuori di StorageGRID. "Utilizzare la crittografia lato server"
Crittografia di un volume esterno o di un datastore	Se la piattaforma di implementazione lo supporta, si utilizza un metodo di crittografia esterno a StorageGRID per crittografare un intero volume o datastore.	Tutti i dati degli oggetti, i metadati e i dati di configurazione del sistema, presupponendo che ogni volume o datastore sia crittografato. Un metodo di crittografia esterno offre un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati.

Opzione di crittografia	Come funziona	Valido per
Crittografia degli oggetti al di fuori di StorageGRID	Si utilizza un metodo di crittografia esterno a StorageGRID per crittografare i dati degli oggetti e i metadati prima che vengano acquisiti in StorageGRID.	Solo dati a oggetti e metadati (i dati di configurazione del sistema non sono crittografati). Un metodo di crittografia esterno offre un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati. "Amazon Simple Storage Service - Guida per gli sviluppatori: Protezione dei dati mediante crittografia lato client"

Utilizzare più metodi di crittografia

A seconda dei requisiti, è possibile utilizzare più metodi di crittografia alla volta. Ad esempio:

- È possibile utilizzare un KMS per proteggere i nodi dell'appliance e utilizzare la funzionalità di sicurezza del disco in Gestione sistema di SANtricity per "crittografare due volte" i dati sui dischi con crittografia automatica delle stesse appliance.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e utilizzare l'opzione di crittografia degli oggetti memorizzati per crittografare tutti gli oggetti quando vengono acquisiti.

Se solo una piccola parte degli oggetti richiede la crittografia, prendere in considerazione il controllo della crittografia a livello di bucket o di singolo oggetto. L'abilitazione di più livelli di crittografia comporta un costo aggiuntivo per le performance.

Gestire i certificati

Gestione dei certificati di sicurezza: Panoramica

I certificati di sicurezza sono piccoli file di dati utilizzati per creare connessioni sicure e affidabili tra i componenti di StorageGRID e tra i componenti di StorageGRID e i sistemi esterni.

StorageGRID utilizza due tipi di certificati di sicurezza:

- **I certificati 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.
- **Certificati client** autenticano un'identità del client o dell'utente sul server, fornendo un'autenticazione più sicura rispetto alle sole password. I certificati client non crittografano i dati.

Quando un client si connette al server utilizzando HTTPS, il server risponde con il certificato del server, che contiene una chiave pubblica. Il client verifica questo certificato confrontando la firma del server con la firma sulla copia del certificato. Se le firme corrispondono, il client avvia una sessione con il server utilizzando la stessa chiave pubblica.

StorageGRID funziona come server per alcune connessioni (come l'endpoint del bilanciamento del carico) o come client per altre connessioni (come il servizio di replica di CloudMirror).

Certificato Grid CA predefinito

StorageGRID include un'autorità di certificazione (CA) incorporata che genera un certificato Grid CA interno durante l'installazione del sistema. Il certificato Grid CA viene utilizzato, per impostazione predefinita, per proteggere il traffico StorageGRID interno. Un'autorità di certificazione esterna (CA) può emettere certificati personalizzati pienamente conformi ai criteri di sicurezza delle informazioni dell'organizzazione. Sebbene sia possibile utilizzare il certificato Grid CA per un ambiente non di produzione, la procedura consigliata per un ambiente di produzione consiste nell'utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Sono supportate anche connessioni non protette senza certificato, ma non sono consigliate.

- I certificati CA personalizzati non rimuovono i certificati interni; tuttavia, i certificati personalizzati devono essere quelli specificati per la verifica delle connessioni al server.
- Tutti i certificati personalizzati devono soddisfare il "linee guida per la protezione avanzata del sistema per i certificati server".
- StorageGRID supporta il raggruppamento di certificati da una CA in un singolo file (noto come bundle di certificati CA).

> StorageGRID include anche certificati CA del sistema operativo che sono gli stessi su tutte le griglie. Negli ambienti di produzione, assicurarsi di specificare un certificato personalizzato firmato da un'autorità di certificazione esterna al posto del certificato CA del sistema operativo.

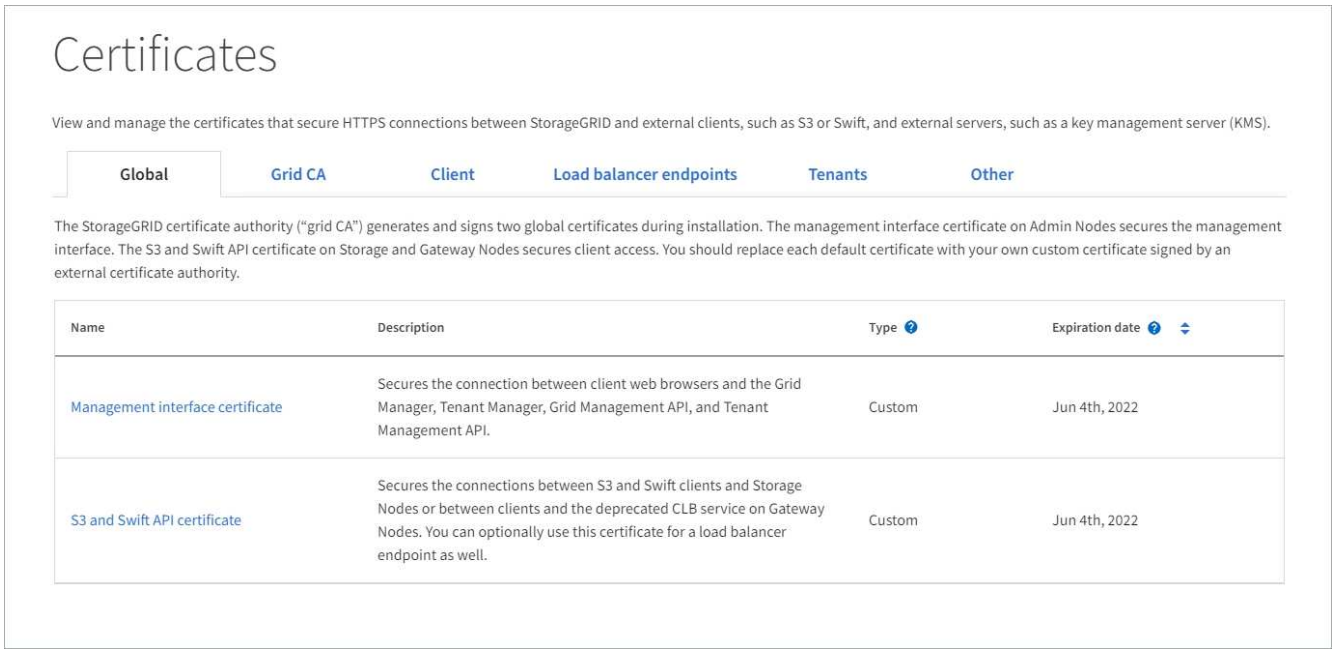
Le varianti dei tipi di certificato server e client vengono implementate in diversi modi. Prima di configurare il sistema, è necessario disporre di tutti i certificati necessari per la configurazione specifica di StorageGRID.

Accesso ai certificati di sicurezza

È possibile accedere alle informazioni su tutti i certificati StorageGRID in una singola posizione, insieme ai collegamenti al flusso di lavoro di configurazione per ciascun certificato.

Fasi

1. Da Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**.



2. Selezionare una scheda nella pagina certificati per informazioni su ciascuna categoria di certificati e per accedere alle impostazioni del certificato. È possibile accedere a una scheda se si dispone di "autorizzazione appropriata".

   - **Globale**: Protegge l'accesso a StorageGRID da browser Web e client API esterni.
   - **Grid CA**: Protegge il traffico StorageGRID interno.
   - **Client**: Protegge le connessioni tra client esterni e il database StorageGRID Prometheus.
   - **Endpoint del bilanciamento del carico**: Protegge le connessioni tra i client S3 e Swift e il bilanciamento del carico StorageGRID.
   - **Tenant**: Protegge le connessioni ai server di federazione delle identità o dagli endpoint dei servizi della piattaforma alle risorse di storage S3.
   - **Altro**: Protegge le connessioni StorageGRID che richiedono certificati specifici.

   Ciascuna scheda viene descritta di seguito con collegamenti a dettagli aggiuntivi del certificato.

Globale

I certificati globali proteggono l'accesso a StorageGRID dai browser Web e dai client API S3 e Swift esterni. Durante l'installazione, l'autorità di certificazione StorageGRID genera inizialmente due certificati globali. La procedura consigliata per un ambiente di produzione consiste nell'utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna.

- Certificato dell'interfaccia di gestione: Protegge le connessioni del browser Web client alle interfacce di gestione StorageGRID.
- Certificato API S3 e Swift: Protegge le connessioni API del client ai nodi di storage, ai nodi di amministrazione e ai nodi gateway, utilizzati dalle applicazioni client S3 e Swift per caricare e scaricare i dati degli oggetti.

Le informazioni sui certificati globali installati includono:

- **Nome**: Nome del certificato con collegamento alla gestione del certificato.
- **Descrizione**
- **Type**: Personalizzato o predefinito.
  Per una migliore protezione della griglia, è sempre consigliabile utilizzare un certificato personalizzato.
- **Data di scadenza**: Se si utilizza il certificato predefinito, non viene visualizzata alcuna data di scadenza.

È possibile:

- Sostituire i certificati predefiniti con certificati personalizzati firmati da un'autorità di certificazione esterna per una maggiore sicurezza della griglia:
  - "Sostituire il certificato predefinito dell'interfaccia di gestione generata da StorageGRID" Utilizzato per le connessioni di Grid Manager e Tenant Manager.
  - "Sostituire il certificato API S3 e Swift" Utilizzato per le connessioni endpoint (opzionali) del nodo di storage e del bilanciamento del carico.
- "Ripristinare il certificato dell'interfaccia di gestione predefinita."
- "Ripristinare il certificato API S3 e Swift predefinito."
- "Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione."
- Copiare o scaricare "certificato dell'interfaccia di gestione" oppure "Certificato API S3 e Swift".

CA griglia

Il Certificato Grid CA, Generata dall'autorità di certificazione StorageGRID durante l'installazione di StorageGRID, protegge tutto il traffico StorageGRID interno.

Le informazioni sul certificato includono la data di scadenza del certificato e il contenuto del certificato.

È possibile "Copia o scarica il certificato Grid CA", ma non è possibile modificarla.

Client

Certificati client, Generata da un'autorità di certificazione esterna, protegge le connessioni tra i tool di monitoraggio esterni e il database StorageGRID Prometheus.

La tabella dei certificati contiene una riga per ciascun certificato client configurato e indica se il certificato può essere utilizzato per l'accesso al database Prometheus, insieme alla data di scadenza del certificato.

È possibile:

- "Caricare o generare un nuovo certificato client."
- Selezionare il nome di un certificato per visualizzare i dettagli del certificato in cui è possibile:
  - "Modificare il nome del certificato client."
  - "Impostare l'autorizzazione di accesso Prometheus."
  - "Caricare e sostituire il certificato del client."
  - "Copiare o scaricare il certificato client."
  - "Rimuovere il certificato client."
- Selezionare **azioni** per eseguire rapidamente "modifica", "allega", o. "rimuovere" un certificato client. È possibile selezionare fino a 10 certificati client e rimuoverli contemporaneamente utilizzando **azioni** > **Rimuovi**.

Endpoint del bilanciamento del carico

Certificati endpoint per il bilanciamento del carico Proteggere le connessioni tra i client S3 e Swift e il servizio di bilanciamento del carico StorageGRID sui nodi gateway e sui nodi di amministrazione.

La tabella degli endpoint del bilanciamento del carico dispone di una riga per ciascun endpoint del bilanciamento del carico configurato e indica se per l'endpoint viene utilizzato il certificato API S3 e Swift globale o un certificato dell'endpoint del bilanciamento del carico personalizzato. Viene visualizzata anche la data di scadenza di ciascun certificato.

> Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

È possibile:

- "Visualizzare un endpoint di bilanciamento del carico", inclusi i dettagli del certificato.
- "Specificare un certificato endpoint per il bilanciamento del carico per FabricPool."
- "Utilizza il certificato globale S3 e Swift API" invece di generare un nuovo certificato endpoint per il bilanciamento del carico.

Tenant

I tenant possono utilizzare certificati del server di federazione delle identità oppure certificati endpoint del servizio di piattaforma Per proteggere le connessioni con StorageGRID.

La tabella tenant ha una riga per ciascun tenant e indica se ciascun tenant dispone dell'autorizzazione per utilizzare la propria origine di identità o i propri servizi di piattaforma.

È possibile:

- "Selezionare il nome di un tenant per accedere al tenant manager"
- "Selezionare un nome tenant per visualizzare i dettagli della federazione delle identità del tenant"
- "Selezionare un nome tenant per visualizzare i dettagli dei servizi della piattaforma tenant"
- "Specificare un certificato endpoint del servizio di piattaforma durante la creazione dell'endpoint"

Altro

StorageGRID utilizza altri certificati di sicurezza per scopi specifici. Questi certificati sono elencati in base

al nome funzionale. Altri certificati di sicurezza includono:

- Certificati Cloud Storage Pool
- Certificati di notifica degli avvisi via email
- Certificati server syslog esterni
- Certificati di connessione Grid Federation
- Certificati di federazione delle identità
- Certificati KMS (Key Management Server)
- Certificati Single Sign-on

Le informazioni indicano il tipo di certificato utilizzato da una funzione e le relative date di scadenza del certificato server e client, a seconda dei casi. Selezionando il nome di una funzione si apre una scheda del browser in cui è possibile visualizzare e modificare i dettagli del certificato.

> ⓘ È possibile visualizzare e accedere alle informazioni relative ad altri certificati solo se si dispone di "autorizzazione appropriata".

È possibile:

- "Specificare un certificato Cloud Storage Pool per S3, C2S S3 o Azure"
- "Specificare un certificato per le notifiche e-mail di avviso"
- "Utilizzare un certificato per un server syslog esterno"
- "Ruotare i certificati di connessione Grid Federation"
- "Visualizzare e modificare un certificato di federazione delle identità"
- "Caricare i certificati del server e del client del server di gestione delle chiavi (KMS)"
- "Specificare manualmente un certificato SSO per un trust della parte che si basa"

Dettagli del certificato di sicurezza

Di seguito sono descritti i tipi di certificato di protezione, con collegamenti alle istruzioni di implementazione.

Certificato dell'interfaccia di gestione

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i browser Web client e l'interfaccia di gestione di StorageGRID, consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza. Questo certificato autentica anche le connessioni API Grid Management e API Tenant Management. È possibile utilizzare il certificato predefinito creato durante l'installazione o caricare un certificato personalizzato.	**CONFIGURATION** > **Security** > **Certificates**, selezionare la scheda **Global**, quindi selezionare **Management interface certificate**	"Configurare i certificati dell'interfaccia di gestione"

Certificato API S3 e Swift

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica le connessioni client sicure S3 o Swift a un nodo di storage e agli endpoint del bilanciamento del carico (opzionale).	**CONFIGURATION** > **Security** > **Certificates**, selezionare la scheda **Global**, quindi **S3 and Swift API certificate**	"Configurare i certificati API S3 e Swift"

Certificato Grid CA

Vedere Descrizione del certificato Grid CA predefinito.

Certificato del client di amministratore

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Client	Installato su ciascun client, consentendo a StorageGRID di autenticare l'accesso client esterno. • Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus. • Consente il monitoraggio sicuro di StorageGRID utilizzando strumenti esterni.	**CONFIGURAZIONE** > **sicurezza** > **certificati**, quindi selezionare la scheda **Client**	"Configurare i certificati client"

Certificato endpoint per il bilanciamento del carico

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i client S3 o Swift e il servizio bilanciamento del carico StorageGRID sui nodi gateway e sui nodi di amministrazione. È possibile caricare o generare un certificato di bilanciamento del carico quando si configura un endpoint di bilanciamento del carico. Le applicazioni client utilizzano il certificato di bilanciamento del carico durante la connessione a StorageGRID per salvare e recuperare i dati degli oggetti. È anche possibile utilizzare una versione personalizzata del Global Certificato API S3 e Swift Certificato per autenticare le connessioni al servizio Load Balancer. Se il certificato globale viene utilizzato per autenticare le connessioni del bilanciamento del carico, non è necessario caricare o generare un certificato separato per ciascun endpoint del bilanciamento del carico. **Nota:** il certificato utilizzato per l'autenticazione del bilanciamento del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID.	**CONFIGURAZIONE** > **rete** > **endpoint del bilanciamento del carico**	• "Configurare gli endpoint del bilanciamento del carico" • "Creare un endpoint di bilanciamento del carico per FabricPool"

Certificato endpoint Cloud Storage Pool

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione da un pool di storage cloud StorageGRID a una posizione di storage esterna, ad esempio lo storage S3 Glacier o Microsoft Azure Blob. Per ogni tipo di cloud provider è necessario un certificato diverso.	**ILM** > **Storage Pools**	"Creare un pool di storage cloud"

Certificato di notifica degli avvisi via email

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra un server e-mail SMTP e StorageGRID utilizzato per le notifiche degli avvisi. • Se le comunicazioni con il server SMTP richiedono TLS (Transport Layer Security), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta SMTP richiede certificati client per l'autenticazione.	**ALERTS** > **email setup**	"Imposta le notifiche via email per gli avvisi"

Certificato server syslog esterno

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione TLS o RELP/TLS tra un server syslog esterno che registra gli eventi in StorageGRID. **Nota:** non è richiesto un certificato server syslog esterno per le connessioni TCP, RELP/TCP e UDP a un server syslog esterno.	**CONFIGURAZIONE** > **monitoraggio** > **Audit and syslog server**	"Utilizzare un server syslog esterno"

certificato di connessione Grid Federation

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autenticare e crittografare le informazioni inviate tra il sistema StorageGRID corrente e un'altra griglia in una connessione a federazione di griglie.	**CONFIGURAZIONE** > **sistema** > **federazione griglia**	• "Creare connessioni di federazione di griglie" • "Ruotare i certificati di connessione"

Certificato di federazione delle identità

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra StorageGRID e un provider di identità esterno, ad esempio Active Directory, OpenLDAP o Oracle Directory Server. Utilizzato per la federazione delle identità, che consente ai gruppi di amministrazione e agli utenti di essere gestiti da un sistema esterno.	**CONFIGURAZIONE** > **controllo accessi** > **federazione identità**	"USA la federazione delle identità"

Certificato del Key Management Server (KMS)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra StorageGRID e un KMS (Key Management Server) esterno, che fornisce chiavi di crittografia ai nodi appliance StorageGRID.	**CONFIGURAZIONE** > **sicurezza** > **Server di gestione delle chiavi**	"Aggiunta del server di gestione delle chiavi (KMS)"

Certificato endpoint dei servizi di piattaforma

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione dal servizio della piattaforma StorageGRID a una risorsa di storage S3.	**Tenant Manager** > **STORAGE (S3)** > **endpoint dei servizi della piattaforma**	"Creare endpoint di servizi di piattaforma" "Modifica dell'endpoint dei servizi della piattaforma"

Certificato SSO (Single Sign-on)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i servizi di federazione delle identità, come ad FS (Active Directory Federation Services) e StorageGRID, utilizzati per le richieste SSO (Single Sign-on).	**CONFIGURAZIONE** > **controllo di accesso** > **Single Sign-on**	"Configurare il single sign-on"

Esempi di certificati

Esempio 1: Servizio di bilanciamento del carico

In questo esempio, StorageGRID agisce come server.

1. È possibile configurare un endpoint di bilanciamento del carico e caricare o generare un certificato server in StorageGRID.
2. È possibile configurare una connessione client S3 o Swift all'endpoint del bilanciamento del carico e caricare lo stesso certificato nel client.
3. Quando il client desidera salvare o recuperare i dati, si connette all'endpoint del bilanciamento del carico utilizzando HTTPS.
4. StorageGRID risponde con il certificato del server, che contiene una chiave pubblica, e con una firma basata sulla chiave privata.

5. Il client verifica questo certificato confrontando la firma del server con la firma sulla copia del certificato. Se le firme corrispondono, il client avvia una sessione utilizzando la stessa chiave pubblica.
6. Il client invia i dati dell'oggetto a StorageGRID.

Esempio 2: Server KMS (Key Management Server) esterno

In questo esempio, StorageGRID agisce come client.

1. Utilizzando il software del server di gestione delle chiavi esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server con firma CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, è possibile configurare un server KMS e caricare i certificati server e client e la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, effettua una richiesta al server KMS che include i dati del certificato e una firma basata sulla chiave privata.
4. Il server KMS convalida la firma del certificato e decide che può fidarsi di StorageGRID.
5. Il server KMS risponde utilizzando la connessione validata.

Configurare i certificati del server

Tipi di certificato server supportati

Il sistema StorageGRID supporta certificati personalizzati crittografati con RSA o ECDSA (algoritmo di firma digitale a curva ellittica).

> Il tipo di crittografia per il criterio di protezione deve corrispondere al tipo di certificato del server. Ad esempio, le crittografia RSA richiedono certificati RSA e le crittografia ECDSA richiedono certificati ECDSA. Vedere "Gestire i certificati di sicurezza". Se si configura un criterio di protezione personalizzato non compatibile con il certificato del server, è possibile "ripristinare temporaneamente il criterio di protezione predefinito".

Per ulteriori informazioni su come StorageGRID protegge le connessioni client, vedere "Sicurezza per client S3 e Swift".

Configurare i certificati dell'interfaccia di gestione

È possibile sostituire il certificato dell'interfaccia di gestione predefinita con un singolo certificato personalizzato che consente agli utenti di accedere a Grid Manager e a Tenant Manager senza incontrare avvisi di sicurezza. È inoltre possibile ripristinare il certificato dell'interfaccia di gestione predefinita o generarne uno nuovo.

A proposito di questa attività

Per impostazione predefinita, ogni nodo amministrativo riceve un certificato firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato dell'interfaccia di gestione personalizzata comune e dalla chiave privata corrispondente.

Poiché per tutti i nodi di amministrazione viene utilizzato un singolo certificato di interfaccia di gestione personalizzata, è necessario specificare il certificato come carattere jolly o certificato multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi Admin nella griglia.

È necessario completare la configurazione sul server e, a seconda dell'autorità di certificazione principale (CA) utilizzata, gli utenti potrebbero dover installare il certificato Grid CA nel browser Web che utilizzeranno per accedere a Grid Manager e a Tenant Manager.

Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** viene attivato quando il certificato del server sta per scadere. Se necessario, è possibile visualizzare la scadenza del certificato corrente selezionando **CONFIGURAZIONE** > **sicurezza** > **certificati** e osservando la data di scadenza del certificato dell'interfaccia di gestione nella scheda Globale.

Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Tu ripristinare da un certificato dell'interfaccia di gestione personalizzata al certificato server predefinito.

Aggiungere un certificato di interfaccia di gestione personalizzata

Per aggiungere un certificato di interfaccia di gestione personalizzato, è possibile fornire un certificato personalizzato o generarne uno utilizzando Grid Manager.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

Carica certificato

Caricare i file dei certificati del server richiesti.

a. Selezionare **carica certificato**.

b. Caricare i file dei certificati del server richiesti:

- **Server certificate**: Il file di certificato del server personalizzato (con codifica PEM).
- **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (`.key`).

> Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere 2048 bit o superiori.

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

  Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Selezionare **Salva**.
Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

Generare un certificato

Generare i file dei certificati del server.

> La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato dell'interfaccia di gestione personalizzata firmato da un'autorità di certificazione esterna.

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.

Campo	Descrizione
IP	Uno o più indirizzi IP da includere nel certificato.
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**.
Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

> Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Dopo aver aggiunto un certificato dell'interfaccia di gestione personalizzata, la pagina del certificato dell'interfaccia di gestione visualizza informazioni dettagliate sul certificato per i certificati in uso.
È possibile scaricare o copiare il certificato PEM come richiesto.

Ripristinare il certificato dell'interfaccia di gestione predefinita

È possibile ripristinare l'utilizzo del certificato dell'interfaccia di gestione predefinita per Grid Manager e Tenant Manager Connections.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato predefinito**.

   Quando si ripristina il certificato dell'interfaccia di gestione predefinita, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. Il certificato predefinito dell'interfaccia di gestione viene utilizzato per tutte le nuove connessioni client successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione

Se è richiesta una convalida rigorosa del nome host, è possibile utilizzare uno script per generare il certificato dell'interfaccia di gestione.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai il `Passwords.txt` file.

A proposito di questa attività

La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato firmato da un'autorità di certificazione esterna.

Fasi

1. Ottenere il nome di dominio completo (FQDN) di ciascun nodo di amministrazione.
2. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

3. Configurare StorageGRID con un nuovo certificato autofirmato.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Per `--domains`, Utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi di amministrazione. Ad esempio, `*.ui.storagegrid.example.com` utilizza il carattere jolly * per rappresentare `admin1.ui.storagegrid.example.com` e. `admin2.ui.storagegrid.example.com`.
   - Impostare `--type` a. `management` Per configurare il certificato dell'interfaccia di gestione, utilizzato da Grid Manager e Tenant Manager.

◦ Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devono essere ricreati prima della scadenza. È possibile utilizzare `--days` argomento per eseguire l'override del periodo di validità predefinito.

> Il periodo di validità di un certificato inizia quando `make-certificate` è eseguito. È necessario assicurarsi che il client di gestione sia sincronizzato con la stessa origine temporale di StorageGRID; in caso contrario, il client potrebbe rifiutare il certificato.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

L'output risultante contiene il certificato pubblico necessario al client API di gestione.

4. Selezionare e copiare il certificato.

   Includere i tag BEGIN e END nella selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`
6. Verificare che il certificato sia stato configurato:
   a. Accedere a Grid Manager.
   b. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**
   c. Nella scheda **Global**, selezionare **Management interface certificate**.
7. Configurare il client di gestione in modo che utilizzi il certificato pubblico copiato. Includere i tag inizio e FINE.

Scaricare o copiare il certificato dell'interfaccia di gestione

È possibile salvare o copiare il contenuto del certificato dell'interfaccia di gestione per utilizzarlo altrove.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scaricare il file di certificato o il bundle CA

Scarica il certificato o il bundle CA `.pem` file. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Scarica certificato** o **Scarica bundle CA**.

   Se si sta scaricando un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM** or **Copy CA bundle PEM**.

   Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incollare il certificato copiato in un editor di testo.

c. Salvare il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati API S3 e Swift

È possibile sostituire o ripristinare il certificato server utilizzato per le connessioni client S3 o Swift ai nodi di storage o agli endpoint del bilanciamento del carico. Il certificato del server personalizzato sostitutivo è specifico dell'organizzazione.

A proposito di questa attività

Per impostazione predefinita, ogni nodo di storage viene emesso un certificato server X.509 firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla chiave privata corrispondente.

Per tutti i nodi di storage viene utilizzato un singolo certificato server personalizzato, pertanto è necessario specificare il certificato come certificato wildcard o multi-dominio se i client devono verificare il nome host durante la connessione all'endpoint di storage. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi di storage nella griglia.

Una volta completata la configurazione sul server, potrebbe essere necessario installare anche il certificato Grid CA nel client S3 o Swift API che verrà utilizzato per accedere al sistema, a seconda dell'autorità di certificazione (CA) root in uso.

Per garantire che le operazioni non vengano interrotte da un certificato server guasto, l'avviso **scadenza del certificato server globale per S3 e Swift API** viene attivato quando il certificato del server root sta per scadere. Se necessario, è possibile visualizzare la scadenza del certificato corrente selezionando **CONFIGURAZIONE** > **sicurezza** > **certificati** e osservando la data di scadenza del certificato API S3 e Swift nella scheda Globale.

È possibile caricare o generare un certificato S3 e Swift API personalizzato.

Aggiungere un certificato API S3 e Swift personalizzato

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

Carica certificato

Caricare i file dei certificati del server richiesti.

a. Selezionare **carica certificato**.
b. Caricare i file dei certificati del server richiesti:
   - **Server certificate**: Il file di certificato del server personalizzato (con codifica PEM).
   - **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (`.key`).

     > Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere 2048 bit o superiori.

   - **Bundle CA**: Un singolo file opzionale contenente i certificati di ciascuna autorità di certificazione di emissione intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
c. Selezionare i dettagli del certificato per visualizzare i metadati e il PEM per ogni certificato S3 e Swift API personalizzato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.
   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.
d. Selezionare **Salva**.

   Il certificato server personalizzato viene utilizzato per le successive nuove connessioni client S3 e Swift.

Generare un certificato

Generare i file dei certificati del server.

a. Selezionare **genera certificato**.
b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
IP	Uno o più indirizzi IP da includere nel certificato.

Campo	Descrizione
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati e il PEM per il certificato S3 e Swift API personalizzato generato.

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**.

   Il certificato server personalizzato viene utilizzato per le successive nuove connessioni client S3 e Swift.

5. Selezionare una scheda per visualizzare i metadati per il certificato del server StorageGRID predefinito, un certificato CA firmato caricato o un certificato personalizzato generato.

   Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

7. Dopo aver aggiunto un certificato API S3 e Swift personalizzato, la pagina del certificato API S3 e Swift visualizza informazioni dettagliate sul certificato per il certificato API S3 e Swift personalizzato in uso.

È possibile scaricare o copiare il certificato PEM come richiesto.

Ripristinare il certificato API S3 e Swift predefinito

È possibile ripristinare l'utilizzo del certificato API S3 e Swift predefinito per le connessioni dei client S3 e Swift ai nodi di storage. Tuttavia, non è possibile utilizzare il certificato S3 e Swift API predefinito per un endpoint di bilanciamento del carico.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**.
3. Selezionare **Usa certificato predefinito**.

   Quando si ripristina la versione predefinita del certificato globale S3 e Swift API, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. Il certificato API S3 e Swift predefinito verrà utilizzato per le successive nuove connessioni dei client S3 e Swift ai nodi di storage.

4. Selezionare **OK** per confermare l'avviso e ripristinare il certificato S3 e Swift API predefinito.

   Se si dispone dell'autorizzazione di accesso Root ed è stato utilizzato il certificato S3 e Swift API personalizzato per le connessioni degli endpoint del bilanciamento del carico, viene visualizzato un elenco degli endpoint del bilanciamento del carico che non saranno più accessibili utilizzando il certificato S3 e Swift API predefinito. Passare a. "Configurare gli endpoint del bilanciamento del carico" per modificare o rimuovere gli endpoint interessati.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Scaricare o copiare il certificato API S3 e Swift

È possibile salvare o copiare i contenuti dei certificati API S3 e Swift per utilizzarli altrove.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scaricare il file di certificato o il bundle CA

Scarica il certificato o il bundle CA `.pem` file. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Scarica certificato** o **Scarica bundle CA**.

   Se si sta scaricando un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM** or **Copy CA bundle PEM**.

   Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incollare il certificato copiato in un editor di testo.

c. Salvare il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Informazioni correlate

- "UTILIZZARE L'API REST S3"
- "Utilizzare l'API REST di Swift"
- "Configurare i nomi di dominio degli endpoint S3"

Copiare il certificato Grid CA

StorageGRID utilizza un'autorità di certificazione interna (CA) per proteggere il traffico interno. Questo certificato non cambia se si caricano i propri certificati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Se è stato configurato un certificato server personalizzato, le applicazioni client devono verificare il server utilizzando il certificato server personalizzato. Non devono copiare il certificato CA dal sistema StorageGRID.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Grid CA**.
2. Nella sezione **Certificate PEM**, scaricare o copiare il certificato.

Scaricare il file del certificato

Scarica il certificato `.pem` file.

a. Selezionare **Scarica certificato**.
b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato PEM

Copiare il testo del certificato per incollarlo altrove.

a. Selezionare **Copy certificate PEM** (Copia certificato PEM).
b. Incollare il certificato copiato in un editor di testo.
c. Salvare il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati StorageGRID per FabricPool

Per i client S3 che eseguono una convalida rigorosa del nome host e non supportano la disattivazione della convalida rigorosa del nome host, ad esempio i client ONTAP che utilizzano FabricPool, è possibile generare o caricare un certificato server quando si configura l'endpoint del bilanciamento del carico.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

Quando si crea un endpoint di bilanciamento del carico, è possibile generare un certificato server autofirmato o caricare un certificato firmato da un'autorità di certificazione (CA) nota. Negli ambienti di produzione, è necessario utilizzare un certificato firmato da una CA nota. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

La procedura riportata di seguito fornisce linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, vedere "Configurare StorageGRID per FabricPool".

Fasi

1. Facoltativamente, configurare un gruppo ad alta disponibilità (ha) da utilizzare per FabricPool.
2. Creare un endpoint di bilanciamento del carico S3 da utilizzare per FabricPool.

Quando si crea un endpoint di bilanciamento del carico HTTPS, viene richiesto di caricare il certificato del server, la chiave privata del certificato e il bundle CA opzionale.

3. Collega StorageGRID come Tier cloud in ONTAP.

   Specificare la porta endpoint del bilanciamento del carico e il nome di dominio completo utilizzato nel certificato CA caricato. Quindi, fornire il certificato CA.

   > Se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.

Configurare i certificati client

I certificati client consentono ai client esterni autorizzati di accedere al database StorageGRID Prometheus, fornendo un modo sicuro per i tool esterni di monitorare StorageGRID.

Se si desidera accedere a StorageGRID utilizzando uno strumento di monitoraggio esterno, è necessario caricare o generare un certificato client utilizzando Grid Manager e copiare le informazioni del certificato nello strumento esterno.

Vedere "Gestire i certificati di sicurezza" e. "Configurare certificati server personalizzati".

> Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza dei certificati client configurati nella pagina certificati** viene attivato quando il certificato del server sta per scadere. Se necessario, è possibile visualizzare la scadenza del certificato corrente selezionando **CONFIGURAZIONE** > **sicurezza** > **certificati** e osservando la data di scadenza del certificato client nella scheda Client.

> Se si utilizza un server di gestione delle chiavi (KMS) per proteggere i dati su nodi appliance appositamente configurati, consultare le informazioni specifiche su "Caricamento di un certificato del client KMS".

Prima di iniziare

- Si dispone dell'autorizzazione di accesso root.
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Per configurare un certificato client:
  - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
  - Se è stato configurato il certificato dell'interfaccia di gestione StorageGRID, si dispone della CA, del certificato client e della chiave privata utilizzati per configurare il certificato dell'interfaccia di gestione.
  - Per caricare il certificato, la chiave privata del certificato è disponibile sul computer locale.
  - La chiave privata deve essere stata salvata o registrata al momento della creazione. Se non si dispone della chiave privata originale, è necessario crearne una nuova.
- Per modificare un certificato client:
  - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
  - Per caricare il proprio certificato o un nuovo certificato, la chiave privata, il certificato client e la CA (se utilizzata) sono disponibili sul computer locale.

Aggiungere certificati client

Per aggiungere il certificato client, attenersi a una delle seguenti procedure:

- Certificato dell'interfaccia di gestione già configurato
- CERTIFICATO client emesso DALLA CA
- Certificato generato da Grid Manager

Certificato dell'interfaccia di gestione già configurato

Utilizzare questa procedura per aggiungere un certificato client se un certificato dell'interfaccia di gestione è già configurato utilizzando una CA, un certificato client e una chiave privata forniti dal cliente.

Fasi

1. In Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, caricare il certificato dell'interfaccia di gestione.
   a. Selezionare **carica certificato**.
   b. Selezionare **Sfoglia** e selezionare il file di certificato dell'interfaccia di gestione (`.pem`).
      - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
      - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
   c. Selezionare **Crea** per salvare il certificato in Grid Manager.

      Il nuovo certificato viene visualizzato nella scheda Client.
7. Configurare uno strumento di monitoraggio esterno, Come Grafana.

CERTIFICATO client emesso DALLA CA

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si intende aggiungere un certificato client per Prometheus che utilizza un certificato client emesso dalla CA e una chiave privata.

Fasi

1. Eseguire i passi da a. "configurare un certificato dell'interfaccia di gestione".
2. In Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
3. Selezionare **Aggiungi**.
4. Immettere un nome per il certificato.
5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare

Allow prometheus (Consenti prometheus).

6. Selezionare **continua**.
7. Per il passo **Allega certificati**, caricare i file di certificato client, chiave privata e bundle CA:
   a. Selezionare **carica certificato**.
   b. Selezionare **Sfoglia** e selezionare i file di certificato client, chiave privata e bundle CA (`.pem`).
      - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
      - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
   c. Selezionare **Crea** per salvare il certificato in Grid Manager.

      I nuovi certificati vengono visualizzati nella scheda Client.
8. Configurare uno strumento di monitoraggio esterno, Come Grafana.

Certificato generato da Grid Manager

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si intende aggiungere un certificato client per Prometheus che utilizza la funzione di generazione del certificato in Grid Manager.

Fasi

1. In Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, selezionare **genera certificato**.
7. Specificare le informazioni del certificato:
   - **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
   - **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
   - **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

     Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

     Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.
8. Selezionare **generate**.
9. selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

  Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

  Specificare il nome del file della chiave privata e la posizione di download.

10. Selezionare **Crea** per salvare il certificato in Grid Manager.

    Il nuovo certificato viene visualizzato nella scheda Client.

11. In Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Global**.
12. Selezionare **certificato interfaccia di gestione**.
13. Selezionare **Usa certificato personalizzato**.
14. Caricare i file certificate.pem e private_key.pem da dettagli del certificato del client fase. Non è necessario caricare il bundle CA.
    a. Selezionare **carica certificato**, quindi selezionare **continua**.
    b. Caricare ciascun file di certificato (`.pem`).
    c. Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.

       Il nuovo certificato viene visualizzato nella pagina Management Interface certificate (certificato interfaccia di gestione).

15. Configurare uno strumento di monitoraggio esterno, Come Grafana.

Configura uno strumento di monitoraggio esterno

Fasi

1. Configurare le seguenti impostazioni sullo strumento di monitoraggio esterno, ad esempio Grafana.
   a. **Nome**: Immettere un nome per la connessione.

      StorageGRID non richiede queste informazioni, ma è necessario fornire un nome per verificare la connessione.

   b. **URL**: Immettere il nome di dominio o l'indirizzo IP per il nodo di amministrazione. Specificare HTTPS e la porta 9091.

      Ad esempio: `https://admin-node.example.com:9091`

c. Abilitare **TLS Client Auth** e **con CA Certate**.

d. In TLS/SSL Auth Details (Dettagli autorizzazione TLS/SSL), copiare e incollare: +

- Il certificato CA dell'interfaccia di gestione a **CA Cert**
- Il certificato del client a **Client Cert**
- La chiave privata per **chiave client**

e. **ServerName**: Immettere il nome di dominio del nodo di amministrazione.

Il nome server deve corrispondere al nome di dominio così come appare nel certificato dell'interfaccia di gestione.

2. Salvare e verificare il certificato e la chiave privata copiati da StorageGRID o da un file locale.

Ora puoi accedere alle metriche Prometheus da StorageGRID con il tuo tool di monitoraggio esterno.

Per informazioni sulle metriche, vedere "Istruzioni per il monitoraggio di StorageGRID".

Modificare i certificati client

È possibile modificare un certificato client amministratore per modificarne il nome, abilitare o disabilitare l'accesso Prometheus o caricare un nuovo certificato quando quello corrente è scaduto.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.

Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.
3. Selezionare **Modifica**, quindi selezionare **Modifica nome e permesso**
4. Immettere un nome per il certificato.
5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
6. Selezionare **continua** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

Allegare un nuovo certificato client

È possibile caricare un nuovo certificato una volta scaduto il certificato corrente.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.

Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.

3. Selezionare **Edit** (Modifica), quindi un’opzione di modifica.

Carica certificato

Copiare il testo del certificato per incollarlo altrove.

a. Selezionare **carica certificato**, quindi selezionare **continua**.
b. Caricare il nome del certificato client (`.pem`).

   Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
c. Selezionare **Crea** per salvare il certificato in Grid Manager.

   Il certificato aggiornato viene visualizzato nella scheda Client.

Generare un certificato

Generare il testo del certificato da incollare altrove.

a. Selezionare **genera certificato**.
b. Specificare le informazioni del certificato:

   - **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
   - **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
   - **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

     Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

     Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.
c. Selezionare **generate**.
d. Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

   Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del

certificato e incollarlo altrove.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

  Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

  Specificare il nome del file della chiave privata e la posizione di download.

e. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

Scaricare o copiare i certificati client

È possibile scaricare o copiare un certificato client da utilizzare altrove.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera copiare o scaricare.
3. Scaricare o copiare il certificato.

Scaricare il file del certificato

Scarica il certificato `.pem` file.

a. Selezionare **Scarica certificato**.
b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato

Copiare il testo del certificato per incollarlo altrove.

a. Selezionare **Copy certificate PEM** (Copia certificato PEM).
b. Incollare il certificato copiato in un editor di testo.
c. Salvare il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Rimuovere i certificati client

Se non è più necessario un certificato client amministratore, è possibile rimuoverlo.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera rimuovere.
3. Selezionare **Delete** (Elimina), quindi confermare.

> Per rimuovere fino a 10 certificati, selezionare ciascun certificato da rimuovere nella scheda Client, quindi selezionare **azioni** > **Elimina**.

Dopo la rimozione di un certificato, i client che hanno utilizzato il certificato devono specificare un nuovo certificato client per accedere al database StorageGRID Prometheus.

Configurare le impostazioni di sicurezza

Gestire i criteri TLS e SSH

I criteri TLS e SSH determinano i protocolli e le crittografia utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure ai servizi StorageGRID interni.

Il criterio di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. In generale, utilizzare il criterio di compatibilità moderno (predefinito), a meno che il sistema non debba essere conforme ai criteri comuni o non sia necessario utilizzare altre crittografia.

> Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare le crittografia di questi criteri.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Selezionare una policy di sicurezza

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Security settings**.

   La scheda **TLS and SSH policies** (Criteri TLS e SSH) mostra i criteri disponibili. Il criterio attualmente attivo è contrassegnato da un segno di spunta verde sul riquadro del criterio.

2. Consulta i riquadri per scoprire le policy disponibili.

Policy	Descrizione
Compatibilità moderna (impostazione predefinita)	Utilizzare il criterio predefinito se è necessaria una crittografia avanzata e se non si dispone di requisiti speciali. Questo criterio è compatibile con la maggior parte dei client TLS e SSH.
Compatibilità con le versioni precedenti	Utilizzare questo criterio se sono necessarie ulteriori opzioni di compatibilità per i client meno recenti. Le opzioni aggiuntive di questa policy potrebbero renderla meno sicura rispetto alla moderna policy di compatibilità.
Criteri comuni	Utilizzare questa policy se si richiede la certificazione Common Criteria.
FIPS rigoroso	Utilizzare questo criterio se si richiede la certificazione Common Criteria e si deve utilizzare il modulo di protezione Cryptographic NetApp 3.0.8 per connessioni client esterne agli endpoint di bilanciamento del carico, a Gestore tenant e a Gestione griglia. L'utilizzo di questo criterio potrebbe ridurre le performance. **Nota**: Dopo aver selezionato questo criterio, tutti i nodi devono essere "riavviato in modo scorrevole" Per attivare il modulo di protezione crittografica NetApp. Utilizzare **manutenzione** > **riavvio in sequenza** per avviare e riavviare il monitor.
Personalizzato	Creare un criterio personalizzato se è necessario applicare le proprie crittografia.

3. Per visualizzare i dettagli relativi a crittografia, protocolli e algoritmi di ogni policy, selezionare **Visualizza dettagli**.
4. Per modificare la policy corrente, selezionare **Usa policy**.

   Un segno di spunta verde viene visualizzato accanto a **policy corrente** nel riquadro del criterio.

Creare una policy di sicurezza personalizzata

È possibile creare una policy personalizzata se è necessario applicare le proprie crittografia.

Fasi

1. Dal riquadro del criterio più simile al criterio personalizzato che si desidera creare, selezionare **Visualizza dettagli**.
2. Selezionare **Copia negli Appunti**, quindi selezionare **Annulla**.

3. Dal riquadro **Custom policy**, selezionare **Configure and use** (Configura e utilizza).
4. Incollare il JSON copiato e apportare le modifiche necessarie.
5. Selezionare **Usa policy**.

   Un segno di spunta verde viene visualizzato accanto a **Current policy** (policy corrente) nel riquadro Custom policy (policy personalizzate).

6. Facoltativamente, selezionare **Edit Configuration** (Modifica configurazione) per apportare ulteriori modifiche al nuovo criterio personalizzato.

Ripristinare temporaneamente il criterio di protezione predefinito

Se è stato configurato un criterio di protezione personalizzato, potrebbe non essere possibile accedere a Grid Manager se il criterio TLS configurato non è compatibile con "certificato server configurato".

È possibile ripristinare temporaneamente i criteri di protezione predefiniti.

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Eseguire il seguente comando:

   ```
   restore-default-cipher-configurations
   ```

3. Da un browser Web, accedere a Grid Manager sullo stesso nodo di amministrazione.
4. Seguire la procedura descritta in Selezionare una policy di sicurezza per configurare nuovamente il criterio.

È possibile configurare la sicurezza di rete e degli oggetti per crittografare gli oggetti memorizzati, per impedire determinate richieste S3 e Swift o per consentire alle connessioni client ai nodi di storage di utilizzare HTTP invece di HTTPS.

Crittografia degli oggetti memorizzati

La crittografia degli oggetti memorizzati consente la crittografia di tutti i dati degli oggetti durante l'acquisizione tramite S3. Per impostazione predefinita, gli oggetti memorizzati non vengono crittografati, ma è possibile scegliere di crittografare gli oggetti utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando si attiva l'impostazione, tutti gli oggetti inseriti di recente vengono crittografati, ma non vengono apportate modifiche agli oggetti memorizzati esistenti. Se si disattiva la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena acquisiti non vengono crittografati.

L'impostazione di crittografia degli oggetti memorizzati si applica solo agli oggetti S3 che non sono stati crittografati mediante crittografia a livello di bucket o a livello di oggetto.

Per ulteriori informazioni sui metodi di crittografia StorageGRID, vedere "Esaminare i metodi di crittografia StorageGRID".

Impedire la modifica del client

Impedisci modifica client è un'impostazione a livello di sistema. Quando si seleziona l'opzione **Impedisci modifica client**, le seguenti richieste vengono rifiutate.

API REST S3

- Richieste DeleteBucket
- Qualsiasi richiesta di modifica dei dati di un oggetto esistente, dei metadati definiti dall'utente o del tagging degli oggetti S3

API Swift REST

- Eliminare le richieste di container
- Richiede di modificare qualsiasi oggetto esistente. Ad esempio, le seguenti operazioni sono negate: Put Overwrite (Inserisci sovrascrittura), Delete (Elimina), Metadata Update (aggiornamento metadati) e così via.

Abilitare HTTP per le connessioni dei nodi di storage

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per qualsiasi connessione diretta ai nodi di storage. È possibile attivare il protocollo HTTP per queste connessioni, ad esempio durante il test di un grid non di produzione.

Utilizzare HTTP per le connessioni dei nodi di storage solo se i client S3 e Swift devono stabilire connessioni HTTP direttamente ai nodi di storage. Non è necessario utilizzare questa opzione per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (perché è possibile "configurare ciascun endpoint del bilanciamento del carico" Per utilizzare HTTP o HTTPS).

Vedere "Riepilogo: Indirizzi IP e porte per le connessioni client" Per sapere quali porte S3 e i client Swift utilizzano per la connessione ai nodi di storage utilizzando HTTP o HTTPS.

Selezionare le opzioni

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso root.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Security settings**.
2. Selezionare la scheda **rete e oggetti**.
3. Per la crittografia degli oggetti memorizzati, utilizzare l'impostazione **None** (predefinita) se non si desidera crittografare gli oggetti memorizzati oppure selezionare **AES-128** o **AES-256** per crittografare gli oggetti memorizzati.
4. Se si desidera impedire ai client S3 e Swift di effettuare richieste specifiche, selezionare **Impedisci modifica client**.

   Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

5. Se si desidera utilizzare connessioni HTTP, selezionare **Enable HTTP for Storage Node Connections** (attiva HTTP per connessioni nodo di storage) se i client si connettono direttamente ai nodi di storage.

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

6. Selezionare **Salva**.

Modificare le impostazioni di sicurezza dell'interfaccia

Le impostazioni di protezione dell'interfaccia consentono di controllare se gli utenti sono disconnessi se sono inattivi per un periodo di tempo superiore a quello specificato e se una traccia dello stack è inclusa nelle risposte di errore API.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "Autorizzazione di accesso root".

A proposito di questa attività

La pagina **Impostazioni di protezione** include le impostazioni **Timeout inattività browser** e **traccia stack API di gestione**.

Timeout di inattività del browser

Indica per quanto tempo il browser di un utente può rimanere inattivo prima che l'utente venga disconnesso. L'impostazione predefinita è 15 minuti.

Il timeout di inattività del browser è controllato anche da:

- Un timer StorageGRID separato, non configurabile, incluso per la sicurezza del sistema. Ogni token di autenticazione dell'utente scade 16 ore dopo l'accesso. Alla scadenza dell'autenticazione di un utente, l'utente viene automaticamente disconnesso, anche se il timeout di inattività del browser è disattivato o

non è stato raggiunto il valore di timeout del browser. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.

- Impostazioni di timeout per il provider di identità, presupponendo che SSO (Single Sign-on) sia abilitato per StorageGRID.

  Se SSO è attivato e il browser dell'utente si disinserisce, l'utente deve immettere nuovamente le proprie credenziali SSO per accedere nuovamente a StorageGRID. Vedere "Configurare il single sign-on".

Traccia stack API di gestione

Controlla se una traccia di stack viene restituita nelle risposte di errore delle API di Gestione griglia e di Gestione tenant.

Questa opzione è disattivata per impostazione predefinita, ma potrebbe essere necessario attivarla per un ambiente di test. In generale, è necessario lasciare disattivata la traccia dello stack negli ambienti di produzione per evitare di rivelare i dettagli del software interno quando si verificano errori API.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Security settings**.
2. Selezionare la scheda **interfaccia**.
3. Per modificare l'impostazione del timeout di inattività del browser:
   a. Espandere la fisarmonica.
   b. Per modificare il periodo di timeout, specificare un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è di 15 minuti.
   c. Per disattivare questa funzione, deselezionare la casella di controllo.
   d. Selezionare **Salva**.

      La nuova impostazione non influisce sugli utenti che hanno effettuato l'accesso. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser per rendere effettiva la nuova impostazione di timeout.

4. Per modificare l'impostazione per la traccia stack API di gestione:
   a. Espandere la fisarmonica.
   b. Selezionare la casella di controllo per restituire una traccia di stack nelle risposte agli errori di API di Gestione griglia e di Gestione tenant.

      Lasciare la traccia dello stack disattivata negli ambienti di produzione per evitare di rivelare dettagli software interni quando si verificano errori API.

   c. Selezionare **Salva**.

Configurare i server di gestione delle chiavi

Configurazione dei server di gestione delle chiavi: Panoramica

È possibile configurare uno o più server di gestione delle chiavi (KMS) esterni per proteggere i dati su nodi appliance appositamente configurati.

StorageGRID supporta solo alcuni server di gestione delle chiavi. Per un elenco dei prodotti e delle versioni supportate, utilizzare "Tool di matrice di interoperabilità NetApp (IMT)".

Che cos'è un server di gestione delle chiavi (KMS)?

Un server di gestione delle chiavi (KMS) è un sistema esterno di terze parti che fornisce chiavi di crittografia ai nodi dell'appliance StorageGRID nel sito StorageGRID associato utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

È possibile utilizzare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi di qualsiasi appliance StorageGRID con l'impostazione **crittografia dei nodi** attivata durante l'installazione. L'utilizzo di server di gestione delle chiavi con questi nodi appliance consente di proteggere i dati anche in caso di rimozione di un'appliance 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.

StorageGRID non crea o gestisce le chiavi esterne utilizzate per crittografare e decrittare i nodi dell'appliance. Se si intende utilizzare un server di gestione delle chiavi esterno per proteggere i dati StorageGRID, è necessario comprendere come configurare tale server e come gestire le chiavi di crittografia. L'esecuzione delle attività di gestione chiave non rientra nell'ambito di queste istruzioni. Per assistenza, consultare la documentazione relativa al server di gestione delle chiavi o contattare il supporto tecnico.

Panoramica di KMS e configurazione dell'appliance

Prima di utilizzare un server di gestione delle chiavi (KMS) per proteggere i dati StorageGRID sui nodi appliance, è necessario completare due attività di configurazione: La configurazione di uno o più server KMS e l'abilitazione della crittografia dei nodi per i nodi appliance. Una volta completate queste due attività di configurazione, il processo di gestione delle chiavi viene eseguito automaticamente.

Il diagramma di flusso mostra i passaggi di alto livello per l'utilizzo di un KMS per proteggere i dati StorageGRID sui nodi dell'appliance.

Il diagramma di flusso mostra la configurazione di KMS e dell'appliance in parallelo; tuttavia, è possibile configurare i server di gestione delle chiavi prima o dopo aver attivato la crittografia dei nodi per i nuovi nodi appliance, in base ai requisiti.

Configurare il server di gestione delle chiavi (KMS)

La configurazione di un server di gestione delle chiavi include i seguenti passaggi di alto livello.

Fase	Fare riferimento a.
Accedere al software KMS e aggiungere un client per StorageGRID a ciascun cluster KMS o KMS.	"Configurare StorageGRID come client nel KMS"
Ottenere le informazioni richieste per il client StorageGRID sul KMS.	"Configurare StorageGRID come client nel KMS"

Fase	Fare riferimento a.
Aggiungere il KMS al Grid Manager, assegnarlo a un singolo sito o a un gruppo predefinito di siti, caricare i certificati richiesti e salvare la configurazione del KMS.	"Aggiunta di un server di gestione delle chiavi (KMS)"

Configurare l'apparecchio

La configurazione di un nodo appliance per l'utilizzo di KMS include i seguenti passaggi di alto livello.

1. Durante la fase di configurazione hardware dell'installazione dell'appliance, utilizzare il programma di installazione dell'appliance StorageGRID per attivare l'impostazione **crittografia del nodo** dell'appliance.

> Non è possibile attivare l'impostazione **Node Encryption** dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non dispongono della crittografia dei nodi abilitata.

2. Eseguire il programma di installazione dell'appliance StorageGRID. Durante l'installazione, a ciascun volume dell'appliance viene assegnata una chiave di crittografia dei dati casuale (DEK), come segue:
   - I DEK vengono utilizzati per crittografare i dati su ciascun volume. Queste chiavi vengono generate utilizzando la crittografia del disco Linux Unified Key Setup (LUKS) nel sistema operativo dell'appliance e non possono essere modificate.
   - Ogni singolo DEK viene crittografato mediante una chiave di crittografia della chiave master (KEK). La chiave iniziale KEK è una chiave temporanea che crittografa i DEK fino a quando l'appliance non riesce a connettersi al KMS.
3. Aggiungere il nodo appliance a StorageGRID.

Vedere "Abilitare la crittografia del nodo" per ulteriori informazioni.

Processo di crittografia per la gestione delle chiavi (si verifica automaticamente)

La crittografia per la gestione delle chiavi include i seguenti passaggi di alto livello che vengono eseguiti automaticamente.

1. Quando si installa un'appliance che ha attivato la crittografia dei nodi nella griglia, StorageGRID determina se esiste una configurazione KMS per il sito che contiene il nuovo nodo.
   - Se un KMS è già stato configurato per il sito, l'appliance riceve la configurazione KMS.
   - Se non è ancora stato configurato un KMS per il sito, i dati dell'appliance continuano a essere crittografati dalla KEK temporanea fino a quando non si configura un KMS per il sito e l'appliance non riceve la configurazione KMS.
2. L'appliance utilizza la configurazione KMS per connettersi al KMS e richiedere una chiave di crittografia.
3. Il KMS invia una chiave di crittografia all'appliance. La nuova chiave del KMS sostituisce la KEK temporanea e viene ora utilizzata per crittografare e decrittare i DEK per i volumi dell'appliance.

> Tutti i dati che esistono prima che il nodo dell'appliance crittografato si connetta al KMS configurato vengono crittografati con una chiave temporanea. Tuttavia, i volumi dell'appliance non devono essere considerati protetti dalla rimozione dal data center fino a quando la chiave temporanea non viene sostituita dalla chiave di crittografia KMS.

4. Se l'appliance viene accesa o riavviata, si ricollega al KMS per richiedere la chiave. La chiave, che viene salvata nella memoria volatile, non può sopravvivere a una perdita di alimentazione o a un riavvio.

Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi

Prima di configurare un KMS (Key Management Server) esterno, è necessario comprendere le considerazioni e i requisiti.

Quale versione di KMIP è supportata?

StorageGRID supporta KMIP versione 1.4.

"Key Management Interoperability Protocol Specification versione 1.4"

Quali sono le considerazioni sulla rete?

Le impostazioni del firewall di rete devono consentire a ciascun nodo dell'appliance di comunicare attraverso la porta utilizzata per le comunicazioni KMIP (Key Management Interoperability Protocol). La porta KMIP predefinita è 5696.

È necessario assicurarsi che ogni nodo dell'appliance che utilizza la crittografia del nodo disponga dell'accesso di rete al cluster KMS o KMS configurato per il sito.

Quali versioni di TLS sono supportate?

Le comunicazioni tra i nodi dell'appliance e il KMS configurato utilizzano connessioni TLS sicure. StorageGRID può supportare il protocollo TLS 1,2 o TLS 1,3 quando stabilisce connessioni KMIP a un cluster KMS o KMS, in base a ciò che il KMS supporta e a quale "Policy TLS e SSH" si sta utilizzando.

StorageGRID negozia il protocollo e il cifrario (TLS 1,2) o la suite di cifratura (TLS 1,3) con il KMS quando effettua la connessione. Per vedere quali versioni di protocollo e pacchetti di crittografia sono disponibili, consultare `tlsOutbound` Sezione del criterio TLS e SSH attivo della griglia (**CONFIGURAZIONE** > **sicurezza Impostazioni di sicurezza**).

Quali appliance sono supportate?

È possibile utilizzare un server di gestione delle chiavi (KMS) per gestire le chiavi di crittografia per qualsiasi appliance StorageGRID nel grid con l'impostazione **crittografia nodo** attivata. Questa impostazione può essere attivata solo durante la fase di configurazione hardware dell'installazione dell'appliance mediante il programma di installazione dell'appliance StorageGRID.

> Non è possibile attivare la crittografia dei nodi dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia dei nodi abilitata.

È possibile utilizzare il KMS configurato per appliance StorageGRID e nodi appliance.

Non è possibile utilizzare il KMS configurato per i nodi software-based (non-appliance), inclusi i seguenti:

- Nodi implementati come macchine virtuali (VM)
- Nodi implementati all'interno di motori container su host Linux

I nodi implementati su queste altre piattaforme possono utilizzare la crittografia all'esterno di StorageGRID a

livello di datastore o disco.

Quando è necessario configurare i server di gestione delle chiavi?

Per una nuova installazione, in genere è necessario configurare uno o più server di gestione delle chiavi in Grid Manager prima di creare tenant. Questo ordine garantisce che i nodi siano protetti prima che i dati degli oggetti siano memorizzati su di essi.

È possibile configurare i server di gestione delle chiavi in Grid Manager prima o dopo l'installazione dei nodi appliance.

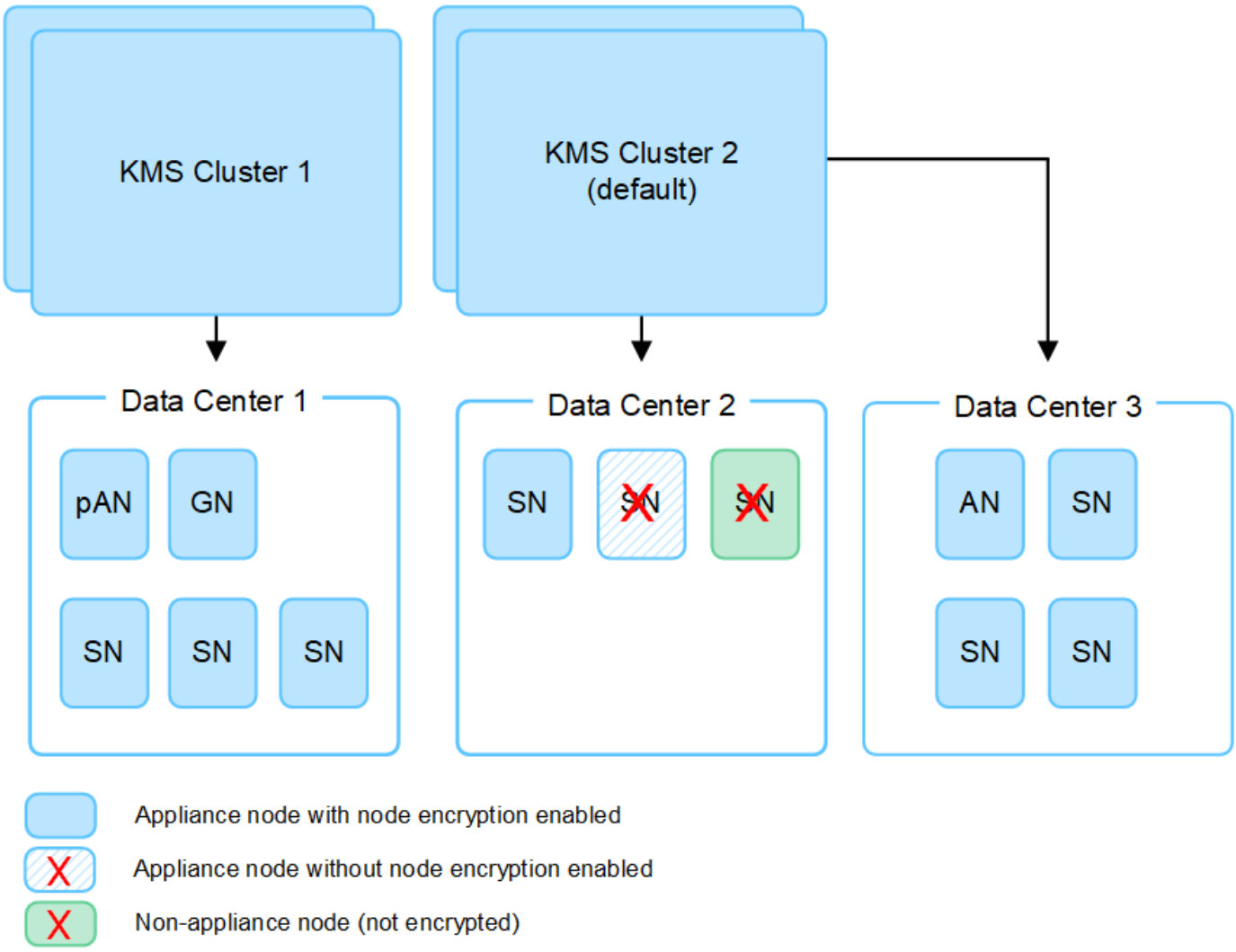
Quanti server di gestione delle chiavi sono necessari?

È possibile configurare uno o più server di gestione delle chiavi esterni per fornire chiavi di crittografia ai nodi dell'appliance nel sistema StorageGRID. Ogni KMS fornisce una singola chiave di crittografia ai nodi dell'appliance StorageGRID in un singolo sito o in un gruppo di siti.

StorageGRID supporta l'utilizzo di cluster KMS. Ogni cluster KMS contiene più server di gestione delle chiavi replicati che condividono le impostazioni di configurazione e le chiavi di crittografia. Si consiglia di utilizzare i cluster KMS per la gestione delle chiavi perché migliora le funzionalità di failover di una configurazione ad alta disponibilità.

Si supponga, ad esempio, che il sistema StorageGRID disponga di tre siti per data center. È possibile configurare un cluster KMS per fornire una chiave a tutti i nodi appliance nel data center 1 e un secondo cluster KMS per fornire una chiave a tutti i nodi appliance in tutti gli altri siti. Quando si aggiunge il secondo cluster KMS, è possibile configurare un KMS predefinito per Data Center 2 e Data Center 3.

Tenere presente che non è possibile utilizzare un KMS per i nodi non appliance o per i nodi appliance che non hanno attivato l'impostazione **Node Encryption** durante l'installazione.



Cosa succede quando si ruota una chiave?

Come Best practice per la sicurezza, è necessario effettuare periodicamente "ruotare la chiave di crittografia" Utilizzato da ciascun KMS configurato.

Quando è disponibile la nuova versione della chiave:

- Viene distribuito automaticamente ai nodi appliance crittografati nel sito o nei siti associati al KMS. La distribuzione deve avvenire entro un'ora dalla rotazione della chiave.
- Se il nodo dell'appliance crittografato non è in linea quando viene distribuita la nuova versione della chiave, il nodo riceverà la nuova chiave non appena verrà riavviato.
- Se la nuova versione della chiave non può essere utilizzata per crittografare i volumi dell'appliance per qualsiasi motivo, viene attivato l'avviso **rotazione chiave di crittografia KMS non riuscita** per il nodo dell'appliance. Potrebbe essere necessario contattare il supporto tecnico per ottenere assistenza nella risoluzione di questo avviso.

È possibile riutilizzare un nodo appliance dopo averlo crittografato?

Se è necessario installare un'appliance crittografata in un altro sistema StorageGRID, è necessario prima decommissionare il nodo Grid per spostare i dati degli oggetti in un altro nodo. Quindi, è possibile utilizzare il programma di installazione dell'appliance StorageGRID per "Cancellare la configurazione KMS". La

cancellazione della configurazione KMS disattiva l'impostazione **crittografia nodo** e rimuove l'associazione tra il nodo appliance e la configurazione KMS per il sito StorageGRID.

> Senza l'accesso alla chiave di crittografia KMS, i dati che rimangono sull'appliance non possono più essere utilizzati e bloccati in modo permanente.

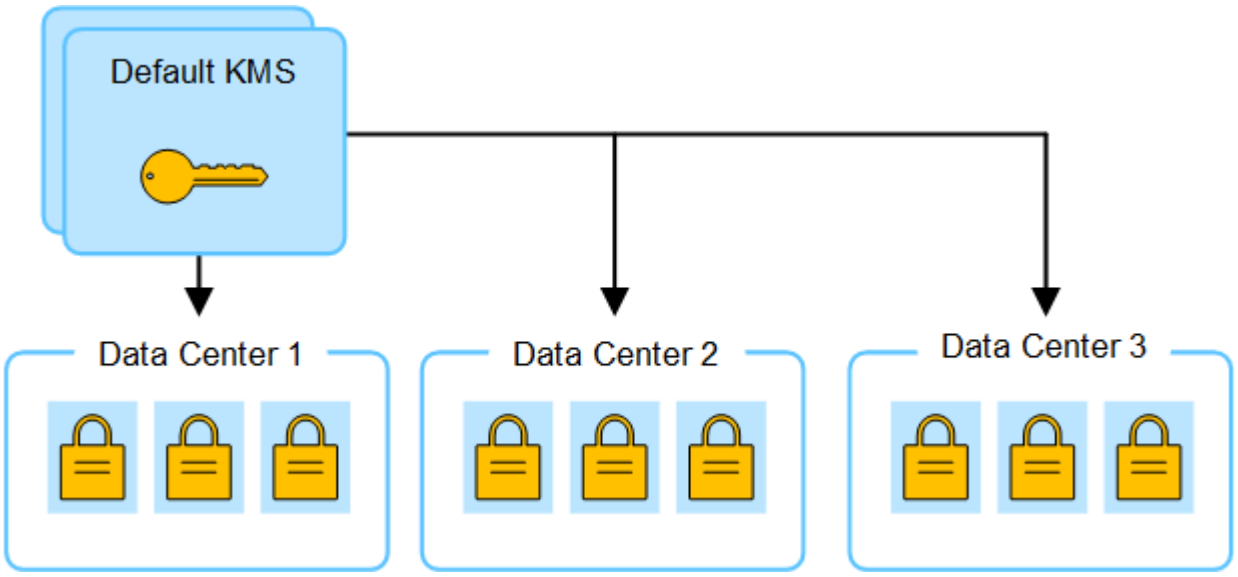
Considerazioni per la modifica del KMS per un sito

Ciascun server di gestione delle chiavi (KMS) o cluster KMS fornisce una chiave di crittografia a tutti i nodi appliance di un singolo sito o di un gruppo di siti. Se è necessario modificare il KMS utilizzato per un sito, potrebbe essere necessario copiare la chiave di crittografia da un KMS all'altro.

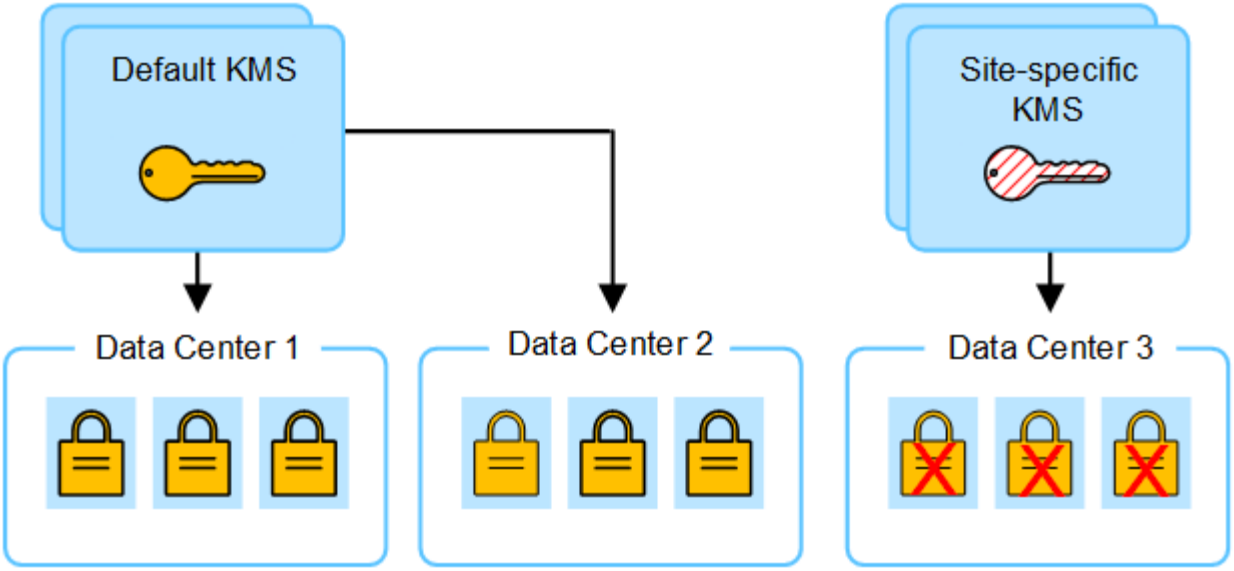
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi appliance precedentemente crittografati in quel sito possano essere decifrati utilizzando la chiave memorizzata nel nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia dal KMS originale al nuovo KMS. È necessario assicurarsi che il KMS disponga della chiave corretta per decrittare i nodi crittografati dell'appliance nel sito.

Ad esempio:

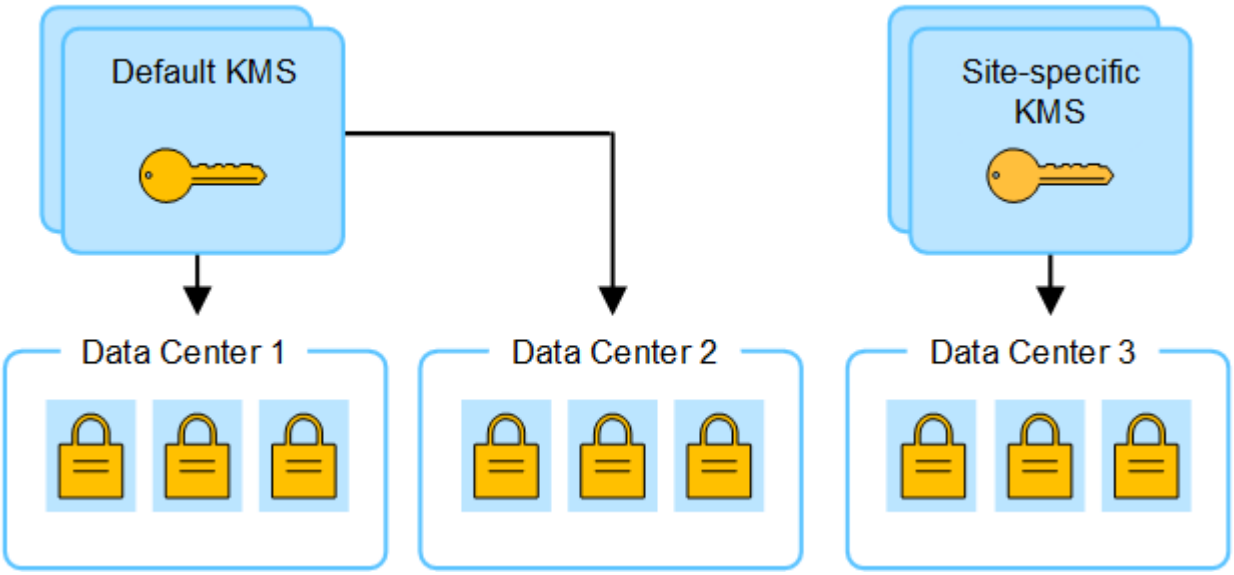
1. Inizialmente, viene configurato un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi appliance con l'impostazione **Node Encryption** attivata si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi dell'appliance in tutti i siti. La stessa chiave deve essere utilizzata anche per decrittare tali appliance.



3. Si decide di aggiungere un KMS specifico del sito per un sito (data center 3 nella figura). Tuttavia, poiché i nodi dell'appliance sono già crittografati, si verifica un errore di convalida quando si tenta di salvare la configurazione per il KMS specifico del sito. L'errore si verifica perché il KMS specifico del sito non dispone della chiave corretta per decrittare i nodi in quel sito.



4. Per risolvere il problema, copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Tecnicamente, si copia la chiave originale in una nuova chiave con lo stesso alias. La chiave originale diventa una versione precedente della nuova chiave). Il KMS specifico del sito dispone ora della chiave corretta per decrittare i nodi dell'appliance nel data center 3, in modo che possa essere salvato in StorageGRID.



Casi di utilizzo per la modifica del KMS utilizzato per un sito

La tabella riassume i passaggi necessari per i casi più comuni di modifica del KMS per un sito.

Caso d'utilizzo per la modifica del KMS di un sito	Passaggi richiesti
Si dispone di una o più voci KMS specifiche del sito e si desidera utilizzarne una come KMS predefinito.	Modificare il KMS specifico del sito. Nel campo **Gestisci chiavi per**, selezionare **Siti non gestiti da un altro KMS (KMS predefinito)**. Il KMS specifico del sito verrà ora utilizzato come KMS predefinito. Si applica a tutti i siti che non dispongono di un KMS dedicato. "Modifica di un server di gestione delle chiavi (KMS)"
Si dispone di un KMS predefinito e si aggiunge un nuovo sito in un'espansione. Non si desidera utilizzare il KMS predefinito per il nuovo sito.	1. Se i nodi dell'appliance nel nuovo sito sono già stati crittografati con il KMS predefinito, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS predefinito a un nuovo KMS. 2. Utilizzando Grid Manager, aggiungere il nuovo KMS e selezionare il sito. "Aggiunta di un server di gestione delle chiavi (KMS)"
Si desidera che il KMS di un sito utilizzi un server diverso.	1. Se i nodi dell'appliance nel sito sono già stati crittografati dal KMS esistente, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS esistente al nuovo KMS. 2. Utilizzando Grid Manager, modificare la configurazione KMS esistente e inserire il nuovo nome host o indirizzo IP. "Aggiunta di un server di gestione delle chiavi (KMS)"

Configurare StorageGRID come client nel KMS

È necessario configurare StorageGRID come client per ogni server di gestione delle chiavi esterno o cluster KMS prima di poter aggiungere KMS a StorageGRID.

Queste istruzioni si applicano a Thales CipherTrust Manager e Hashicorp Vault. Per un elenco dei prodotti e delle versioni supportate, utilizzare "Tool di matrice di interoperabilità NetApp (IMT)".

Fasi

1. Dal software KMS, creare un client StorageGRID per ogni cluster KMS o KMS che si intende utilizzare.

   Ogni KMS gestisce una singola chiave di crittografia per i nodi delle appliance StorageGRID in un singolo sito o in un gruppo di siti.

2. creare una chiave utilizzando uno dei due metodi seguenti:
   - Utilizzare la pagina di gestione delle chiavi del prodotto KMS. Creare una chiave di crittografia AES per ogni cluster KMS o KMS.

     La chiave di crittografia deve essere 2,048 bit o superiore e deve essere esportabile.

   - Chiedere a StorageGRID di creare la chiave. Viene richiesto quando si esegue il test e si salva dopo "caricamento dei certificati client".

3. Registrare le seguenti informazioni per ciascun cluster KMS o KMS.

   Queste informazioni sono necessarie quando si aggiunge il KMS a StorageGRID:

   - Nome host o indirizzo IP per ciascun server.
   - Porta KMIP utilizzata dal KMS.
   - Alias chiave per la chiave di crittografia nel KMS.

4. Per ogni cluster KMS o KMS, ottenere un certificato server firmato da un'autorità di certificazione (CA) o un bundle di certificati che contenga ciascuno dei file di certificato CA con codifica PEM, concatenati nell'ordine della catena di certificati.

   Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

   - Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64.
   - Il campo Subject alternative Name (SAN) in ciascun certificato del server deve includere il nome di dominio completo (FQDN) o l'indirizzo IP a cui StorageGRID si connetterà.

     > Quando si configura il KMS in StorageGRID, è necessario immettere gli stessi FQDN o indirizzi IP nel campo **Nome host**.

   - Il certificato del server deve corrispondere al certificato utilizzato dall'interfaccia KMIP del KMS, che in genere utilizza la porta 5696.

5. Ottenere il certificato del client pubblico rilasciato a StorageGRID dal KMS esterno e la chiave privata per il certificato del client.

   Il certificato client consente a StorageGRID di autenticarsi nel KMS.

Aggiunta di un server di gestione delle chiavi (KMS)

Utilizzare la procedura guidata del server di gestione delle chiavi StorageGRID per aggiungere ogni cluster KMS o KMS.

Prima di iniziare

- Hai esaminato il "considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi".
- Lo hai fatto "StorageGRID configurato come client nel KMS"E si dispone delle informazioni necessarie per ogni cluster KMS o KMS.
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

Se possibile, configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS. Se si crea prima il KMS predefinito, tutte le appliance crittografate con nodo nella griglia verranno crittografate con il KMS predefinito. Se si desidera creare un KMS specifico del sito in un secondo momento, è necessario prima copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Vedere "Considerazioni per la modifica del KMS per un sito" per ulteriori informazioni.

Fase 1: Dettagli DI KMS

Nella fase 1 (dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono forniti dettagli sul cluster KMS o KMS.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) con la scheda Configuration details (Dettagli di configurazione) selezionata.

2. Selezionare **Crea**.

   Viene visualizzata la fase 1 (dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi).

3. Immettere le seguenti informazioni per il KMS e il client StorageGRID configurati in tale KMS.

Campo	Descrizione
NOME DEL KM	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome della chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri. **Nota**: Se non è stata creata una chiave utilizzando il prodotto KMS, verrà richiesto di fare in modo che StorageGRID crei la chiave.
Gestisce le chiavi per	Il sito StorageGRID che sarà associato a questo KMS. Se possibile, è necessario configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS. • Selezionare un sito se il KMS gestirà le chiavi di crittografia per i nodi dell'appliance in un sito specifico. • Selezionare **Siti non gestiti da un altro KMS (KMS predefinito)** per configurare un KMS predefinito che si applicherà a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti nelle espansioni successive. **Nota:** Quando si salva la configurazione KMS, si verifica Un errore di convalida se si seleziona un sito precedentemente crittografato dal KMS predefinito ma non si fornisce la versione corrente della chiave di crittografia originale al nuovo KMS.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.

Campo	Descrizione
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. **Nota:** il campo Subject alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server di un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Add another hostname** (Aggiungi un altro nome host) per aggiungere un nome host per ciascun server del cluster.
5. Selezionare **continua**.

Fase 2: Caricare il certificato del server

Nella fase 2 (carica certificato server) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), viene caricato il certificato del server (o bundle di certificati) per il KMS. Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

Fasi

1. Dal **passaggio 2 (carica certificato server)**, individuare la posizione del certificato server o del bundle di certificati salvato.
2. Caricare il file del certificato.

   Vengono visualizzati i metadati del certificato del server.

   > Se hai caricato un bundle di certificati, i metadati di ciascun certificato vengono visualizzati nella relativa scheda.

3. Selezionare **continua**.

Fase 3: Caricare i certificati client

Nella fase 3 (carica certificati client) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono caricati il certificato client e la chiave privata del certificato client. Il certificato client consente a StorageGRID di autenticarsi nel KMS.

Fasi

1. Dal **passaggio 3 (carica certificati client)**, individuare la posizione del certificato client.
2. Caricare il file di certificato del client.

   Vengono visualizzati i metadati del certificato client.

3. Individuare la posizione della chiave privata per il certificato client.
4. Caricare il file della chiave privata.
5. Selezionare **Test e salvare**.

   Se una chiave non esiste, viene richiesto di crearne una da StorageGRID.

   Vengono verificate le connessioni tra il server di gestione delle chiavi e i nodi dell'appliance. Se tutte le connessioni sono valide e la chiave corretta viene trovata nel KMS, il nuovo server di gestione delle chiavi

viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.

> Subito dopo aver aggiunto un KMS, lo stato del certificato nella pagina Server gestione chiavi viene visualizzato come Sconosciuto. Per ottenere lo stato effettivo di ciascun certificato, StorageGRID potrebbe impiegare fino a 30 minuti. È necessario aggiornare il browser Web per visualizzare lo stato corrente.

6. Se viene visualizzato un messaggio di errore quando si seleziona **Test and Save** (verifica e salva), rivedere i dettagli del messaggio e selezionare **OK**.

   Ad esempio, se un test di connessione non riesce, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

7. Se si desidera salvare la configurazione corrente senza verificare la connessione esterna, selezionare **Force Save** (forza salvataggio).

   > Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

8. Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.

   La configurazione KMS viene salvata ma la connessione al KMS non viene verificata.

Gestire un KMS

La gestione di un server di gestione delle chiavi (KMS) comporta la visualizzazione o la modifica dei dettagli, la gestione dei certificati, la visualizzazione dei nodi crittografati e la rimozione di un KMS quando non è più necessario.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "autorizzazione di accesso richiesta".

Visualizza i dettagli di KMS

È possibile visualizzare informazioni su ciascun server di gestione delle chiavi (KMS) nel sistema StorageGRID, inclusi i dettagli delle chiavi e lo stato corrente dei certificati server e client.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina del server di gestione delle chiavi con le seguenti informazioni:

   - La scheda Dettagli configurazione elenca tutti i server di gestione delle chiavi configurati.
   - La scheda nodi crittografati elenca tutti i nodi con la crittografia dei nodi abilitata.

2. Per visualizzare i dettagli di un KMS specifico ed eseguire operazioni su tale KMS, selezionare il nome del KMS. Nella pagina dei dettagli del KMS sono elencate le seguenti informazioni:

Campo	Descrizione
Gestisce le chiavi per	Il sito StorageGRID associato al KMS. Questo campo visualizza il nome di un sito StorageGRID specifico o **Siti non gestiti da un altro KMS (KMS predefinito).**
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. Se è presente un cluster di due server di gestione delle chiavi, vengono elencati il nome di dominio completo o l'indirizzo IP di entrambi i server. Se in un cluster sono presenti più di due server di gestione delle chiavi, viene elencato il nome di dominio completo o l'indirizzo IP del primo KMS insieme al numero di server di gestione delle chiavi aggiuntivi nel cluster. Ad esempio: `10.10.10.10 and 10.10.10.11` oppure `10.10.10.10 and 2 others`. Per visualizzare tutti i nomi host in un cluster, selezionare un KMS e selezionare **Modifica** o **azioni** > **Modifica**.

3. Selezionare una scheda nella pagina dei dettagli KMS per visualizzare le seguenti informazioni:

Scheda	Campo	Descrizione
Dettagli chiave	Nome della chiave	L'alias della chiave per il client StorageGRID nel KMS.
UID chiave	L'identificatore univoco dell'ultima versione della chiave.	Ultima modifica
La data e l'ora dell'ultima versione della chiave.	Certificato del server	Metadati
I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.	Certificato PEM	Il contenuto del file PEM (privacy Enhanced mail) per il certificato.
Certificato del client	Metadati	I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.

4. tutte le volte che richiesto dalle procedure di sicurezza dell'organizzazione, selezionare **Rotate key**, oppure utilizzare il software KMS, per creare una nuova versione della chiave.

   Quando la rotazione della chiave ha esito positivo, i campi UID chiave e ultima modifica vengono aggiornati.

Se si ruota la chiave di crittografia utilizzando il software KMS, ruotarla dall'ultima versione utilizzata della chiave a una nuova versione della stessa chiave. Non ruotare su una chiave completamente diversa.

Non tentare mai di ruotare una chiave cambiando il nome della chiave (alias) per il KMS. StorageGRID richiede che tutte le versioni delle chiavi utilizzate in precedenza (così come quelle future) siano accessibili dal KMS con lo stesso alias della chiave. Se si modifica l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittare i dati.

Gestire i certificati

Risolvere tempestivamente eventuali problemi relativi ai certificati server o client. Se possibile, sostituire i certificati prima che scadano.

Per mantenere l'accesso ai dati, è necessario risolvere al più presto eventuali problemi di certificato.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.
2. Nella tabella, esaminare il valore della scadenza del certificato per ogni KMS.
3. Se la scadenza del certificato per qualsiasi KMS è sconosciuta, attendere fino a 30 minuti, quindi aggiornare il browser Web.
4. Se la colonna scadenza certificato indica che un certificato è scaduto o è prossimo alla scadenza, selezionare il KMS per accedere alla pagina dei dettagli del KMS.
   a. Selezionare **certificato server** e verificare il valore del campo "scade il".
   b. Per sostituire il certificato, selezionare **Modifica certificato** per caricare un nuovo certificato.
   c. Ripetere questi passaggi secondari e selezionare **Client certificate** invece di Server certificate (certificato server).
5. Quando vengono attivati gli avvisi **scadenza certificato CA KMS**, **scadenza certificato client KMS** e **scadenza certificato server KMS**, annotare la descrizione di ciascun avviso ed eseguire le azioni consigliate.

Per ottenere gli aggiornamenti alla scadenza del certificato, StorageGRID potrebbe richiedere fino a 30 minuti. Aggiornare il browser Web per visualizzare i valori correnti.

Visualizzare i nodi crittografati

È possibile visualizzare informazioni sui nodi appliance nel sistema StorageGRID per i quali è stata attivata l'impostazione **crittografia nodo**.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina Key Management Server (Server di gestione delle chiavi). La scheda Dettagli configurazione mostra tutti i server di gestione delle chiavi configurati.

2. Nella parte superiore della pagina, selezionare la scheda **nodi crittografati**.

La scheda nodi crittografati elenca i nodi appliance nel sistema StorageGRID con l'impostazione **crittografia nodo** attivata.

3. Esaminare le informazioni contenute nella tabella per ciascun nodo appliance.

Colonna	Descrizione
Nome del nodo	Il nome del nodo appliance.
Tipo di nodo	Il tipo di nodo: Storage, Admin o Gateway.
Sito	Il nome del sito StorageGRID in cui è installato il nodo.
NOME DEL KM	Il nome descrittivo del KMS utilizzato per il nodo. Se non è elencato alcun KMS, selezionare la scheda Dettagli di configurazione per aggiungere un KMS. "Aggiunta di un server di gestione delle chiavi (KMS)"
UID chiave	ID univoco della chiave di crittografia utilizzata per crittografare e decrittare i dati sul nodo dell'appliance. Per visualizzare un UID chiave completo, selezionare il testo. Un trattino (--) indica che l'UID della chiave non è noto, probabilmente a causa di un problema di connessione tra il nodo dell'appliance e il KMS.
Stato	Lo stato della connessione tra il KMS e il nodo dell'appliance. Se il nodo è connesso, l'indicatore data e ora viene aggiornato ogni 30 minuti. L'aggiornamento dello stato di connessione può richiedere alcuni minuti dopo le modifiche della configurazione KMS. **Nota:** aggiornare il browser Web per visualizzare i nuovi valori.

4. Se la colonna Status (Stato) indica un problema KMS, risolverlo immediatamente.

   Durante le normali operazioni KMS, lo stato sarà **connesso a KMS**. Se un nodo viene disconnesso dalla rete, viene visualizzato lo stato di connessione del nodo (amministrativamente inattivo o Sconosciuto).

   Gli altri messaggi di stato corrispondono agli avvisi StorageGRID con gli stessi nomi:

   - Impossibile caricare la configurazione KMS
   - Errore di connettività KMS
   - Nome chiave di crittografia KMS non trovato
   - Rotazione della chiave di crittografia KMS non riuscita
   - La chiave KMS non è riuscita a decrittare un volume dell'appliance
   - KMS non configurato

   Eseguire le azioni consigliate per questi avvisi.

È necessario affrontare immediatamente qualsiasi problema per garantire la completa protezione dei dati.

Modificare un KMS

Potrebbe essere necessario modificare la configurazione di un server di gestione delle chiavi, ad esempio, se un certificato sta per scadere.

Prima di iniziare

- Se si prevede di aggiornare il sito selezionato per un KMS, è stata esaminata la "Considerazioni per la modifica del KMS per un sito".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

2. Selezionare il KMS che si desidera modificare e selezionare **azioni** > **Modifica**.

   Puoi anche modificare un KMS selezionando il nome del KMS nella tabella e selezionando **Edit** nella pagina dei dettagli del KMS.

3. Facoltativamente, aggiornare i dettagli nel **Passo 1 (dettagli KMS)** della procedura guidata Modifica un server di gestione delle chiavi.

Campo	Descrizione
NOME DEL KM	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome della chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri. È sufficiente modificare il nome della chiave solo in rari casi. Ad esempio, è necessario modificare il nome della chiave se l'alias viene rinominato in KMS o se tutte le versioni della chiave precedente sono state copiate nella cronologia delle versioni del nuovo alias.
Gestisce le chiavi per	Se si sta modificando un KMS specifico del sito e non si dispone già di un KMS predefinito, selezionare **Sites Not Managed by another KMS (default KMS)** (Siti non gestiti da un altro KMS (default KMS)*). Questa selezione converte un KMS specifico del sito nel KMS predefinito, che verrà applicato a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti in un'espansione. **Nota:** se stai modificando un KMS specifico del sito, non puoi selezionare un altro sito. Se stai modificando il KMS predefinito, non puoi selezionare un sito specifico.

Campo	Descrizione
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. **Nota:** il campo Subject alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server di un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Add another hostname** (Aggiungi un altro nome host) per aggiungere un nome host per ciascun server del cluster.
5. Selezionare **continua**.

   Viene visualizzata la fase 2 (carica certificato server) della procedura guidata Modifica un server di gestione delle chiavi.

6. Se è necessario sostituire il certificato del server, selezionare **Sfoglia** e caricare il nuovo file.
7. Selezionare **continua**.

   Viene visualizzata la fase 3 (carica certificati client) della procedura guidata Modifica un server di gestione delle chiavi.

8. Se è necessario sostituire il certificato client e la chiave privata del certificato client, selezionare **Browse** (Sfoglia) e caricare i nuovi file.
9. Selezionare **Test e salvare**.

   Vengono testate le connessioni tra il server di gestione delle chiavi e tutti i nodi di appliance con crittografia a nodo nei siti interessati. Se tutte le connessioni dei nodi sono valide e la chiave corretta viene trovata nel KMS, il server di gestione delle chiavi viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.

10. Se viene visualizzato un messaggio di errore, esaminare i dettagli del messaggio e selezionare **OK**.

    Ad esempio, se il sito selezionato per questo KMS è già gestito da un altro KMS o se un test di connessione non ha avuto esito positivo, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

11. Se è necessario salvare la configurazione corrente prima di risolvere gli errori di connessione, selezionare **Imponi salvataggio**.

    > Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

    La configurazione KMS viene salvata.

12. Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.

La configurazione del KMS viene salvata, ma la connessione al KMS non viene verificata.

Rimozione di un server di gestione delle chiavi (KMS)

In alcuni casi, potrebbe essere necessario rimuovere un server di gestione delle chiavi. Ad esempio, è possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato.

Prima di iniziare

- Hai esaminato il "considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

È possibile rimuovere un KMS nei seguenti casi:

- È possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato o se il sito non include nodi appliance con crittografia del nodo attivata.
- È possibile rimuovere il KMS predefinito se esiste già un KMS specifico del sito per ogni sito che ha nodi appliance con crittografia del nodo attivata.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

2. Selezionare il KMS che si desidera rimuovere e selezionare **azioni** > **Rimuovi**.

   Puoi anche rimuovere un KMS selezionando il nome del KMS nella tabella e selezionando **Remove** dalla pagina dei dettagli del KMS.

3. Verificare che quanto segue sia vero:
   - Si sta rimuovendo un KMS specifico del sito per un sito che non dispone di un nodo appliance con crittografia del nodo attivata.
   - Si sta rimuovendo il KMS predefinito, ma esiste già un KMS specifico del sito per ogni sito con crittografia del nodo.
4. Selezionare **Sì**.

   La configurazione KMS viene rimossa.

Gestire le impostazioni del proxy

Configurare il proxy di archiviazione

Se si utilizzano servizi di piattaforma o Cloud Storage Pool, è possibile configurare un proxy non trasparente tra i nodi di storage e gli endpoint S3 esterni. Ad esempio, potrebbe essere necessario un proxy non trasparente per consentire l'invio dei messaggi dei servizi della piattaforma a endpoint esterni, ad esempio un endpoint su Internet.

Le impostazioni proxy di storage configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

È possibile configurare le impostazioni per un singolo proxy di archiviazione.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **Impostazioni proxy**.
2. Nella scheda **archiviazione**, selezionare la casella di controllo **Abilita proxy di archiviazione**.
3. Selezionare il protocollo per il proxy di archiviazione.
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, inserire la porta utilizzata per connettersi al server proxy.

   Lasciare vuoto questo campo per utilizzare la porta predefinita per il protocollo: 80 per HTTP o 1080 per SOCKS5.

6. Selezionare **Salva**.

   Dopo il salvataggio del proxy di storage, è possibile configurare e testare nuovi endpoint per i servizi della piattaforma o i pool di cloud storage.

   Le modifiche del proxy possono richiedere fino a 10 minuti.

7. Controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma da StorageGRID non vengano bloccati.
8. Se è necessario disattivare un proxy di archiviazione, deselezionare la casella di controllo e selezionare **Salva**.

Configurare le impostazioni del proxy amministratore

Se si inviano pacchetti AutoSupport utilizzando HTTP o HTTPS, è possibile configurare un server proxy non trasparente tra i nodi Admin e il supporto tecnico (AutoSupport).

Per ulteriori informazioni su AutoSupport, vedere "Configurare AutoSupport".

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

È possibile configurare le impostazioni per un singolo proxy amministratore.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **Impostazioni proxy**.

Viene visualizzata la pagina Impostazioni proxy. Per impostazione predefinita, l'opzione Storage (archiviazione) è selezionata nel menu Tab (scheda).

2. Selezionare la scheda **Ammin**.
3. Selezionare la casella di controllo **Enable Admin Proxy** (attiva proxy amministratore).
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Inserire la porta utilizzata per la connessione al server proxy.
6. Facoltativamente, immettere un nome utente e una password per il server proxy.

   Se il server proxy non richiede un nome utente o una password, lasciare vuoti questi campi.

7. Selezionare una delle seguenti opzioni:

   - Se si desidera proteggere la connessione al proxy amministratore, selezionare **verifica certificato proxy**. Caricare un pacchetto CA per verificare l'autenticità dei certificati SSL presentati dal server proxy amministratore.

     AutoSupport on Demand, e-Series AutoSupport tramite StorageGRID e la determinazione del percorso di aggiornamento nella pagina dell'upgrade della StorageGRID non funzionano se viene verificato un certificato proxy.

   Dopo aver caricato il pacchetto CA, vengono visualizzati i relativi metadati.

   - Se non si desidera convalidare i certificati quando si comunica con il server proxy dell'amministratore, selezionare **non verificare il certificato proxy**.

8. Selezionare **Salva**.

   Dopo aver salvato il proxy dell'amministratore, viene configurato il server proxy tra i nodi Admin e il supporto tecnico.

   Le modifiche del proxy possono richiedere fino a 10 minuti.

9. Se è necessario disattivare il proxy amministratore, deselezionare la casella di controllo **Abilita proxy amministratore**, quindi selezionare **Salva**.

Firewall di controllo

Controllare l'accesso al firewall esterno

È possibile aprire o chiudere porte specifiche sul firewall esterno.

È possibile controllare l'accesso alle interfacce utente e alle API sui nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche sul firewall esterno. Ad esempio, è possibile impedire ai tenant di connettersi a Grid Manager dal firewall, oltre a utilizzare altri metodi per controllare l'accesso al sistema.

Se si desidera configurare il firewall interno di StorageGRID, vedere "Configurare il firewall interno".

Porta	Descrizione	Se la porta è aperta…
443	Porta HTTPS predefinita per i nodi di amministrazione	I browser Web e i client API di gestione possono accedere a Grid Manager, Grid Management API, Tenant Manager e Tenant Management API. **Nota:** la porta 443 viene utilizzata anche per il traffico interno.
8443	Porta Grid Manager limitata sui nodi di amministrazione	• I browser Web e i client API di gestione possono accedere a Grid Manager e all'API di Grid Management utilizzando HTTPS. • I browser Web e i client API di gestione non possono accedere a tenant Manager o all'API di gestione tenant. • Le richieste di contenuto interno verranno rifiutate.
9443	Porta limitata di Tenant Manager sui nodi di amministrazione	• I browser Web e i client API di gestione possono accedere a Tenant Manager e all'API di gestione tenant utilizzando HTTPS. • I browser Web e i client API di gestione non possono accedere a Grid Manager o all'API di Grid Management. • Le richieste di contenuto interno verranno rifiutate.

Single Sign-on (SSO) non è disponibile sulle porte limitate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443).

Informazioni correlate

- "Accedi a Grid Manager"
- "Creare un account tenant"
- "Comunicazioni esterne"

Gestire i controlli firewall interni

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della rete consentendo di controllare l'accesso alla rete. Utilizzare il firewall per impedire l'accesso alla rete su tutte le porte, ad eccezione di quelle necessarie per l'implementazione della griglia specifica. Le modifiche apportate alla configurazione nella pagina di controllo Firewall vengono distribuite a ciascun nodo.

Utilizzare le tre schede della pagina di controllo Firewall per personalizzare l'accesso necessario per la griglia.

- **Privileged address list**: Utilizzare questa scheda per consentire l'accesso selezionato alle porte chiuse. È possibile aggiungere indirizzi IP o sottoreti nella notazione CIDR che possono accedere alle porte chiuse utilizzando la scheda Manage external access (Gestisci accesso esterno).

- **Gestisci accesso esterno**: Utilizzare questa scheda per chiudere le porte aperte per impostazione predefinita o riaprire le porte chiuse in precedenza.
- **Untrusted Client Network**: Utilizzare questa scheda per specificare se un nodo considera attendibile il traffico in entrata dalla rete client.

  Le impostazioni di questa scheda sovrascrivono quelle della scheda Gestisci accesso esterno.

  - Un nodo con una rete client non attendibile accetta solo le connessioni sulle porte endpoint del bilanciamento del carico configurate su quel nodo (endpoint globali, di interfaccia di nodo e di tipo di nodo).
  - Le porte endpoint del bilanciamento del carico *sono le uniche porte aperte* sulle reti client non attendibili, indipendentemente dalle impostazioni nella scheda Gestisci reti esterne.
  - Se attendibili, tutte le porte aperte nella scheda Manage external access (Gestisci accesso esterno) sono accessibili, così come tutti gli endpoint del bilanciamento del carico aperti nella rete client.

> Le impostazioni effettuate in una scheda possono influire sulle modifiche di accesso apportate in un'altra scheda. Verificare le impostazioni di tutte le schede per assicurarsi che la rete funzioni nel modo previsto.

Per configurare i controlli firewall interni, vedere "Configurare i controlli firewall".

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere "Controllare l'accesso al firewall esterno".

Elenco degli indirizzi privilegiati e schede di gestione degli accessi esterni

La scheda Privileged address list (elenco indirizzi privilegiati) consente di registrare uno o più indirizzi IP ai quali viene concesso l'accesso alle porte della griglia chiuse. La scheda Manage external access (Gestisci accesso esterno) consente di chiudere l'accesso esterno alle porte esterne selezionate o a tutte le porte esterne aperte (le porte esterne sono porte accessibili per impostazione predefinita dai nodi non grid). Queste due schede spesso possono essere utilizzate insieme per personalizzare l'esatto accesso di rete necessario per la griglia.

> Per impostazione predefinita, gli indirizzi IP privilegiati non dispongono dell'accesso alla porta della griglia interna.

Esempio 1: Utilizzare un host di collegamento per le attività di manutenzione

Si supponga di voler utilizzare un host jump (un host con protezione avanzata) per l'amministrazione di rete. È possibile utilizzare questi passaggi generali:

1. Utilizzare la scheda Privileged address list (elenco indirizzi privilegiati) per aggiungere l'indirizzo IP dell'host di collegamento.
2. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte.

> Aggiungere l'indirizzo IP privilegiato prima di bloccare le porte 443 e 8443. Tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, tutte le porte esterne sul nodo di amministrazione nella griglia verranno

bloccate per tutti gli host, ad eccezione dell'host di collegamento. È quindi possibile utilizzare l'host jump per eseguire attività di manutenzione sulla griglia in modo più sicuro.

Esempio 2: Bloccare le porte sensibili

Si supponga di voler bloccare le porte sensibili e il servizio su tale porta (ad esempio, SSH sulla porta 22). È possibile utilizzare i seguenti passaggi generali:

1. Utilizzare la scheda Privileged address list (elenco indirizzi con privilegi) per concedere l'accesso solo agli host che devono accedere al servizio.
2. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte.

> Aggiungere l'indirizzo IP con privilegi prima di bloccare l'accesso a tutte le porte assegnate per accedere a Grid Manager e Tenant Manager (le porte preimpostate sono 443 e 8443). Tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, la porta 22 e il servizio SSH saranno disponibili per gli host nell'elenco degli indirizzi privilegiati. A tutti gli altri host verrà negato l'accesso al servizio, indipendentemente dall'interfaccia da cui proviene la richiesta.

Esempio 3: Disabilitare l'accesso ai servizi non utilizzati

A livello di rete, è possibile disattivare alcuni servizi che non si intende utilizzare. Ad esempio, se non si fornisce l'accesso a Swift, attenersi alla seguente procedura generale:

1. Utilizzare il pulsante di commutazione nella scheda Manage external access (Gestisci accesso esterno) per bloccare la porta 18083.
2. Utilizzare l'interruttore sulla scheda Gestisci accesso esterno per bloccare la porta 18085.

Dopo aver salvato la configurazione, Storage Node non consente più la connettività Swift, ma continua a consentire l'accesso ad altri servizi su porte sbloccate.

Scheda Untrusted Client Networks

Se si utilizza una rete client, è possibile proteggere StorageGRID da attacchi ostili accettando il traffico client in entrata solo su endpoint configurati esplicitamente.

Per impostazione predefinita, la rete client su ciascun nodo della griglia è *trusted*. Ovvero, per impostazione predefinita, StorageGRID considera attendibili le connessioni in entrata a ciascun nodo della griglia su tutti "porte esterne disponibili".

È possibile ridurre la minaccia di attacchi ostili al sistema StorageGRID specificando che la rete client di ciascun nodo è *non 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. Vedere "Configurare gli endpoint del bilanciamento del carico" e. "Configurare i controlli firewall".

Esempio 1: Il nodo gateway accetta solo richieste HTTPS S3

Si supponga che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste HTTPS S3. Eseguire le seguenti operazioni generali:

1. Dal "Endpoint del bilanciamento del carico" Configurare un endpoint di bilanciamento del carico per S3 su HTTPS sulla porta 443.
2. Dalla pagina di controllo Firewall, selezionare Untrusted (non attendibile) per specificare che la rete client sul nodo gateway non è attendibile.

Dopo aver salvato la configurazione, tutto il traffico in entrata sulla rete client del nodo gateway viene interrotto, ad eccezione delle richieste HTTPS S3 sulla porta 443 e delle richieste ICMP echo (ping).

Esempio 2: Storage Node invia richieste di servizi della piattaforma S3

Si supponga di voler attivare il traffico dei servizi della piattaforma S3 in uscita da un nodo di storage, ma di voler impedire qualsiasi connessione in entrata a tale nodo di storage sulla rete client. Eseguire questa fase generale:

- Dalla scheda Untrusted Client Networks (reti client non attendibili) della pagina di controllo Firewall, indicare che la rete client nel nodo di storage non è attendibile.

Dopo aver salvato la configurazione, il nodo di storage non accetta più alcun traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita verso destinazioni di servizi della piattaforma configurate.

Esempio 3: Limitazione dell'accesso a Grid Manager a una subnet

Si supponga di voler consentire l'accesso a Grid Manager solo su una subnet specifica. Attenersi alla seguente procedura:

1. Collegare la rete client dei nodi di amministrazione alla subnet.
2. Utilizzare la scheda Untrusted Client Network (rete client non attendibile) per configurare la rete client come non attendibile.
3. Quando si crea un endpoint per il bilanciamento del carico dell'interfaccia di gestione, immettere la porta e selezionare l'interfaccia di gestione a cui la porta accede.
4. Selezionare **Sì** per la rete client non attendibile.
5. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte esterne (con o senza indirizzi IP privilegiati impostati per gli host esterni alla subnet).

Dopo aver salvato la configurazione, solo gli host della subnet specificata possono accedere a Grid Manager. Tutti gli altri host sono bloccati.

Configurare il firewall interno

È possibile configurare il firewall StorageGRID per controllare l'accesso di rete a porte specifiche sui nodi StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Le informazioni sono state esaminate in "Gestire i controlli firewall" e. "Linee guida per il networking".
- Se si desidera che un nodo Admin o un nodo gateway accetti il traffico in entrata solo su endpoint configurati esplicitamente, sono stati definiti gli endpoint del bilanciamento del carico.

Quando si modifica la configurazione della rete client, le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

A proposito di questa attività

StorageGRID include un firewall interno su ciascun nodo che consente di aprire o chiudere alcune porte sui nodi della griglia. È possibile utilizzare le schede di controllo Firewall per aprire o chiudere le porte aperte per impostazione predefinita in Grid Network, Admin Network e Client Network. È inoltre possibile creare un elenco di indirizzi IP privilegiati che possono accedere alle porte della griglia chiuse. Se si utilizza una rete client, è possibile specificare se un nodo considera attendibile il traffico in entrata dalla rete client ed è possibile configurare l'accesso a porte specifiche sulla rete client.

Limitare il numero di porte aperte agli indirizzi IP esterni alla griglia solo a quelle assolutamente necessarie migliora la sicurezza della griglia. Utilizzare le impostazioni di ciascuna delle tre schede di controllo del firewall per assicurarsi che siano aperte solo le porte necessarie.

Per ulteriori informazioni sull'utilizzo dei controlli firewall, inclusi esempi, vedere "Gestire i controlli firewall".

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere "Controllare l'accesso al firewall esterno".

Accedere ai controlli firewall

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Firewall control**.

   Le tre schede di questa pagina sono descritte nella "Gestire i controlli firewall".

2. Selezionare una scheda qualsiasi per configurare i controlli del firewall.

   È possibile utilizzare queste schede in qualsiasi ordine. Le configurazioni impostate su una scheda non limitano le operazioni che è possibile eseguire sulle altre schede; tuttavia, le modifiche alla configurazione apportate su una scheda potrebbero modificare il comportamento delle porte configurate su altre schede.

Elenco di indirizzi con privilegi

La scheda elenco indirizzi privilegiati consente agli host di accedere alle porte chiuse per impostazione predefinita o chiuse dalle impostazioni della scheda Gestisci accesso esterno.

Per impostazione predefinita, gli indirizzi IP e le subnet privilegiati non dispongono di accesso alla rete interna. Inoltre, gli endpoint del bilanciamento del carico e le porte aggiuntive aperte nella scheda Privileged address list (elenco indirizzi con privilegi) sono accessibili anche se bloccati nella scheda Manage external access (Gestisci accesso esterno).

Le impostazioni della scheda elenco indirizzi privilegiati non possono sostituire quelle della scheda rete client non attendibile.

Fasi

1. Nella scheda Privileged address list (elenco indirizzi privilegiati), inserire l'indirizzo o la subnet IP che si desidera concedere l'accesso alle porte chiuse.
2. Facoltativamente, selezionare **Aggiungi un altro indirizzo IP o subnet nella notazione CIDR** per aggiungere altri client con privilegi.

Aggiungere il minor numero possibile di indirizzi all'elenco dei privilegi.

3. Facoltativamente, selezionare **Allow Privileged IP address to access StorageGRID internal ports** (Consenti indirizzi IP privilegiati per l'accesso alle porte interne di Vedere "Porte interne StorageGRID".

Questa opzione rimuove alcune protezioni per i servizi interni. Se possibile, lasciarlo disattivato.

4. Selezionare **Salva**.

Gestire l'accesso esterno

Quando una porta viene chiusa nella scheda Manage external access (Gestisci accesso esterno), non è possibile accedervi da alcun indirizzo IP non Grid, a meno che non si aggiunga l'indirizzo IP all'elenco degli indirizzi privilegiati. Per impostazione predefinita, è possibile chiudere solo le porte aperte e solo quelle chiuse.

Le impostazioni della scheda Manage external access (Gestisci accesso esterno) non possono sostituire quelle della scheda Untrusted Client Network (rete client non attendibile). Ad esempio, se un nodo non è attendibile, la porta SSH/22 viene bloccata sulla rete client anche se è aperta nella scheda Manage external access (Gestisci accesso esterno). Le impostazioni della scheda Untrusted Client Network (rete client non attendibile) sovrascrivono le porte chiuse (ad esempio 443, 8443, 9443) della rete client.

Fasi

1. Selezionare **Gestisci accesso esterno**.
   La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non griglia) per i nodi della griglia.
2. Configurare le porte che si desidera aprire e chiudere utilizzando le seguenti opzioni:
   - Utilizzare il pulsante di commutazione accanto a ciascuna porta per aprire o chiudere la porta selezionata.
   - Selezionare **Open all displayed ports** (Apri tutte le porte visualizzate) per aprire tutte le porte elencate nella tabella.
   - Selezionare **Chiudi tutte le porte visualizzate** per chiudere tutte le porte elencate nella tabella.

Se si chiudono le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Utilizzare la barra di scorrimento sul lato destro della tabella per verificare di aver visualizzato tutte le porte disponibili. Utilizzare il campo di ricerca per trovare le impostazioni di qualsiasi porta esterna immettendo un numero di porta. È possibile inserire un numero di porta parziale. Ad esempio, se si immette **2**, vengono visualizzate tutte le porte che hanno la stringa "2" come parte del loro nome.

3. Selezionare **Salva**

Rete client non attendibile

Se la rete client di un nodo non è attendibile, il nodo accetta solo il traffico in entrata sulle porte configurate

come endpoint del bilanciamento del carico e, facoltativamente, le porte aggiuntive selezionate in questa scheda. È inoltre possibile utilizzare questa scheda per specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.

> Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

Le modifiche apportate alla configurazione nella scheda **Untrusted Client Network** (rete client non attendibile) sovrascrivono le impostazioni nella scheda **Manage external access** (Gestisci accesso esterno).

Fasi

1. Selezionare **Untrusted Client Network**.
2. Nella sezione Set New Node Default (Imposta nuovo nodo predefinito), specificare l'impostazione predefinita quando si aggiungono nuovi nodi alla griglia in una procedura di espansione.
   - **Trusted** (impostazione predefinita): Quando un nodo viene aggiunto in un'espansione, la sua rete client viene considerata attendibile.
   - **Untrusted**: Quando un nodo viene aggiunto in un'espansione, la sua rete client non è attendibile.

     Se necessario, è possibile tornare a questa scheda per modificare l'impostazione di un nuovo nodo specifico.

     > Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID.
3. Utilizzare le seguenti opzioni per selezionare i nodi che devono consentire le connessioni client solo su endpoint del bilanciamento del carico configurati esplicitamente o su porte selezionate aggiuntive:
   - Selezionare **Untrust on displayed nodes** per aggiungere tutti i nodi visualizzati nella tabella all'elenco Untrusted Client Network (rete client non attendibile).
   - Selezionare **Trust on displayed nodes** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Untrusted Client Network (rete client non attendibile).
   - Utilizzare l'interruttore accanto a ciascun nodo per impostare la rete client come attendibile o non attendibile per il nodo selezionato.

     Ad esempio, è possibile selezionare **Untrust on displayed nodes** per aggiungere tutti i nodi all'elenco Untrusted Client Network (rete client non attendibile), quindi utilizzare il pulsante di attivazione accanto a un singolo nodo per aggiungere tale singolo nodo all'elenco Trusted Client Network (rete client attendibile).

     > Utilizzare la barra di scorrimento sul lato destro della tabella per verificare di aver visualizzato tutti i nodi disponibili. Utilizzare il campo di ricerca per trovare le impostazioni per qualsiasi nodo immettendo il nome del nodo. È possibile immettere un nome parziale. Ad esempio, se si immette un valore **GW**, vengono visualizzati tutti i nodi che hanno la stringa "GW" come parte del loro nome.
4. Selezionare **Salva**.

   Le nuove impostazioni del firewall vengono applicate e applicate immediatamente. Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

Gestire i tenant

Gestire i tenant: Panoramica

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.

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

Cosa sono gli account tenant?

Un account tenant consente di utilizzare l'API REST di S3 (Simple Storage Service) o l'API REST di Swift per memorizzare e recuperare oggetti in un sistema StorageGRID.

Ogni account tenant dispone di gruppi federati o locali, utenti, bucket S3 o container Swift e oggetti.

Gli account tenant possono essere utilizzati per separare gli oggetti memorizzati da diverse entità. Ad esempio, è possibile utilizzare più account tenant per uno dei seguenti casi di utilizzo:

- **Caso d'utilizzo aziendale:** se si amministra un sistema StorageGRID in un'applicazione aziendale, è possibile separare lo storage a oggetti del grid dai diversi reparti dell'organizzazione. In questo caso, è possibile creare account tenant per il reparto Marketing, il reparto Assistenza clienti, il reparto risorse umane e così via.

  Se si utilizza il protocollo client S3, è possibile utilizzare i bucket S3 e le policy bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario utilizzare account tenant. Vedere le istruzioni per l'implementazione "Bucket S3 e policy bucket" per ulteriori informazioni.

- **Caso d'utilizzo del provider di servizi:** se si amministra un sistema StorageGRID come provider di servizi, è possibile separare lo storage a oggetti della griglia dalle diverse entità che affitteranno lo storage sulla griglia. In questo caso, è necessario creare account tenant per la società A, la società B, la società C e così via.

Per ulteriori informazioni, vedere "Utilizzare un account tenant".

Come si crea un account tenant?

Quando si crea un account tenant, si specificano le seguenti informazioni:

- Informazioni di base, tra cui il nome del tenant, il tipo di client (S3 o Swift) e la quota di storage opzionale.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine di identità, utilizzare S3 Select o utilizzare una connessione a federazione di griglie.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione di identità o SSO (Single Sign-on).

Inoltre, è possibile attivare l'impostazione blocco oggetti S3 per il sistema StorageGRID se gli account tenant S3 devono soddisfare i requisiti normativi. Quando S3 Object Lock è attivato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

A cosa serve il tenant manager?

Dopo aver creato l'account tenant, gli utenti tenant possono accedere a tenant Manager per eseguire attività come le seguenti:

- Configurare la federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia)
- Gestire gruppi e utenti
- Utilizza la federazione di grid per il clone dell'account e la replica cross-grid
- Gestire le chiavi di accesso S3
- Creare e gestire i bucket S3
- Utilizzare i servizi della piattaforma S3
- USA S3 Select
- Monitorare l'utilizzo dello storage

Mentre gli utenti del tenant S3 possono creare e gestire chiavi di accesso S3 e bucket con Tenant Manager, devono utilizzare un'applicazione client S3 per acquisire e gestire gli oggetti. Vedere "UTILIZZARE L'API REST S3" per ulteriori informazioni.

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

Creare un account tenant

È necessario creare almeno un account tenant per controllare l'accesso allo storage nel sistema StorageGRID.

I passaggi per la creazione di un account tenant variano in base al tipo di account "federazione delle identità" e. "single sign-on" Sono configurati e se l'account Grid Manager utilizzato per creare l'account tenant appartiene a un gruppo amministrativo con l'autorizzazione di accesso root.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Accesso root o autorizzazione account tenant".
- Se l'account tenant utilizza l'origine dell'identità configurata per Grid Manager e si desidera concedere l'autorizzazione di accesso root per l'account tenant a un gruppo federato, il gruppo federated è stato importato in Grid Manager. Non è necessario assegnare alcuna autorizzazione Grid Manager a questo gruppo di amministratori. Vedere "Gestire i gruppi di amministratori".
- Se si desidera consentire a un tenant S3 di clonare i dati dell'account e replicare gli oggetti bucket in un altro grid utilizzando una connessione a federazione di grid:
  - Lo hai fatto "configurazione della connessione a federazione di griglie".
  - Lo stato della connessione è **connesso**.
  - Si dispone dell'autorizzazione di accesso root.
  - Hai esaminato le considerazioni per "gestione dei tenant consentiti per la federazione di grid".

◦ Se l'account tenant utilizza l'origine dell'identità configurata per Grid Manager, lo stesso gruppo federated è stato importato in Grid Manager su entrambe le griglie.

Quando si crea il tenant, si seleziona questo gruppo per disporre dell'autorizzazione di accesso root iniziale per gli account tenant di origine e di destinazione.

Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non viene replicato nella destinazione.

Accedere alla procedura guidata

Fasi

1. Selezionare **TENANT**.
2. Selezionare **Crea**.

Inserire i dettagli

Fasi

1. Inserire i dettagli del tenant.

Campo	Descrizione
Nome	Un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Quando viene creato, l'account tenant riceve un ID account univoco di 20 cifre.
Descrizione (opzionale)	Una descrizione che aiuta a identificare il tenant. Se si crea un tenant che utilizzerà una connessione a federazione di griglie, utilizzare questo campo per identificare il tenant di origine e il tenant di destinazione. Ad esempio, questa descrizione per un tenant creato sulla griglia 1 verrà visualizzata anche per il tenant replicato sulla griglia 2: "Questo tenant è stato creato sulla griglia 1".
Tipo di client	Il tipo di protocollo client utilizzato dal tenant, **S3** o **Swift**. **Nota**: Il supporto per le applicazioni client Swift è stato obsoleto e verrà rimosso in una release futura.
Quota di storage (opzionale)	Se si desidera che il tenant disponga di una quota di storage, un valore numerico per la quota e le unità.

2. Selezionare **continua**.

selezionare le autorizzazioni

Fasi

1. Se si desidera, selezionare le autorizzazioni desiderate per il tenant.

Alcune di queste autorizzazioni hanno requisiti aggiuntivi. Per ulteriori informazioni, selezionare l'icona della guida per ciascuna autorizzazione.

Permesso	Se selezionato…
Consentire i servizi della piattaforma	Il tenant può utilizzare servizi della piattaforma S3 come CloudMirror. Vedere "Gestire i servizi della piattaforma per gli account tenant S3".
Utilizza la propria origine di identità	Il tenant può configurare e gestire la propria origine di identità per gruppi e utenti federati. Questa opzione è disattivata se si dispone di "SSO configurato" Per il tuo sistema StorageGRID.
Consenti selezione S3	Il tenant può emettere richieste API S3 SelectObjectContent per filtrare e recuperare i dati degli oggetti. Vedere "Manage S3 (Gestisci S3): Selezionare per gli account tenant". **Importante**: Le richieste SelectObjectContent possono ridurre le performance di bilanciamento del carico per tutti i client S3 e per tutti i tenant. Attivare questa funzione solo quando richiesto e solo per tenant attendibili.
USA connessione a federazione di griglie	Il tenant può utilizzare una connessione a federazione di grid. Selezionando questa opzione: • Consente di clonare questo tenant e tutti i gruppi tenant e gli utenti aggiunti all'account da questa griglia (la *griglia di origine*) all'altra griglia della connessione selezionata (la *griglia di destinazione*). • Consente a questo tenant di configurare la replica cross-grid tra i bucket corrispondenti su ogni grid. Vedere "Gestire i tenant consentiti per la federazione di grid".

2. Se si seleziona **Usa connessione federazione griglia**, selezionare una delle connessioni federazione griglia disponibili.

3. Selezionare **continua**.

Definire l'accesso root e creare il tenant

Fasi

1. Definire l'accesso root per l'account tenant, a seconda che il sistema StorageGRID utilizzi la federazione di identità, il single sign-on (SSO) o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

2. Selezionare **Crea tenant**.

   Viene visualizzato un messaggio di successo e il nuovo tenant viene elencato nella pagina tenant. Per informazioni su come visualizzare i dettagli del tenant e monitorare l'attività del tenant, vedere "Monitorare l'attività del tenant".

3. Se è stata selezionata l'autorizzazione **Usa connessione federazione griglia** per il tenant:
   a. Verificare che un tenant identico sia stato replicato nell'altra griglia della connessione. I tenant di entrambe le griglie avranno lo stesso ID account a 20 cifre, il nome, la descrizione, la quota e le autorizzazioni.

      Se viene visualizzato il messaggio di errore "tenant creato senza clone", fare riferimento alle istruzioni riportate nella "Risolvere i problemi relativi agli errori di federazione della griglia".

   b. Se è stata fornita una password utente root locale durante la definizione dell'accesso root, "modificare la password per l'utente root locale" per il tenant replicato.

      Un utente root locale non può accedere a Tenant Manager nella griglia di destinazione fino a quando la password non viene modificata.

Accesso al tenant (facoltativo)

Se necessario, è possibile accedere al nuovo tenant ora per completare la configurazione oppure accedere al tenant in un secondo momento. La procedura di accesso dipende dal fatto che si sia effettuato l'accesso a Grid Manager utilizzando la porta predefinita (443) o una porta con restrizioni. Vedere "Controllare l'accesso al firewall esterno".

Accedi subito

Se si utilizza…	Eseguire questa operazione…
Porta 443 e viene impostata una password per l'utente root locale	1. Selezionare **Accedi come root**. Al momento dell'accesso, vengono visualizzati i collegamenti per la configurazione di bucket, federazione di identità, gruppi e utenti. 2. Selezionare i collegamenti per configurare l'account tenant. Ciascun collegamento apre la pagina corrispondente in Tenant Manager. Per completare la pagina, consultare "istruzioni per l'utilizzo degli account tenant".
Porta 443 e non è stata impostata una password per l'utente root locale	Selezionare **Accedi** e immettere le credenziali per un utente nel gruppo federated di accesso root.
Una porta con restrizioni	1. Selezionare **fine** 2. Selezionare **limitato** nella tabella tenant per ulteriori informazioni sull'accesso a questo account tenant. L'URL del tenant manager ha il seguente formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* È un nome di dominio completo o l'indirizzo IP di un nodo amministratore ◦ *port* è la porta solo tenant ◦ *20-digit-account-id* È l'ID account univoco del tenant

Accedi più tardi

Se si utilizza…	Eseguire una di queste operazioni…
Porta 443	• Da Grid Manager, selezionare **TENANT** e selezionare **Sign in** (Accedi) a destra del nome del tenant. • Inserire l'URL del tenant in un browser Web: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* È un nome di dominio completo o l'indirizzo IP di un nodo amministratore ◦ *20-digit-account-id* È l'ID account univoco del tenant

Se si utilizza…	Eseguire una di queste operazioni…
Una porta con restrizioni	• Da Grid Manager, selezionare **TENANT** e selezionare **Restricted**. • Inserire l'URL del tenant in un browser Web: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* È un nome di dominio completo o l'indirizzo IP di un nodo amministratore ◦ *port* è la porta limitata solo tenant ◦ *20-digit-account-id* È l'ID account univoco del tenant

Configurare il tenant

Seguire le istruzioni riportate in "Utilizzare un account tenant" Per gestire gruppi di tenant e utenti, chiavi di accesso S3, bucket, servizi di piattaforma e replica di cloni di account e cross-grid.

Modificare l'account tenant

È possibile modificare un account tenant per modificare il nome visualizzato, la quota di storage o le autorizzazioni del tenant.

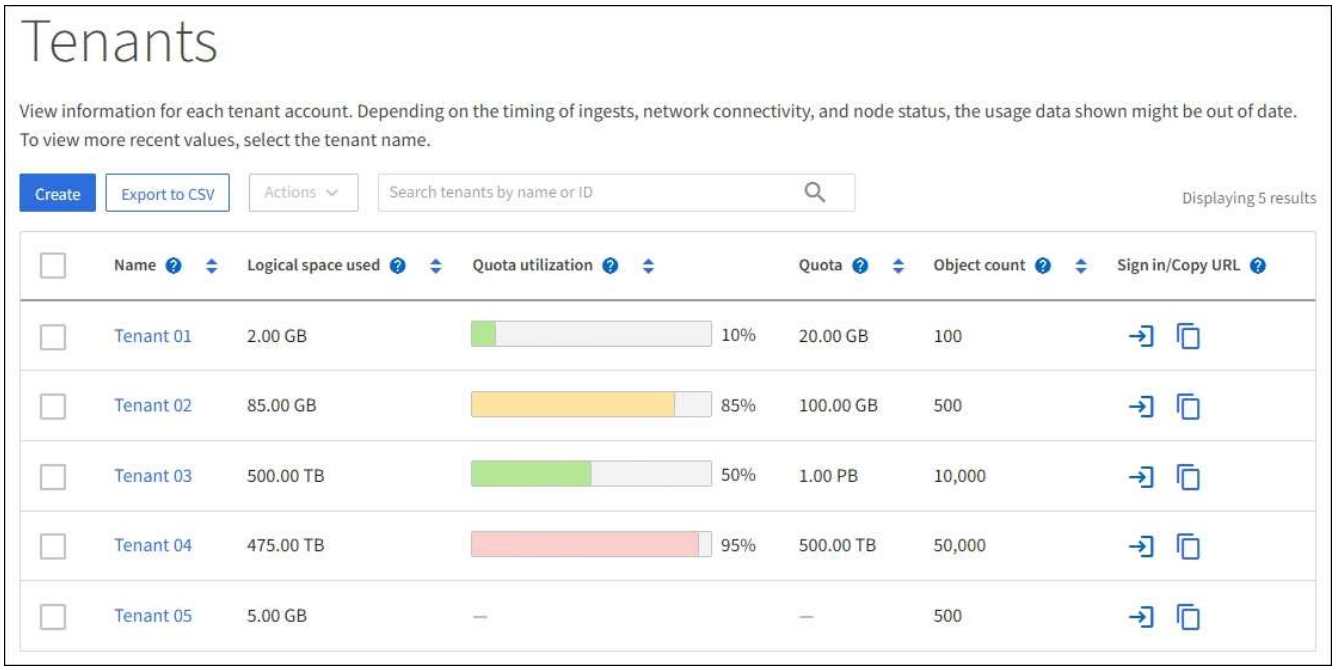
> Se un tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile modificare i dettagli del tenant da una delle griglie della connessione. Tuttavia, qualsiasi modifica apportata su una griglia della connessione non verrà copiata nell'altra griglia. Se si desidera mantenere i dettagli del tenant perfettamente sincronizzati tra le griglie, apportare le stesse modifiche su entrambe le griglie. Vedere "Gestire i tenant consentiti per la connessione a federazione di grid".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Accesso root o autorizzazione account tenant".

Fasi

1. Selezionare **TENANT**.



2. Individuare l'account tenant che si desidera modificare.

   Utilizzare la casella di ricerca per cercare un tenant in base al nome o all'ID del tenant.

3. Selezionare il tenant. È possibile effettuare una delle seguenti operazioni:
   - Selezionare la casella di controllo del tenant e selezionare **azioni** > **Modifica**.
   - Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **Modifica**.
4. Facoltativamente, modificare i valori per questi campi:
   - **Nome**
   - **Descrizione**
   - **Quota di storage**
5. Selezionare **continua**.
6. Selezionare o deselezionare le autorizzazioni per l'account tenant.
   - Se si disattiva **Platform Services** per un tenant che li sta già utilizzando, i servizi configurati per i bucket S3 smetteranno di funzionare. Non viene inviato alcun messaggio di errore al tenant. Ad esempio, se il tenant ha configurato la replica CloudMirror per un bucket S3, può comunque memorizzare oggetti nel bucket, ma le copie di tali oggetti non verranno più eseguite nel bucket S3 esterno configurato come endpoint. Vedere "Gestire i servizi della piattaforma per gli account tenant S3".
   - Modificare l'impostazione di **utilizza la propria origine dell'identità** per determinare se l'account tenant utilizzerà la propria origine dell'identità o l'origine dell'identità configurata per Grid Manager.

     Se **utilizza la propria origine di identità** è:

     - Disattivato e selezionato, il tenant ha già attivato la propria origine di identità. Un tenant deve disattivare l'origine dell'identità prima di poter utilizzare l'origine dell'identità configurata per Grid Manager.
     - Disattivato e non selezionato, SSO è attivato per il sistema StorageGRID. Il tenant deve utilizzare l'origine dell'identità configurata per Grid Manager.

- Selezionare o deselezionare l'autorizzazione **Allow S3 Select** (Consenti selezione S3) in base alle necessità. Vedere "Manage S3 (Gestisci S3): Selezionare per gli account tenant".
- Per rimuovere l'autorizzazione **Use grid Federation Connection**:
  i. Vai alla pagina dei dettagli del locatario.
  ii. Selezionare la scheda **federazione griglia**.
  iii. Selezionare **Rimuovi permesso**.
- Per aggiungere l'autorizzazione **Use grid Federation Connection**:
  i. Selezionare la casella di controllo **Usa connessione federazione griglia**.
  ii. Facoltativamente, selezionare **Clona utenti e gruppi locali esistenti** per clonarli nella griglia remota. Se si desidera, è possibile interrompere la clonazione in corso o riprovare a eseguire la clonazione se la clonazione di alcuni utenti o gruppi locali non è riuscita una volta completata l'ultima operazione di clonazione.

Modificare la password per l'utente root locale del tenant

Potrebbe essere necessario modificare la password per l'utente root locale di un tenant se l'utente root è bloccato dall'account.

Prima di iniziare

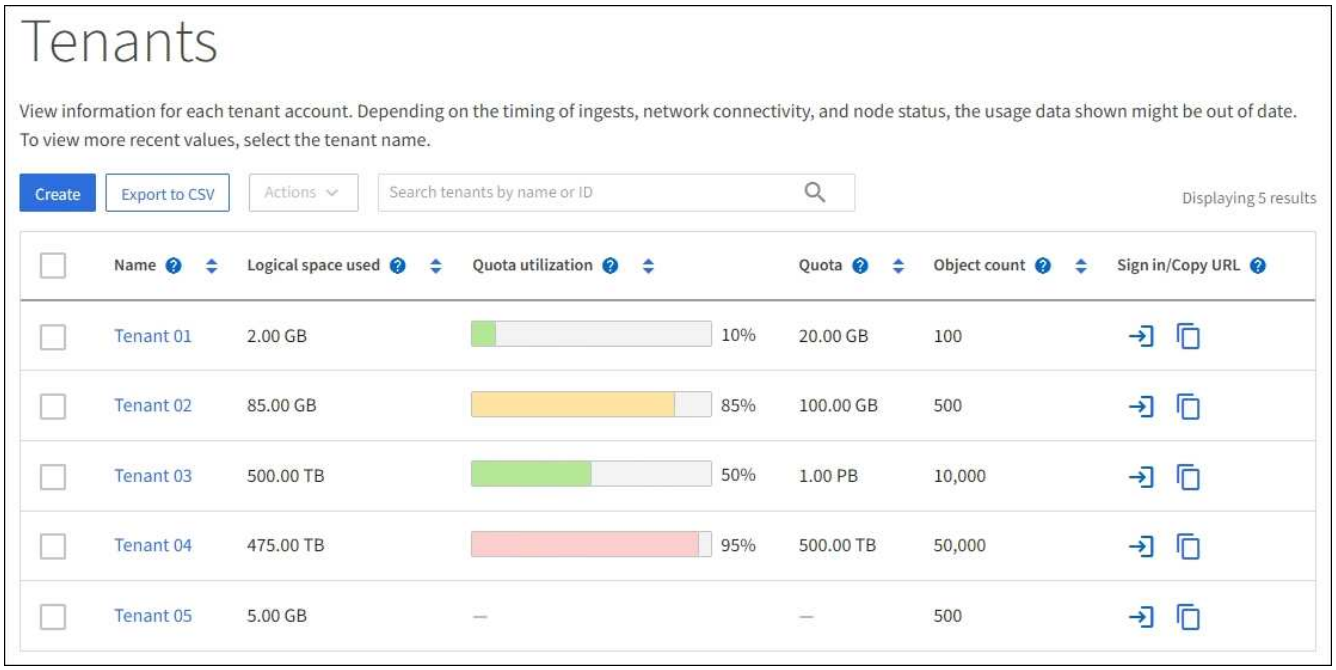
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Se il sistema StorageGRID è abilitato per il Single Sign-on (SSO), l'utente root locale non può accedere all'account tenant. Per eseguire le attività dell'utente root, gli utenti devono appartenere a un gruppo federated che disponga dell'autorizzazione di accesso root per il tenant.

Fasi

1. Selezionare **TENANT**.



2. Selezionare l'account tenant. È possibile effettuare una delle seguenti operazioni:
   - Selezionare la casella di controllo del tenant e selezionare **azioni** > **Modifica password root**.
   - Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **azioni** > **Modifica password root**.
3. Inserire la nuova password per l'account tenant.
4. Selezionare **Salva**.

Elimina account tenant

È possibile eliminare un account tenant se si desidera rimuovere in modo permanente l'accesso del tenant al sistema.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Sono stati rimossi tutti i bucket (S3), i container (Swift) e gli oggetti associati all'account tenant.
- Se il tenant è autorizzato a utilizzare una connessione a federazione di griglie, sono state esaminate le considerazioni per "Eliminazione di un tenant con l'autorizzazione di connessione Usa federazione griglia".

Fasi

1. Selezionare **TENANT**.
2. Individuare l'account tenant o gli account che si desidera eliminare.

   Utilizzare la casella di ricerca per cercare un tenant in base al nome o all'ID del tenant.

3. Per eliminare più tenant, selezionare le caselle di controllo e selezionare **azioni** > **Elimina**.
4. Per eliminare un singolo tenant, effettuare una delle seguenti operazioni:
   - Selezionare la casella di controllo e selezionare **azioni** > **Elimina**.
   - Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **azioni** > **Elimina**.
5. Selezionare **Sì**.

Gestire i servizi della piattaforma

Gestione dei servizi di piattaforma per i tenant: Panoramica

Se si abilitano i servizi della piattaforma per gli account tenant S3, è necessario configurare il grid in modo che i tenant possano accedere alle risorse esterne necessarie per l'utilizzo di questi servizi.

Cosa sono i servizi della piattaforma?

I servizi della piattaforma includono la replica di CloudMirror, le notifiche degli eventi e il servizio di integrazione della ricerca.

Replica di CloudMirror

Il servizio di replica di StorageGRID CloudMirror viene utilizzato per eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.

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.

> La replica di CloudMirror presenta alcune importanti analogie differenze con la funzionalità di replica cross-grid. Per ulteriori informazioni, vedere "Confronta la replica cross-grid e la replica CloudMirror".

> La replica di CloudMirror non è supportata se il bucket di origine ha attivato il blocco oggetti S3.

Notifiche

Le notifiche degli eventi per bucket vengono utilizzate per inviare notifiche su azioni specifiche eseguite su oggetti a un cluster Kafka esterno specifico o ad Amazon Simple Notification Service.

Ad esempio, è possibile configurare gli avvisi da inviare agli amministratori in merito a ciascun oggetto aggiunto a un bucket, in cui gli oggetti rappresentano i file di registro associati a un evento di sistema critico.

> Sebbene la notifica degli eventi possa essere configurata su un bucket con blocco oggetti S3 attivato, i metadati del blocco oggetti S3 (inclusi lo stato Mantieni fino alla data e conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.

Servizio di integrazione della ricerca

Il servizio di integrazione della ricerca viene utilizzato per inviare i metadati degli oggetti S3 a un indice Elasticsearch specificato, in cui è possibile cercare o analizzare i metadati utilizzando il servizio esterno.

Ad esempio, è possibile configurare i bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. È quindi possibile utilizzare Elasticsearch per eseguire ricerche tra bucket ed eseguire analisi sofisticate dei modelli presenti nei metadati degli oggetti.

> Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock attivato, i metadati S3 Object Lock (inclusi Retain until Date e Legal Hold status) degli oggetti non saranno inclusi nei messaggi di notifica.

I servizi della piattaforma offrono ai tenant la possibilità di utilizzare risorse di storage esterne, servizi di notifica e servizi di ricerca o analisi con i propri dati. Poiché la posizione di destinazione dei servizi della piattaforma è generalmente esterna alla distribuzione di StorageGRID, è necessario decidere se consentire ai tenant di utilizzare questi servizi. In tal caso, è necessario abilitare l'utilizzo dei servizi della piattaforma quando si creano o modificano gli account tenant. È inoltre necessario configurare la rete in modo che i messaggi dei servizi della piattaforma generati dai tenant possano raggiungere le proprie destinazioni.

Consigli per l'utilizzo dei servizi della piattaforma

Prima di utilizzare i servizi della piattaforma, tenere presenti i seguenti consigli:

- Se in un bucket S3 nel sistema StorageGRID sono attivate sia la versione che la replica CloudMirror, è necessario attivare anche la versione del bucket S3 per l'endpoint di destinazione. Ciò consente alla replica di CloudMirror di generare versioni di oggetti simili sull'endpoint.

- Non utilizzare più di 100 tenant attivi con richieste S3 che richiedono la replica CloudMirror, le notifiche e l'integrazione della ricerca. La presenza di più di 100 tenant attivi può rallentare le performance del client S3.
- Le richieste a un endpoint che non possono essere completate verranno messe in coda per un massimo di 500,000 richieste. Questo limite è equamente condiviso tra i tenant attivi. I nuovi tenant possono superare temporaneamente questo limite di 500,000, in modo che i nuovi tenant non vengano penalizzati in modo ingiusto.

Informazioni correlate

- "Gestire i servizi della piattaforma"
- "Configurare le impostazioni del proxy di storage"
- "Monitorare StorageGRID"

Rete e porte per i servizi della piattaforma

Se si consente a un tenant S3 di utilizzare i servizi della piattaforma, è necessario configurare la rete per la griglia per garantire che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

È possibile abilitare i servizi della piattaforma per un account tenant S3 quando si crea o si aggiorna l'account tenant. Se i servizi della piattaforma sono attivati, il tenant può creare endpoint che fungono da destinazione per la replica CloudMirror, le notifiche di eventi o i messaggi di integrazione di ricerca dai bucket S3. Questi messaggi dei servizi della piattaforma vengono inviati dai nodi di storage che eseguono il servizio ADC agli endpoint di destinazione.

Ad esempio, i tenant potrebbero configurare i seguenti tipi di endpoint di destinazione:

- Cluster Elasticsearch ospitato localmente
- Un'applicazione locale che supporta la ricezione di messaggi Amazon Simple Notification Service
- Un cluster Kafka ospitato localmente
- Un bucket S3 ospitato localmente sulla stessa o su un'altra istanza di StorageGRID
- Un endpoint esterno, ad esempio un endpoint su Amazon Web Services.

Per garantire che i messaggi dei servizi della piattaforma possano essere inviati, è necessario configurare la rete o le reti contenenti i nodi di storage ADC. È necessario assicurarsi che le seguenti porte possano essere utilizzate per inviare messaggi di servizi della piattaforma agli endpoint di destinazione.

Per impostazione predefinita, i messaggi dei servizi della piattaforma vengono inviati alle seguenti porte:

- **80**: Per gli URI endpoint che iniziano con http (la maggior parte degli endpoint)
- **443**: Per gli URI endpoint che iniziano con https (la maggior parte degli endpoint)
- **9092**: Per gli URI endpoint che iniziano con http o https (solo endpoint Kafka)

I tenant possono specificare una porta diversa quando creano o modificano un endpoint.

> Se si utilizza un'implementazione StorageGRID come destinazione della replica di CloudMirror, i messaggi di replica potrebbero essere ricevuti su una porta diversa da 80 o 443. Assicurarsi che la porta utilizzata per S3 dall'implementazione StorageGRID di destinazione sia specificata nell'endpoint.

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.

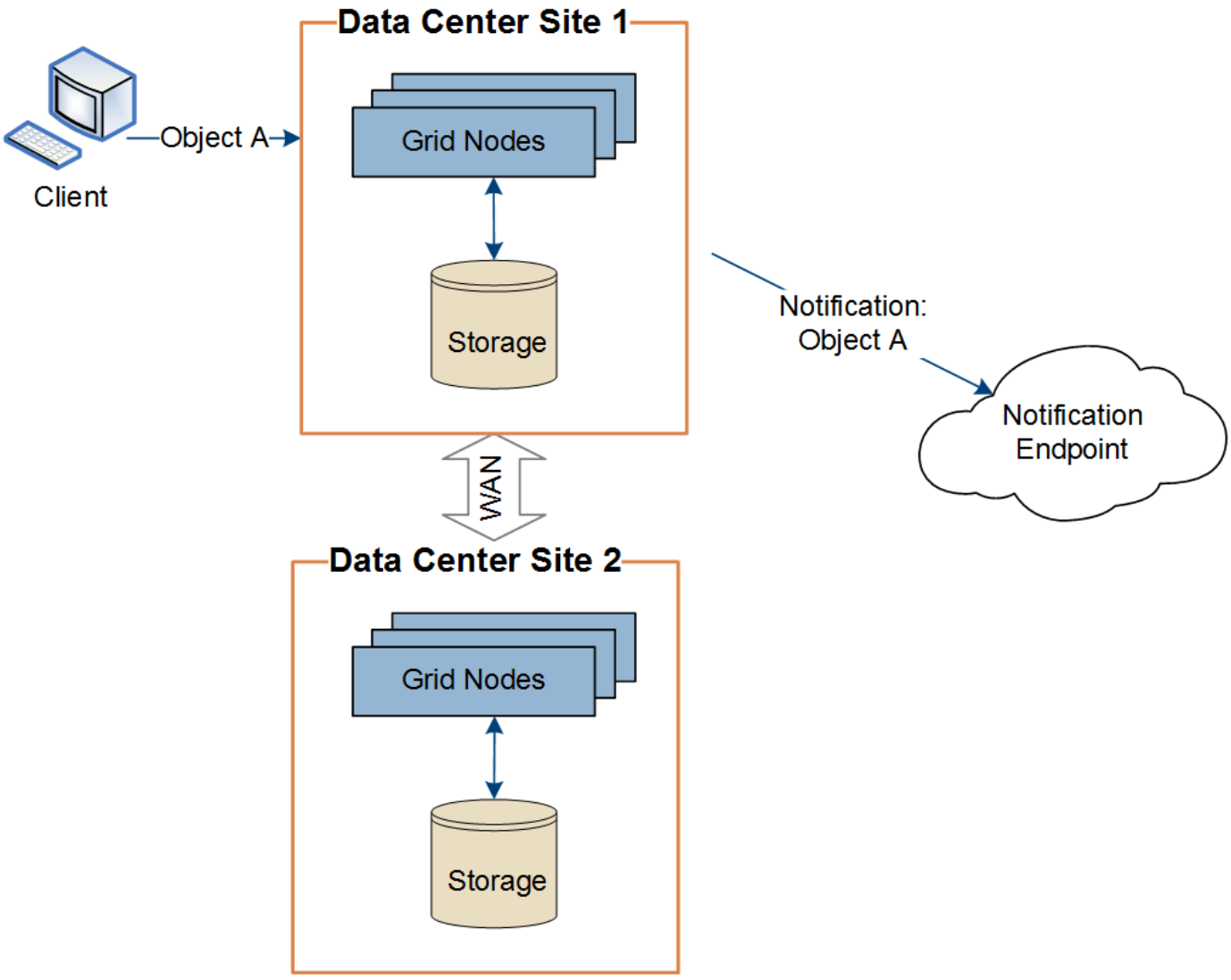
Informazioni correlate

- "Utilizzare un account tenant"

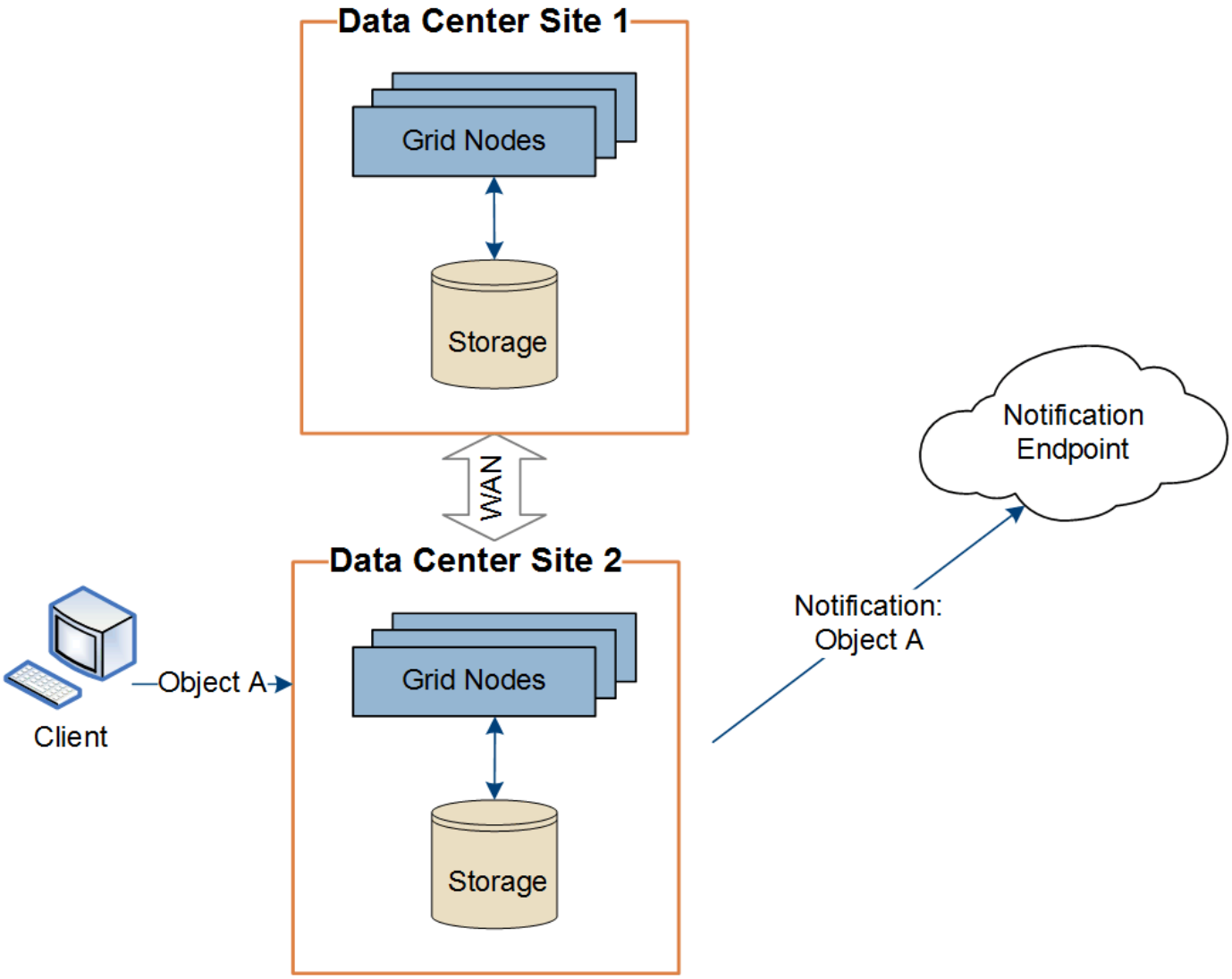
Erogazione per sito di messaggi relativi ai servizi della piattaforma

Tutte le operazioni dei servizi della piattaforma vengono eseguite in base al sito.

Cioè, se un tenant utilizza un client per eseguire un'operazione S3 API Create su un oggetto connettendosi a un nodo gateway nel sito 1 del data center, la notifica relativa a tale azione viene attivata e inviata dal sito 1 del data center.



Se il client esegue successivamente un'operazione di eliminazione API S3 sullo stesso oggetto dal sito del data center 2, la notifica relativa all'azione di eliminazione viene attivata e inviata dal sito del data center 2.



Assicurarsi che la rete di ciascun sito sia configurata in modo che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

Risolvere i problemi relativi ai servizi della piattaforma

Gli endpoint utilizzati nei servizi della piattaforma vengono creati e gestiti dagli utenti del tenant in Tenant Manager; tuttavia, se un tenant ha problemi nella configurazione o nell'utilizzo dei servizi della piattaforma, potrebbe essere possibile utilizzare Grid Manager per risolvere il problema.

Problemi con i nuovi endpoint

Prima che un tenant possa utilizzare i servizi della piattaforma, deve creare uno o più endpoint utilizzando il tenant Manager. Ciascun endpoint rappresenta una destinazione esterna per un servizio di piattaforma, come un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento del servizio di notifica semplice Amazon, un argomento di Kafka o un cluster Elasticsearch ospitato localmente o su AWS. Ogni endpoint include sia la posizione della risorsa esterna che le credenziali necessarie per accedere a tale risorsa.

Quando un tenant crea un endpoint, il sistema StorageGRID convalida che l'endpoint esiste e che può essere raggiunto utilizzando le credenziali specificate. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Se la convalida degli endpoint non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida degli endpoint non è riuscita. L'utente tenant dovrebbe risolvere il problema, quindi provare a creare nuovamente l'endpoint.

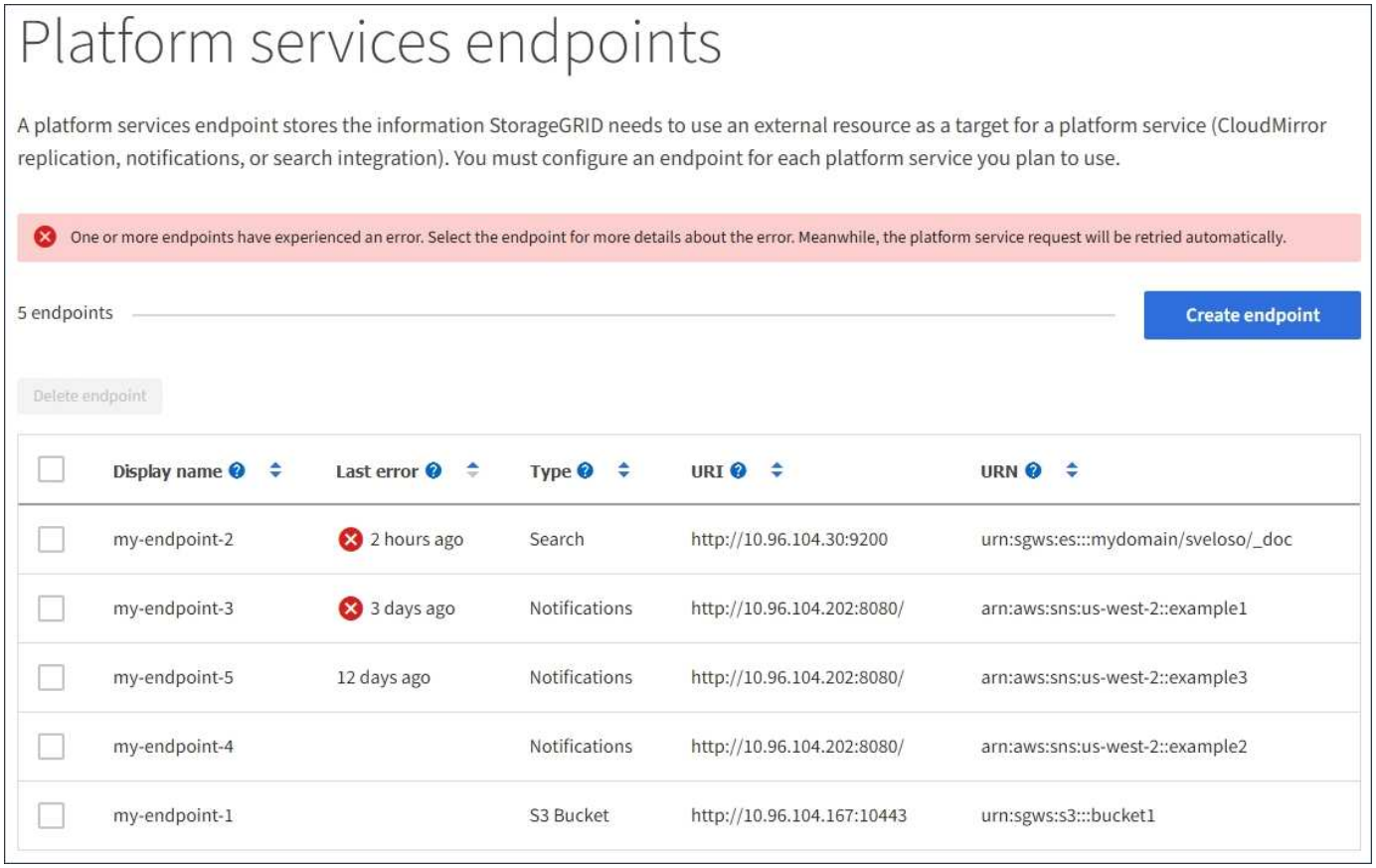
La creazione dell'endpoint non riesce se i servizi della piattaforma non sono abilitati per l'account tenant.

Problemi con gli endpoint esistenti

Se si verifica un errore quando StorageGRID tenta di raggiungere un endpoint esistente, viene visualizzato un messaggio sul dashboard in Gestione tenant.

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

Gli utenti del tenant possono accedere alla pagina degli endpoint per esaminare il messaggio di errore più recente per ciascun endpoint e per determinare quanto tempo fa si è verificato l'errore. La colonna **ultimo errore** visualizza il messaggio di errore più recente per ciascun endpoint e indica per quanto tempo si è verificato l'errore. Errori che includono si è verificata negli ultimi 7 giorni.



Alcuni messaggi di errore nella colonna **ultimo errore** potrebbero includere un LOGID tra parentesi. Un amministratore della griglia o il supporto tecnico può utilizzare questo ID per individuare informazioni più dettagliate sull'errore nel file bycast.log.

Problemi relativi ai server proxy

Se è stato configurato un "proxy di storage" Tra i nodi di storage e gli endpoint del servizio della piattaforma, potrebbero verificarsi errori se il servizio proxy non consente messaggi da StorageGRID. Per risolvere questi problemi, controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma non siano bloccati.

Determinare se si è verificato un errore

Se si sono verificati errori degli endpoint negli ultimi 7 giorni, il dashboard di Tenant Manager visualizza un messaggio di avviso. È possibile accedere alla pagina Endpoint per ulteriori dettagli sull'errore.

Le operazioni del client non riescono

Alcuni problemi relativi ai servizi della piattaforma potrebbero causare il malfunzionamento delle operazioni client sul bucket S3. Ad esempio, le operazioni del client S3 non vengono eseguite correttamente se il servizio RSM (Replicated state Machine) interno viene arrestato o se sono presenti troppi messaggi dei servizi della piattaforma in coda per il recapito.

Per controllare lo stato dei servizi:

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > ***Storage Node*** > **SSM** > **Services**.

Errori degli endpoint ripristinabili e non ripristinabili

Una volta creati gli endpoint, gli errori di richiesta del servizio della piattaforma possono verificarsi per diversi motivi. Alcuni errori possono essere ripristinati con l'intervento dell'utente. Ad esempio, potrebbero verificarsi errori ripristinabili per i seguenti motivi:

- Le credenziali dell'utente sono state eliminate o scadute.
- Il bucket di destinazione non esiste.
- Impossibile ricevere la notifica.

Se StorageGRID rileva un errore ripristinabile, la richiesta di servizio della piattaforma verrà rievitata fino a quando non avrà esito positivo.

Altri errori non sono ripristinabili. Ad esempio, se l'endpoint viene cancellato, si verifica un errore irreversibile.

Se StorageGRID rileva un errore irreversibile dell'endpoint, l'allarme legacy Eventi totali (SMTT) viene attivato in Gestione griglia. Per visualizzare l'allarme legacy Total Events (Eventi totali):

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***site*** > ***node*** > **SSM** > **Eventi**.
3. Visualizza ultimo evento nella parte superiore della tabella.

   I messaggi degli eventi sono elencati anche nella `/var/local/log/bycast-err.log`.

4. Seguire le indicazioni fornite nel contenuto degli allarmi SMTT per correggere il problema.
5. Selezionare la scheda **Configurazione** per ripristinare i conteggi degli eventi.
6. Notificare al tenant gli oggetti i cui messaggi dei servizi della piattaforma non sono stati recapitati.

7. Chiedere al tenant di riattivare la replica o la notifica non riuscita aggiornando i metadati o i tag dell'oggetto.

   Il tenant può reinviare i valori esistenti per evitare modifiche indesiderate.

I messaggi dei servizi della piattaforma non possono essere inviati

Se la destinazione incontra un problema che impedisce l'accettazione dei messaggi dei servizi della piattaforma, l'operazione client sul bucket riesce, ma il messaggio dei servizi della piattaforma non viene recapitato. Ad esempio, questo errore potrebbe verificarsi se le credenziali vengono aggiornate sulla destinazione in modo che StorageGRID non possa più autenticare il servizio di destinazione.

Se i messaggi dei servizi della piattaforma non possono essere inviati a causa di un errore irreversibile, l'allarme legacy SMTT (Total Events) viene attivato in Grid Manager.

Performance più lente per le richieste di servizi della piattaforma

Il software StorageGRID potrebbe ridurre le richieste S3 in entrata per un bucket se la velocità con cui le richieste vengono inviate supera la velocità con cui l'endpoint di destinazione può ricevere le richieste. La limitazione si verifica solo quando è presente un backlog di richieste in attesa di essere inviate all'endpoint di destinazione.

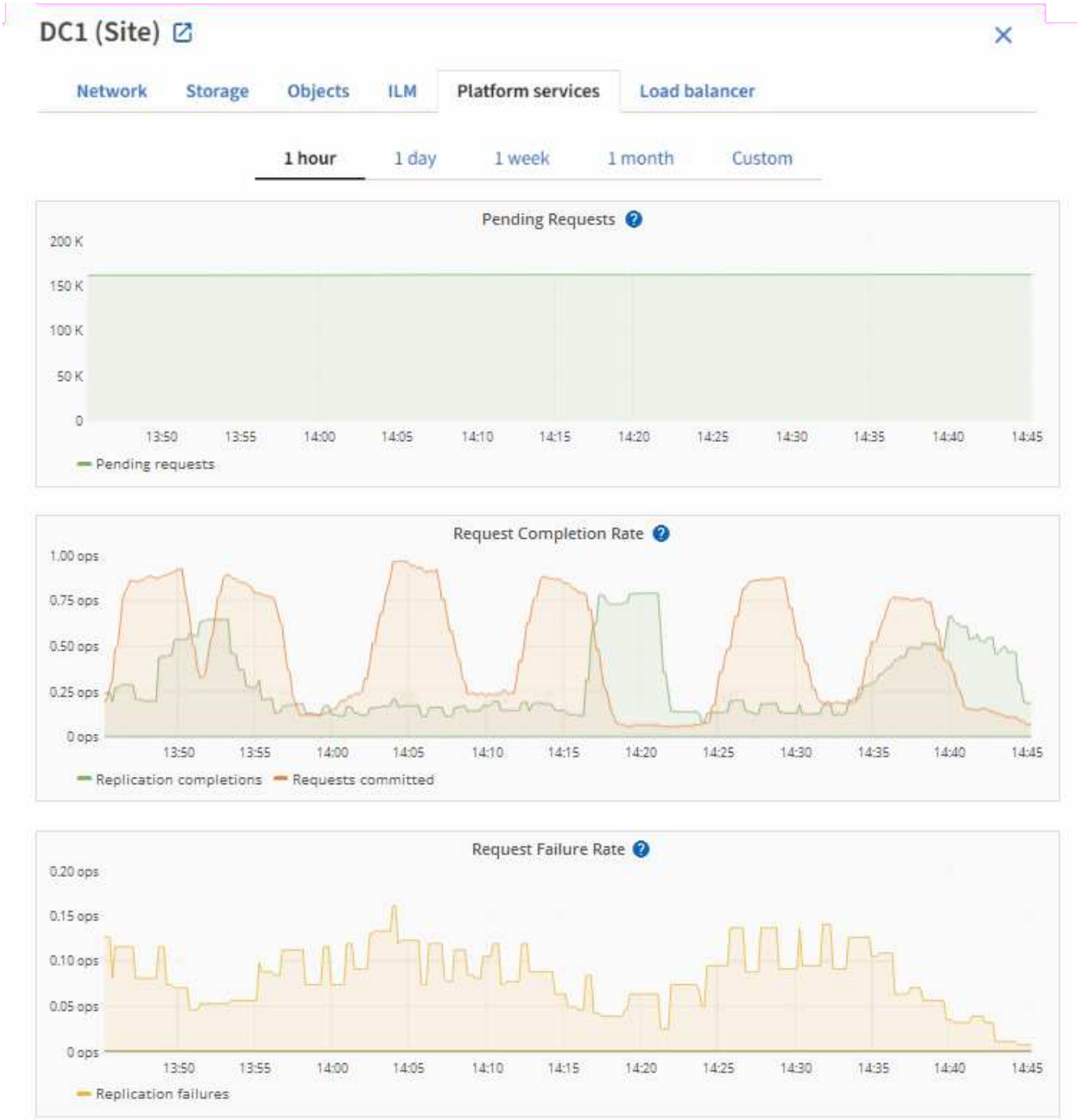
L'unico effetto visibile è che l'esecuzione delle richieste S3 in entrata richiederà più tempo. Se si inizia a rilevare performance significativamente più lente, è necessario ridurre il tasso di acquisizione o utilizzare un endpoint con capacità superiore. Se il backlog delle richieste continua a crescere, le operazioni del client S3 (come LE richieste PUT) finiranno per fallire.

È più probabile che le richieste CloudMirror siano influenzate dalle performance dell'endpoint di destinazione, perché queste richieste comportano in genere un maggior numero di trasferimenti di dati rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Le richieste di servizio della piattaforma non vengono soddisfatte

Per visualizzare il tasso di errore della richiesta per i servizi della piattaforma:

1. Selezionare **NODI**.
2. Selezionare ***Site*** > **Platform Services**.
3. Visualizza il grafico tasso di errore della richiesta.



Avviso di servizi della piattaforma non disponibili

L'avviso **Platform Services unavailable** (servizi piattaforma non disponibili) indica che non è possibile eseguire operazioni di servizio della piattaforma in un sito perché sono in esecuzione o disponibili troppi nodi di storage con il servizio RSM.

Il servizio RSM garantisce che le richieste di servizio della piattaforma vengano inviate ai rispettivi endpoint.

Per risolvere questo avviso, determinare quali nodi di storage del sito includono il servizio RSM. (Il servizio RSM è presente sui nodi di storage che includono anche il servizio ADC). Quindi, assicurarsi che la maggior parte di questi nodi di storage sia in esecuzione e disponibile.

Se più di un nodo di storage che contiene il servizio RSM si guasta in un sito, si perdono le richieste di servizio della piattaforma in sospeso per quel sito.

Ulteriori linee guida per la risoluzione dei problemi per gli endpoint dei servizi della piattaforma

Per ulteriori informazioni, vedere **Utilizzare un account tenant › risolvere i problemi relativi agli endpoint dei servizi della piattaforma**.

Informazioni correlate

- "Risolvere i problemi relativi al sistema StorageGRID"

Manage S3 (Gestisci S3): Selezionare per gli account tenant

È possibile consentire a determinati tenant S3 di utilizzare S3 Select per emettere richieste SelectObjectContent su singoli oggetti.

S3 Select offre un modo efficiente per cercare grandi quantità di dati senza dover implementare un database e le risorse associate per abilitare le ricerche. Inoltre, riduce i costi e la latenza del recupero dei dati.

Che cos'è S3 Select?

S3 Select consente ai client S3 di utilizzare le richieste SelectObjectContent per filtrare e recuperare solo i dati necessari da un oggetto. L'implementazione StorageGRID di S3 Select include un sottoinsieme di comandi e funzionalità S3 Select.

Considerazioni e requisiti per l'utilizzo di S3 Select

Requisiti di amministrazione della griglia

L'amministratore della griglia deve concedere ai tenant l'abilità S3 Select. Selezionare **Allow S3 Select** when (Consenti selezione S3) "creazione di un tenant" oppure "modifica di un tenant".

Requisiti di formato degli oggetti

L'oggetto che si desidera sottoporre a query deve essere in uno dei seguenti formati:

- **CSV**. Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
- **Parquet**. Requisiti aggiuntivi per gli oggetti in parquet:
  - S3 Select supporta solo la compressione colonnare con GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti parquet.
  - S3 Select non supporta l'output parquet. Specificare il formato di output come CSV o JSON.
  - La dimensione massima del gruppo di righe non compresso è di 512 MB.
  - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
  - Non è possibile utilizzare TIPI logici INTERVAL, JSON, LIST, TIME o UUID.

Requisiti degli endpoint

La richiesta SelectObjectContent deve essere inviata a "Endpoint del bilanciamento del carico di StorageGRID".

I nodi Admin e Gateway utilizzati dall'endpoint devono essere uno dei seguenti:

- Un nodo di appliance per i servizi
- Nodo software basato su VMware
- Nodo bare metal che esegue un kernel con cgroup v2 abilitato

Considerazioni generali

Le query non possono essere inviate direttamente ai nodi di storage.

> Le richieste SelectObjectContent possono ridurre le performance di bilanciamento del carico per tutti i client S3 e per tutti i tenant. Attivare questa funzione solo quando richiesto e solo per tenant attendibili.

Vedere "Istruzioni per l'utilizzo di S3 Select".

Per visualizzare "Grafici Grafana" Per le operazioni S3 Select nel tempo, selezionare **SUPPORT** > **Tools** > **Metrics** in Grid Manager.

Configurare le connessioni client

Configurazione delle connessioni client S3 e Swift: Panoramica

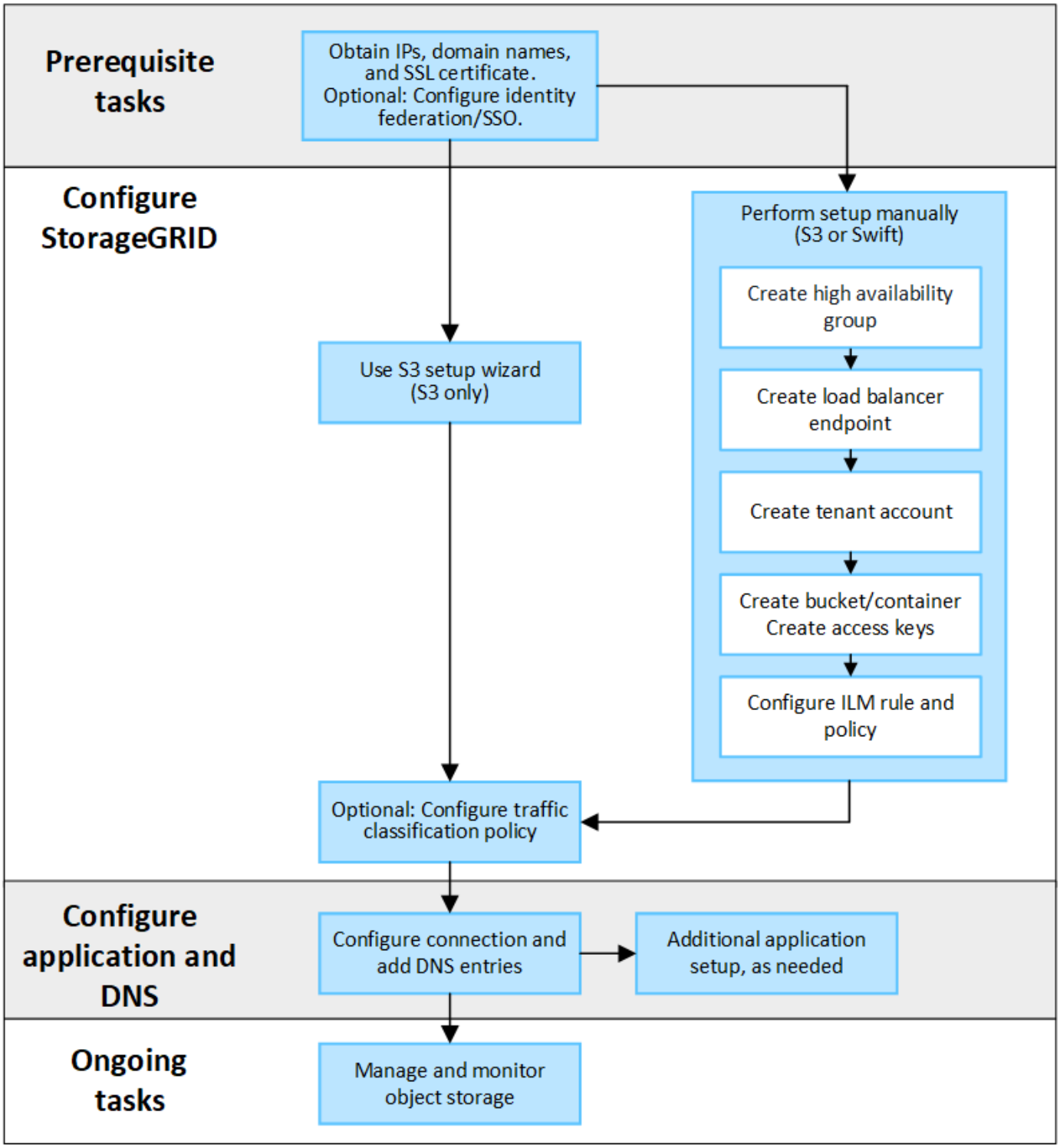
In qualità di amministratore di grid, gestisci le opzioni di configurazione che controllano il modo in cui le applicazioni client S3 e Swift si connettono al sistema StorageGRID per memorizzare e recuperare i dati.

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

Workflow di configurazione

Come illustrato nel diagramma del flusso di lavoro, sono disponibili quattro passaggi principali per la connessione di StorageGRID a qualsiasi applicazione S3 o Swift:

1. Eseguire attività preliminari in StorageGRID, in base al modo in cui l'applicazione client si connetterà a StorageGRID.
2. Utilizzare StorageGRID per ottenere i valori necessari all'applicazione per connettersi alla griglia. È possibile utilizzare l'installazione guidata S3 o configurare manualmente ogni entità StorageGRID.
3. Utilizzare l'applicazione S3 o Swift per completare la connessione a StorageGRID. Creare voci DNS per associare gli indirizzi IP ai nomi di dominio che si intende utilizzare.
4. Eseguire attività in corso nell'applicazione e in StorageGRID per gestire e monitorare lo storage a oggetti nel tempo.



Informazioni necessarie per collegare StorageGRID a un'applicazione client

Prima di poter collegare StorageGRID a un'applicazione client S3 o Swift, è necessario eseguire i passaggi di configurazione in StorageGRID e ottenere un determinato valore.

Di quali valori ho bisogno?

La seguente tabella mostra i valori da configurare in StorageGRID e i valori utilizzati dall'applicazione S3 o Swift e dal server DNS.

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Indirizzi IP virtuali (VIP)	StorageGRID > Gruppo ha	Voce DNS
Porta	StorageGRID > endpoint del bilanciamento del carico	Applicazione client
Certificato SSL	StorageGRID > endpoint del bilanciamento del carico	Applicazione client
Nome server (FQDN)	StorageGRID > endpoint del bilanciamento del carico	• Applicazione client • Voce DNS
ID chiave di accesso S3 e chiave di accesso segreta	StorageGRID > tenant e bucket	Applicazione client
Nome bucket/container	StorageGRID > tenant e bucket	Applicazione client

Come si ottengono questi valori?

In base alle proprie esigenze, è possibile effettuare una delle seguenti operazioni per ottenere le informazioni necessarie:

- **Utilizzare il "Installazione guidata S3"**. L'installazione guidata S3 consente di configurare rapidamente i valori richiesti in StorageGRID e di creare uno o due file da utilizzare per la configurazione dell'applicazione S3. La procedura guidata guida l'utente attraverso i passaggi richiesti e aiuta a verificare che le impostazioni siano conformi alle Best practice di StorageGRID.

  > Se si sta configurando un'applicazione S3, si consiglia di utilizzare la procedura guidata di configurazione S3, a meno che non si sappiano requisiti speciali o l'implementazione richieda una personalizzazione significativa.

- **Utilizzare il "Installazione guidata di FabricPool"**. Analogamente all'installazione guidata di S3, l'installazione guidata di FabricPool consente di configurare rapidamente i valori richiesti e di creare un file da utilizzare quando si configura un livello cloud FabricPool in ONTAP.

  > Se si prevede di utilizzare StorageGRID come sistema di storage a oggetti per un livello cloud FabricPool, si consiglia di utilizzare la procedura guidata di installazione di FabricPool, a meno che non si sappiano requisiti speciali o l'implementazione richieda una personalizzazione significativa.

- **Configurare gli elementi manualmente**. Se si sta effettuando la connessione a un'applicazione Swift (o si sta effettuando la connessione a un'applicazione S3 e si preferisce non utilizzare l'installazione guidata S3), è possibile ottenere i valori richiesti eseguendo la configurazione manualmente. Attenersi alla seguente procedura:

  a. Configurare il gruppo ad alta disponibilità (ha) che si desidera utilizzare per l'applicazione S3 o Swift. Vedere "Configurare i gruppi ad alta disponibilità".

  b. Creare l'endpoint del bilanciamento del carico che verrà utilizzato dall'applicazione S3 o Swift. Vedere "Configurare gli endpoint del bilanciamento del carico".

c. Creare l'account tenant utilizzato dall'applicazione S3 o Swift. Vedere "Creare un account tenant".

d. Per un tenant S3, accedere all'account tenant e generare un ID della chiave di accesso e una chiave di accesso segreta per ogni utente che accede all'applicazione. Vedere "Creare le proprie chiavi di accesso".

e. Creare uno o più bucket S3 o container Swift all'interno dell'account tenant. Per S3, vedere "Creare un bucket S3". Per Swift, utilizzare "INSERIRE la richiesta di container".

f. Per aggiungere istruzioni di posizionamento specifiche per gli oggetti appartenenti al nuovo tenant o bucket/container, creare una nuova regola ILM e attivare un nuovo criterio ILM per utilizzare tale regola. Vedere "Creare una regola ILM" e. "Creare un criterio ILM".

Sicurezza per client S3 o Swift

Gli account tenant di StorageGRID utilizzano applicazioni client S3 o Swift per salvare i dati degli oggetti in StorageGRID. È necessario esaminare le misure di protezione implementate per le applicazioni client.

Riepilogo

La tabella seguente riassume il modo in cui viene implementata la sicurezza per le API REST S3 e Swift:

Problema di sicurezza	Implementazione per API REST
Sicurezza della connessione	TLS
Autenticazione del server	Certificato server X.509 firmato dalla CA di sistema o certificato server personalizzato fornito dall'amministratore
Autenticazione del client	**S3** Account S3 (ID chiave di accesso e chiave di accesso segreta) **Rapido** Account Swift (nome utente e password)
Autorizzazione del client	**S3** Proprietà dei bucket e tutte le policy di controllo degli accessi applicabili **Rapido** Accesso al ruolo di amministratore

In che modo StorageGRID fornisce la protezione per le applicazioni client

Le applicazioni client S3 e Swift possono connettersi al servizio Load Balancer su nodi gateway o nodi amministrativi o direttamente ai nodi storage.

- I client che si connettono al servizio Load Balancer possono utilizzare HTTPS o HTTP, in base alla modalità di utilizzo "configurare l'endpoint del bilanciamento del carico".

  HTTPS fornisce una comunicazione sicura e crittografata TLS ed è consigliato. È necessario allegare un certificato di protezione all'endpoint.

HTTP fornisce comunicazioni meno sicure e non crittografate e dovrebbe essere utilizzato solo per reti non di produzione o di test.

- I client che si connettono ai nodi di archiviazione possono anche utilizzare HTTPS o HTTP.

  HTTPS è l'impostazione predefinita ed è consigliata.

  HTTP fornisce una comunicazione meno sicura e non crittografata, ma può essere opzionale "attivato" per reti non di produzione o di prova.

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

Certificati di sicurezza e applicazioni client

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

- Quando le applicazioni client si connettono al servizio Load Balancer, utilizzano il certificato configurato per l'endpoint del bilanciamento del carico. Ogni endpoint del bilanciatore di carico dispone di un proprio certificato—un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dall'amministratore della griglia in StorageGRID durante la configurazione dell'endpoint.

  Vedere "Considerazioni per il bilanciamento del carico".

- Quando le applicazioni client si connettono direttamente a un nodo di storage, utilizzano i certificati server generati dal sistema e generati per i nodi di storage al momento dell'installazione del sistema StorageGRID (firmati dall'autorità di certificazione del sistema), oppure un singolo certificato server personalizzato fornito per la griglia da un amministratore della griglia. Vedere "Aggiunta di un certificato API S3 o Swift personalizzato".

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

Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un insieme di pacchetti di crittografia che le applicazioni client possono utilizzare quando stabiliscono una sessione TLS. Per configurare le crittografia, andare a **CONFIGURATION** > **Security** > **Security settings** e selezionare **TLS and SSH policy**.

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3.

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

Utilizzare l'installazione guidata S3

È possibile utilizzare l'installazione guidata S3 per configurare StorageGRID come sistema di storage a oggetti per un'applicazione S3.

Quando utilizzare l'installazione guidata S3

L'installazione guidata S3 guida l'utente attraverso ogni fase della configurazione di StorageGRID per l'utilizzo con un'applicazione S3. Durante il completamento della procedura guidata, è possibile scaricare i file da utilizzare per immettere i valori nell'applicazione S3. Utilizzare la procedura guidata per configurare il sistema più rapidamente e per assicurarsi che le impostazioni siano conformi alle Best practice StorageGRID.

Se si dispone di "Autorizzazione di accesso root", È possibile completare l'installazione guidata di S3 quando si inizia a utilizzare il Gestore griglie di StorageGRID oppure è possibile accedere e completare la procedura guidata in qualsiasi momento. A seconda dei requisiti, è possibile configurare manualmente alcuni o tutti gli elementi richiesti e utilizzare la procedura guidata per assemblare i valori richiesti da un'applicazione S3.

Prima di utilizzare la procedura guidata

Prima di utilizzare la procedura guidata, verificare di aver completato questi prerequisiti.

Ottenere gli indirizzi IP e configurare le interfacce VLAN

Se si configura un gruppo ad alta disponibilità (ha), si conoscono i nodi a cui si connetterà l'applicazione S3 e la rete StorageGRID da utilizzare. Si conoscono anche i valori da inserire per la subnet CIDR, l'indirizzo IP del gateway e gli indirizzi IP virtuali (VIP).

Se si intende utilizzare una LAN virtuale per separare il traffico dall'applicazione S3, l'interfaccia VLAN è già stata configurata. Vedere "Configurare le interfacce VLAN".

Configurare la federazione di identità e SSO

Se si prevede di utilizzare la federazione di identità o il Single Sign-on (SSO) per il sistema StorageGRID, queste funzionalità sono state attivate. Si sa anche quale gruppo federato deve disporre dell'accesso root per l'account tenant utilizzato dall'applicazione S3. Vedere "USA la federazione delle identità" e. "Configurare il single sign-on".

Ottenere e configurare i nomi di dominio

Si conosce il nome di dominio completo (FQDN) da utilizzare per StorageGRID. Le voci DNS (Domain Name Server) associano questo FQDN agli indirizzi IP virtuali (VIP) del gruppo ha creato utilizzando la procedura guidata.

Se si prevede di utilizzare le richieste in stile host virtuale S3, è necessario "Nomi di dominio degli endpoint S3 configurati". Si consiglia di utilizzare richieste virtuali in stile host.

Esaminare i requisiti del bilanciamento del carico e del certificato di sicurezza

Se si intende utilizzare il bilanciamento del carico StorageGRID, sono state esaminate le considerazioni generali sul bilanciamento del carico. Si dispone dei certificati da caricare o dei valori necessari per generare un certificato.

Se si intende utilizzare un endpoint esterno (di terze parti) per il bilanciamento del carico, si dispone del nome di dominio completo (FQDN), della porta e del certificato per il bilanciamento del carico.

Configurare le connessioni di federazione di griglie

Se si desidera consentire al tenant S3 di clonare i dati dell'account e replicare gli oggetti bucket in un'altra griglia utilizzando una connessione a federazione di griglie, prima di avviare la procedura guidata,

confermare quanto segue:

- Lo hai fatto "configurazione della connessione a federazione di griglie".
- Lo stato della connessione è **connesso**.
- Si dispone dell'autorizzazione di accesso root.

Accedere e completare l'installazione guidata di S3

È possibile utilizzare l'installazione guidata S3 per configurare StorageGRID per l'utilizzo con un'applicazione S3. L'installazione guidata fornisce i valori necessari all'applicazione per accedere a un bucket StorageGRID e per salvare gli oggetti.

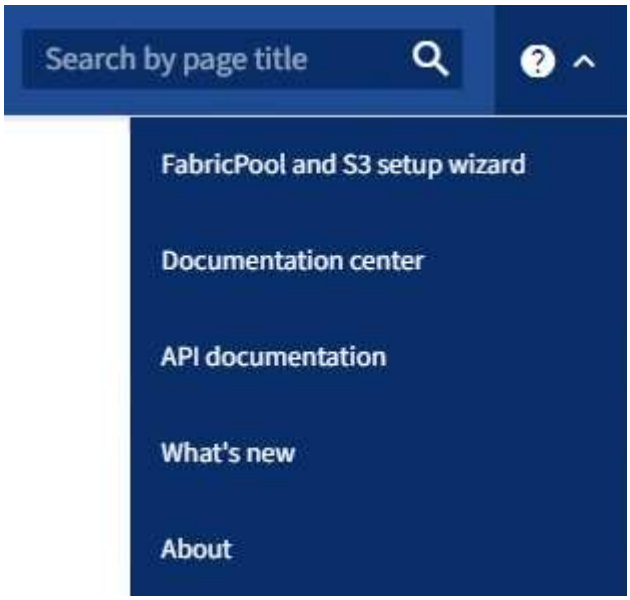
Prima di iniziare

- Hai il "Autorizzazione di accesso root".
- Hai esaminato il "considerazioni e requisiti" per utilizzare la procedura guidata.

Accedere alla procedura guidata

Fasi

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Se nella dashboard viene visualizzato il banner **FabricPool and S3 setup wizard**, selezionare il link nel banner. Se il banner non viene più visualizzato, selezionare l'icona della guida dalla barra di intestazione in Gestione griglia e selezionare **Installazione guidata FabricPool and S3**.



3. Nella sezione dell'applicazione S3 della pagina di installazione guidata di FabricPool e S3, selezionare **Configura ora**.

Fase 1 di 6: Configurare il gruppo ha

Un gruppo ha è un insieme di nodi che contengono ciascuno il servizio bilanciamento del carico StorageGRID. Un gruppo ha può contenere nodi gateway, nodi di amministrazione o entrambi.

È possibile utilizzare un gruppo ha per mantenere disponibili le connessioni dati S3. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle

operazioni S3.

Per ulteriori informazioni su questa attività, vedere "Gestire i gruppi ad alta disponibilità".

Fasi

1. Se si prevede di utilizzare un bilanciamento del carico esterno, non è necessario creare un gruppo ha. Selezionare **Ignora questo passaggio** e passare a. Fase 2 di 6: Configurare l'endpoint del bilanciamento del carico.
2. Per utilizzare il bilanciamento del carico StorageGRID, è possibile creare un nuovo gruppo ha o utilizzare un gruppo ha esistente.

Creare un gruppo ha

a. Per creare un nuovo gruppo ha, selezionare **Crea gruppo ha**.

b. Per la fase **inserire i dettagli**, completare i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome di visualizzazione univoco per questo gruppo ha.
Descrizione (opzionale)	La descrizione di questo gruppo ha.

c. Per il passo **Add interfaces**, selezionare le interfacce di nodo che si desidera utilizzare in questo gruppo ha.

   Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.

   È possibile selezionare uno o più nodi, ma è possibile selezionare una sola interfaccia per ciascun nodo.

d. Per la fase **prioritize interfaces**, determinare l'interfaccia primaria e le interfacce di backup per questo gruppo ha.

   Trascinare le righe per modificare i valori nella colonna **Ordine di priorità**.

   La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.

   Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi IP virtuali (VIP) si spostano nella 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. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

e. Per il passo **inserire gli indirizzi IP**, completare i seguenti campi.

Campo	Descrizione
Subnet CIDR	L'indirizzo della subnet VIP nella notazione CIDR e n. 8212; un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere bit host impostati. Ad esempio, `192.16.0.0/22`.
Indirizzo IP del gateway (opzionale)	Se gli indirizzi IP S3 utilizzati per accedere a StorageGRID non si trovano sulla stessa sottorete degli indirizzi VIP StorageGRID, inserire l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve trovarsi all'interno della subnet VIP.

Campo	Descrizione
Virtual IP address (Indirizzo IP virtuale)	Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP. Almeno un indirizzo deve essere IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

f. Selezionare **Create ha group** (Crea gruppo ha), quindi selezionare **Finish** (fine) per tornare all'installazione guidata S3.

g. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Utilizzare il gruppo ha esistente

a. Per utilizzare un gruppo ha esistente, selezionare il nome del gruppo ha dal menu **Select an ha group** (Seleziona un gruppo ha).

b. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Fase 2 di 6: Configurare l'endpoint del bilanciamento del carico

StorageGRID utilizza un bilanciamento del carico per gestire il carico di lavoro dalle applicazioni client. Il bilanciamento del carico massimizza la velocità e la capacità di connessione tra più nodi di storage.

È possibile utilizzare il servizio bilanciamento del carico StorageGRID, disponibile su tutti i nodi gateway e di amministrazione, oppure connettersi a un bilanciamento del carico esterno (di terze parti). Si consiglia di utilizzare il bilanciamento del carico StorageGRID.

Per ulteriori informazioni su questa attività, vedere "Considerazioni per il bilanciamento del carico".

Per utilizzare il servizio bilanciamento del carico di StorageGRID, selezionare la scheda **StorageGRID load balancer**, quindi creare o selezionare l'endpoint di bilanciamento del carico che si desidera utilizzare. Per utilizzare un bilanciamento del carico esterno, selezionare la scheda **bilanciamento del carico esterno** e fornire i dettagli sul sistema già configurato.

Creare l'endpoint

Fasi

1. Per creare un endpoint di bilanciamento del carico, selezionare **Crea endpoint**.
2. Per il passo **inserire i dettagli dell'endpoint**, completare i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433 per il primo endpoint creato, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché queste porte sono riservate sui nodi Admin. **Nota:** le porte utilizzate da altri servizi di rete non sono consentite. Vedere "Riferimento porta di rete".
Tipo di client	Deve essere **S3**.
Protocollo di rete	Selezionare **HTTPS**. **Nota**: La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

3. Per il passo **Select binding mode**, specificare la modalità di binding. La modalità di associazione controlla l'accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (impostazione predefinita)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione **Global** (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.

Modalità	Descrizione
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

4. Per la fase di accesso del tenant, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

5. Per il passo **Allega certificato**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Carica certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato dalla CA, una chiave privata del certificato e un bundle CA opzionale.
Generare un certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciamento del carico" per informazioni dettagliate su cosa inserire.
Utilizza il certificato StorageGRID S3 e Swift	Utilizzare questa opzione solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID. Vedere "Configurare i certificati API S3 e Swift" per ulteriori informazioni.

6. Selezionare **fine** per tornare all'installazione guidata S3.
7. Selezionare **continua** per passare al punto tenant e bucket.

> Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Utilizzare l'endpoint del bilanciamento del carico esistente

Fasi

1. Per utilizzare un endpoint esistente, selezionarne il nome dal campo **Select a load balancer endpoint**.

2. Selezionare **continua** per passare al punto tenant e bucket.

Utilizzare un bilanciamento del carico esterno

Fasi

1. Per utilizzare un bilanciamento del carico esterno, completare i seguenti campi.

Campo	Descrizione
FQDN	Il nome di dominio completo (FQDN) del bilanciamento del carico esterno.
Porta	Il numero di porta che l'applicazione S3 utilizzerà per connettersi al bilanciamento del carico esterno.
Certificato	Copiare il certificato del server per il bilanciamento del carico esterno e incollarlo in questo campo.

2. Selezionare **continua** per passare al punto tenant e bucket.

Fase 3 di 6: Creazione di tenant e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per memorizzare e recuperare oggetti in StorageGRID. Ogni tenant dispone di utenti, chiavi di accesso, bucket, oggetti e un set specifico di funzionalità. È necessario creare il tenant prima di poter creare il bucket che l'applicazione S3 utilizzerà per memorizzare i propri oggetti.

Un bucket è un container utilizzato per memorizzare gli oggetti e i metadati degli oggetti di un tenant. Anche se alcuni tenant potrebbero avere molti bucket, la procedura guidata consente di creare un tenant e un bucket nel modo più rapido e semplice. Puoi utilizzare il tenant Manager in un secondo momento per aggiungere altri bucket necessari.

È possibile creare un nuovo tenant da utilizzare per questa applicazione S3. In alternativa, è anche possibile creare un bucket per il nuovo tenant. Infine, è possibile consentire alla procedura guidata di creare le chiavi di accesso S3 per l'utente root del tenant.

Per ulteriori informazioni su questa attività, vedere "Creare un account tenant" e. "Creare un bucket S3".

Fasi

1. Selezionare **Crea tenant**.
2. Per la procedura di inserimento dei dettagli, immettere le seguenti informazioni.

Campo	Descrizione
Nome	Un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Una volta creato, l'account tenant riceve un ID account numerico univoco.
Descrizione (opzionale)	Una descrizione che aiuta a identificare il tenant.

Campo	Descrizione
Tipo di client	Il tipo di protocollo client utilizzato dal tenant. Per l'installazione guidata S3, è selezionato **S3** e il campo è disattivato.
Quota di storage (opzionale)	Se si desidera che il tenant disponga di una quota di storage, un valore numerico per la quota e le unità.

3. Selezionare **continua**.
4. Se si desidera, selezionare le autorizzazioni desiderate per il tenant.

> Alcune di queste autorizzazioni hanno requisiti aggiuntivi. Per ulteriori informazioni, selezionare l'icona della guida per ciascuna autorizzazione.

Permesso	Se selezionato…
Consentire i servizi della piattaforma	Il tenant può utilizzare servizi della piattaforma S3 come CloudMirror. Vedere "Gestire i servizi della piattaforma per gli account tenant S3".
Utilizza la propria origine di identità	Il tenant può configurare e gestire la propria origine di identità per gruppi e utenti federati. Questa opzione è disattivata se si dispone di "SSO configurato" Per il tuo sistema StorageGRID.
Consenti selezione S3	Il tenant può emettere richieste API S3 SelectObjectContent per filtrare e recuperare i dati degli oggetti. Vedere "Manage S3 (Gestisci S3): Selezionare per gli account tenant". **Importante**: Le richieste SelectObjectContent possono ridurre le performance di bilanciamento del carico per tutti i client S3 e per tutti i tenant. Attivare questa funzione solo quando richiesto e solo per tenant attendibili.
USA connessione a federazione di griglie	Il tenant può utilizzare una connessione a federazione di grid. Selezionando questa opzione: • Consente di clonare questo tenant e tutti i gruppi tenant e gli utenti aggiunti all'account da questa griglia (la *griglia di origine*) all'altra griglia della connessione selezionata (la *griglia di destinazione*). • Consente a questo tenant di configurare la replica cross-grid tra i bucket corrispondenti su ogni grid. Vedere "Gestire i tenant consentiti per la federazione di grid".

5. Se si seleziona **Usa connessione federazione griglia**, selezionare una delle connessioni federazione griglia disponibili.
6. Definire l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del sistema StorageGRID "federazione delle identità", "SSO (Single Sign-on)", o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

7. Se si desidera che la procedura guidata crei l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root, selezionare **Crea automaticamente la chiave di accesso S3 dell'utente root**.

   Selezionare questa opzione se l'unico utente per il tenant sarà l'utente root. Se altri utenti utilizzeranno questo tenant, utilizzare Tenant Manager per configurare le chiavi e le autorizzazioni.

8. Selezionare **continua**.
9. Per il passo Create bucket, è possibile creare un bucket per gli oggetti del tenant. Altrimenti, selezionare **Create tenant without bucket** (Crea tenant senza bucket) per accedere a. fase di download dei dati.

   Se S3 Object Lock è attivato per la griglia, il bucket creato in questa fase non ha S3 Object Lock abilitato. Se è necessario utilizzare un bucket S3 Object Lock per questa applicazione S3, selezionare **Create tenant without bucket** (Crea tenant senza bucket). Quindi, utilizzare Tenant Manager per "creare il bucket" invece.

   a. Immettere il nome del bucket utilizzato dall'applicazione S3. Ad esempio, `S3-bucket`.

      Non è possibile modificare il nome del bucket dopo averlo creato.

   b. Selezionare **Region** per questo bucket.

      Utilizzare la regione predefinita (`us-east-1`) A meno che non si preveda di utilizzare ILM in futuro per filtrare gli oggetti in base all'area del bucket.

   c. Selezionare **Enable object versioning** (attiva versione oggetto) se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket.
   d. Selezionare **Create tenant and bucket** (Crea tenant e bucket) e passare alla fase di download dei dati.

fase 4 di 6: Download dei dati

Nella fase di download dei dati, è possibile scaricare uno o due file per salvare i dettagli di ciò che si è appena configurato.

Fasi

1. Se è stato selezionato **Create root user S3 access key automatically** (Crea chiave di accesso S3 utente root automaticamente), eseguire una o entrambe le operazioni seguenti:
   - Selezionare **Download access key** (Scarica chiavi di accesso) per scaricare un `.csv` File contenente il nome dell'account tenant, l'ID della chiave di accesso e la chiave di accesso segreta.
   - Selezionare l'icona di copia ( ) Per copiare l'ID della chiave di accesso e la chiave di accesso segreta negli Appunti.
2. Selezionare **Download Configuration Values** (Scarica valori di configurazione) per scaricare un `.txt` file contenente le impostazioni per l'endpoint del bilanciamento del carico, il tenant, il bucket e l'utente root.
3. Salvare queste informazioni in una posizione sicura.

> Non chiudere questa pagina prima di aver copiato entrambi i tasti di accesso. I tasti non saranno disponibili dopo la chiusura di questa pagina. Assicurarsi di salvare queste informazioni in una posizione sicura perché possono essere utilizzate per ottenere dati dal sistema StorageGRID.

4. Se richiesto, selezionare la casella di controllo per confermare che le chiavi sono state scaricate o copiate.
5. Selezionare **continua** per passare alla regola ILM e al passaggio del criterio.

Fase 5 di 6: Esaminare la regola ILM e il criterio ILM per S3

Le regole ILM (Information Lifecycle Management) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel sistema StorageGRID. Il criterio ILM incluso in StorageGRID crea due copie replicate di tutti gli oggetti. Questo criterio è attivo fino a quando non si attiva almeno un nuovo criterio.

Fasi

1. Esaminare le informazioni fornite nella pagina.
2. Se si desidera aggiungere istruzioni specifiche per gli oggetti appartenenti al nuovo tenant o bucket, creare una nuova regola e una nuova policy. Vedere "Creare una regola ILM" e. "Criteri ILM: Panoramica".
3. Selezionare **ho esaminato questi passaggi e ho compreso cosa devo fare**.
4. Selezionare la casella di controllo per indicare che si comprende cosa fare in seguito.
5. Selezionare **continua** per accedere a **Riepilogo**.

Fase 6 di 6: Riepilogo

Fasi

1. Esaminare il riepilogo.
2. Prendere nota dei dettagli nei passaggi successivi, che descrivono la configurazione aggiuntiva che potrebbe essere necessaria prima di connettersi al client S3. Ad esempio, selezionando **Accedi come root** si passa a Tenant Manager, dove è possibile aggiungere utenti tenant, creare bucket aggiuntivi e aggiornare le impostazioni del bucket.
3. Selezionare **fine**.
4. Configurare l'applicazione utilizzando il file scaricato da StorageGRID o i valori ottenuti manualmente.

Gestire i gruppi ha

È possibile raggruppare le interfacce di rete di più nodi Admin e Gateway in un gruppo ad alta disponibilità (ha). Se l'interfaccia attiva nel gruppo ha non riesce, un'interfaccia di backup può gestire il carico di lavoro.

Che cos'è un gruppo ha?

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.

Ciascun gruppo ha fornisce l'accesso ai servizi condivisi sui nodi selezionati.

- I gruppi HA che includono nodi gateway, nodi di amministrazione o entrambi forniscono connessioni dati altamente disponibili per i client S3 e Swift.
- I gruppi HA che includono solo nodi Admin forniscono connessioni altamente disponibili al Grid Manager e al Tenant Manager.
- Un gruppo ha che include solo appliance di servizi e nodi software basati su VMware può offrire connessioni ad alta disponibilità per "S3 tenant che utilizzano S3 Select".
  I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.

Come crei un gruppo ha?

1. Selezionare un'interfaccia di rete per uno o più nodi Admin o Gateway. È possibile utilizzare un'interfaccia Grid Network (eth0), un'interfaccia Client Network (eth2), un'interfaccia VLAN o un'interfaccia di accesso aggiunta al nodo.

   > ⓘ Non è possibile aggiungere un'interfaccia a un gruppo ha se dispone di un indirizzo IP assegnato da DHCP.

2. Specificare un'interfaccia come principale. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.
3. È possibile determinare l'ordine di priorità per le interfacce di backup.
4. Al gruppo vengono assegnati da uno a 10 indirizzi IP virtuali (VIP). Le applicazioni client possono utilizzare uno qualsiasi di questi indirizzi VIP per connettersi a StorageGRID.

Per istruzioni, vedere "Configurare i gruppi ad alta disponibilità".

Che cos'è l'interfaccia attiva?

Durante il normale funzionamento, tutti gli indirizzi VIP per il gruppo ha vengono aggiunti all'interfaccia primaria, che è la prima interfaccia nell'ordine di priorità. Finché l'interfaccia primaria rimane disponibile, viene utilizzata quando i client si connettono a qualsiasi indirizzo VIP del gruppo. Cioè, durante il normale funzionamento, l'interfaccia primaria è l'interfaccia "attiva" per il gruppo.

Analogamente, durante il normale funzionamento, qualsiasi interfaccia a priorità inferiore per il gruppo ha agisce come interfacce di "backup". Queste interfacce di backup non vengono utilizzate a meno che l'interfaccia primaria (attualmente attiva) non diventi disponibile.

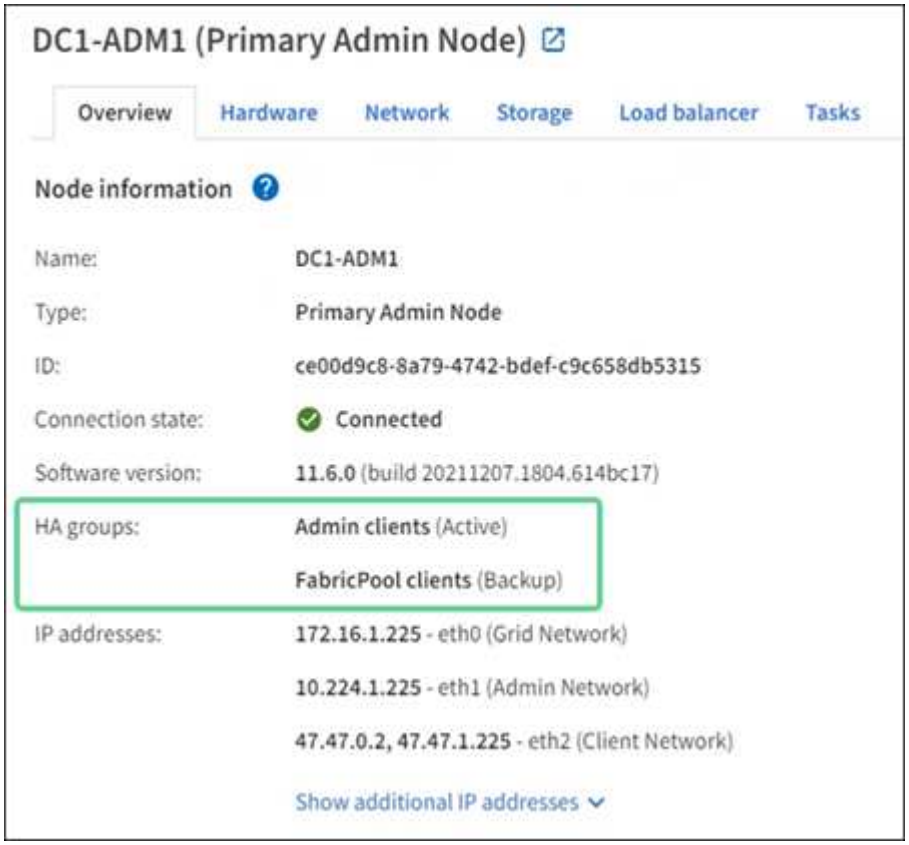
Visualizzare lo stato corrente del gruppo ha di un nodo

Per verificare se un nodo è assegnato a un gruppo ha e determinarne lo stato corrente, selezionare **NODES** > ***Node***.

Se la scheda **Panoramica** include una voce per **gruppi ha**, il nodo viene assegnato ai gruppi ha elencati. Il valore dopo il nome del gruppo corrisponde allo stato corrente del nodo nel gruppo ha:

- **Attivo**: Il gruppo ha è attualmente ospitato su questo nodo.
- **Backup**: Il gruppo ha non sta attualmente utilizzando questo nodo; si tratta di un'interfaccia di backup.
- **Arrestato**: Il gruppo ha non può essere ospitato su questo nodo perché il servizio ad alta disponibilità (keepalived) è stato arrestato manualmente.
- **Fault**: Il gruppo ha non può essere ospitato su questo nodo a causa di uno o più dei seguenti fattori:
  - Il servizio Load Balancer (nginx-gw) non è in esecuzione sul nodo.
  - L'interfaccia eth0 o VIP del nodo non è disponibile.
  - Il nodo non è attivo.

In questo esempio, il nodo di amministrazione primario è stato aggiunto a due gruppi ha. Questo nodo è attualmente l'interfaccia attiva per il gruppo di client di amministrazione e un'interfaccia di backup per il gruppo di client FabricPool.



Cosa succede quando l'interfaccia attiva non funziona?

L'interfaccia che attualmente ospita gli indirizzi VIP è l'interfaccia attiva. Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi VIP si spostano sulla prima interfaccia di backup disponibile nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano alla successiva interfaccia di backup disponibile e così via.

Il failover può essere attivato per uno dei seguenti motivi:

- Il nodo su cui è configurata l'interfaccia non funziona.
- Il nodo su cui è configurata l'interfaccia perde la connettività con tutti gli altri nodi per almeno 2 minuti.
- L'interfaccia attiva non funziona.
- Il servizio Load Balancer si arresta.
- Il servizio High Availability si interrompe.

> Il failover potrebbe non essere attivato da guasti di rete esterni al nodo che ospita l'interfaccia attiva. Allo stesso modo, il failover non viene attivato dai servizi per Grid Manager o Tenant Manager.

Il processo di failover richiede in genere solo pochi secondi ed è abbastanza rapido da consentire alle applicazioni client di avere un impatto minimo e può fare affidamento sui normali comportamenti di ripetizione per continuare a funzionare.

Quando il guasto viene risolto e un'interfaccia con priorità più alta diventa nuovamente disponibile, gli indirizzi VIP vengono automaticamente spostati nell'interfaccia con priorità più alta disponibile.

Come vengono utilizzati i gruppi ha?

È possibile utilizzare gruppi ad alta disponibilità (ha) per fornire connessioni altamente disponibili a StorageGRID per i dati a oggetti e per l'utilizzo amministrativo.

- Un gruppo ha può fornire connessioni amministrative altamente disponibili al Grid Manager o al tenant Manager.
- Un gruppo ha può fornire connessioni dati altamente disponibili per i client S3 e Swift.
- Un gruppo ha che contiene una sola interfaccia consente di fornire molti indirizzi VIP e di impostare esplicitamente gli indirizzi IPv6.

Un gruppo ha può fornire alta disponibilità solo se tutti i nodi inclusi nel gruppo forniscono gli stessi servizi. Quando si crea un gruppo ha, aggiungere interfacce dai tipi di nodi che forniscono i servizi richiesti.

- **Admin Node**: Include il servizio Load Balancer e abilita l'accesso al Grid Manager o al Tenant Manager.
- **Gateway Node**: Include il servizio Load Balancer.

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso a Grid Manager	• Nodo amministratore primario (**primario**) • Nodi amministrativi non primari **Nota:** l'Admin Node primario deve essere l'interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.
Accesso solo al tenant manager	• Nodi di amministrazione primari o non primari

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso client S3 o Swift — Servizio Load Balancer	• Nodi di amministrazione • Nodi gateway
Accesso al client S3 per "S3 Seleziona"	• Appliance di servizi • Nodi software basati su VMware **Nota**: I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.

Limitazioni dell'utilizzo di gruppi ha con Grid Manager o Tenant Manager

Se un servizio Grid Manager o Tenant Manager non funziona, il failover del gruppo ha non viene attivato.

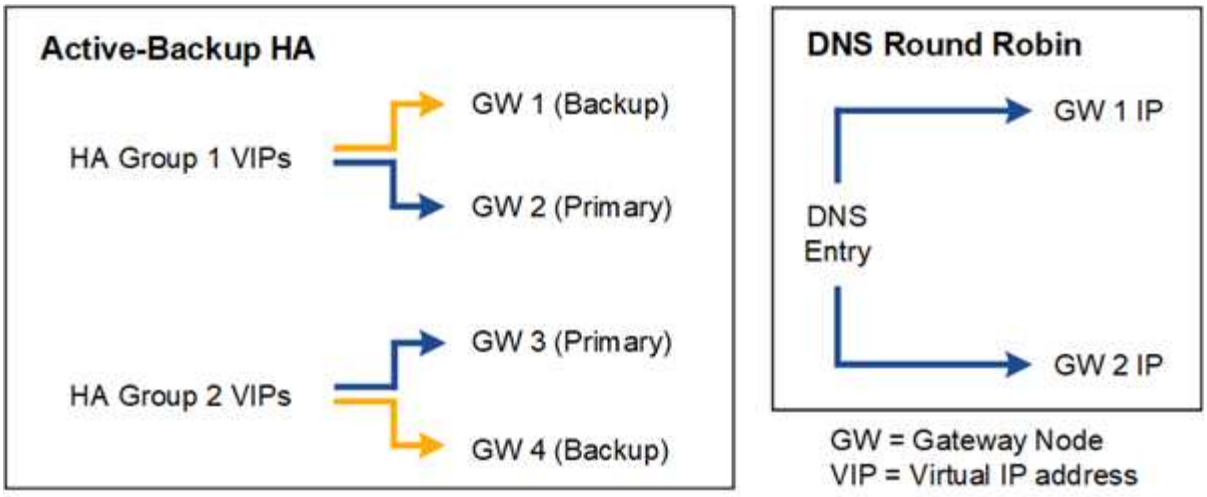
Se hai effettuato l'accesso a Grid Manager o a Tenant Manager quando si verifica il failover, sei disconnesso e devi effettuare nuovamente l'accesso per riprendere l'attività.

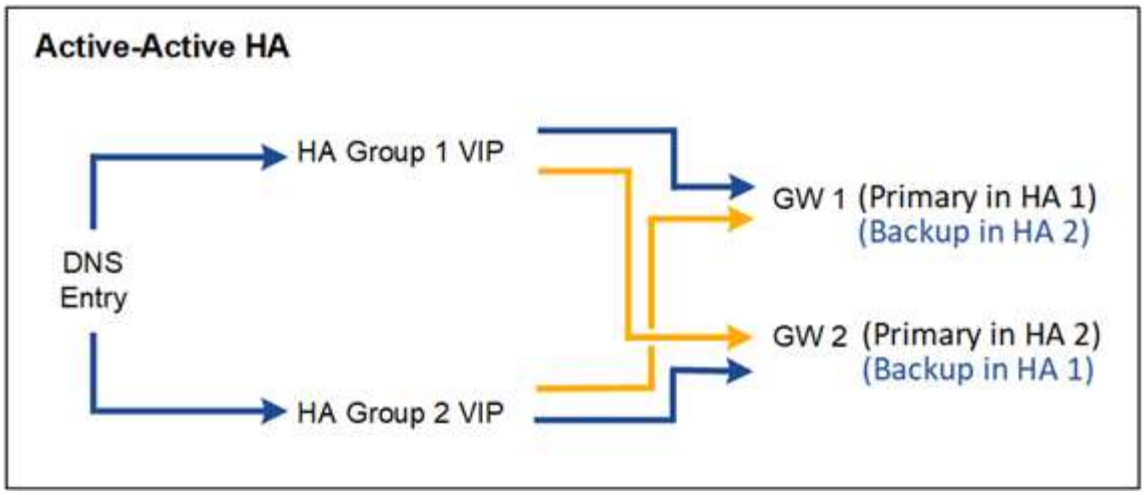
Non è possibile eseguire alcune procedure di manutenzione quando il nodo di amministrazione primario non è disponibile. Durante il failover, è possibile utilizzare Grid Manager per monitorare il sistema StorageGRID.

Opzioni di configurazione per i gruppi ha

I seguenti diagrammi forniscono esempi di diversi modi per configurare i gruppi ha. Ogni opzione presenta vantaggi e svantaggi.

Nei diagrammi, il blu indica l'interfaccia principale nel gruppo ha e il giallo indica l'interfaccia di backup nel gruppo ha.





La tabella riassume i vantaggi di ciascuna configurazione ha mostrata nel diagramma.

Configurazione	Vantaggi	Svantaggi
Ha Active-Backup	• Gestito da StorageGRID senza dipendenze esterne. • Failover rapido.	• Solo un nodo in un gruppo ha è attivo. Almeno un nodo per gruppo ha sarà inattivo.
DNS Round Robin	• Maggiore throughput aggregato. • Nessun host inattivo.	• Failover lento, che potrebbe dipendere dal comportamento del client. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Ha bisogno di un controllo dello stato di salute implementato dal cliente.

Configurazione	Vantaggi	Svantaggi
Ha Active-Active	• Il traffico viene distribuito tra più gruppi ha. • Throughput aggregato elevato che si adatta al numero di gruppi ha. • Failover rapido.	• Più complesso da configurare. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Ha bisogno di un controllo dello stato di salute implementato dal cliente.

Configurare i gruppi ad alta disponibilità

È possibile configurare i gruppi ad alta disponibilità (ha) per fornire l'accesso altamente disponibile ai servizi sui nodi Admin o Gateway.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Se si intende utilizzare un'interfaccia VLAN in un gruppo ha, l'interfaccia VLAN è stata creata. Vedere "Configurare le interfacce VLAN".
- Se si intende utilizzare un'interfaccia di accesso per un nodo in un gruppo ha, l'interfaccia è stata creata:
  - **Red Hat Enterprise Linux (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"
  - **Linux (dopo l'installazione del nodo)**: "Linux: Aggiunta di interfacce di accesso o trunk a un nodo"
  - **VMware (dopo l'installazione del nodo)**: "VMware: Aggiunta di interfacce di accesso o trunk a un nodo"

Creare un gruppo ad alta disponibilità

Quando si crea un gruppo ad alta disponibilità, selezionare una o più interfacce e organizzarle in ordine di priorità. Quindi, assegnare uno o più indirizzi VIP al gruppo.

Un'interfaccia deve essere un nodo gateway o un nodo amministratore per essere incluso in un gruppo ha. Un gruppo ha può utilizzare solo un'interfaccia per un dato nodo; tuttavia, altre interfacce per lo stesso nodo possono essere utilizzate in altri gruppi ha.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.
2. Selezionare **Crea**.

Inserire i dettagli del gruppo ha

Fasi

1. Fornire un nome univoco per il gruppo ha.
2. Facoltativamente, inserire una descrizione per il gruppo ha.

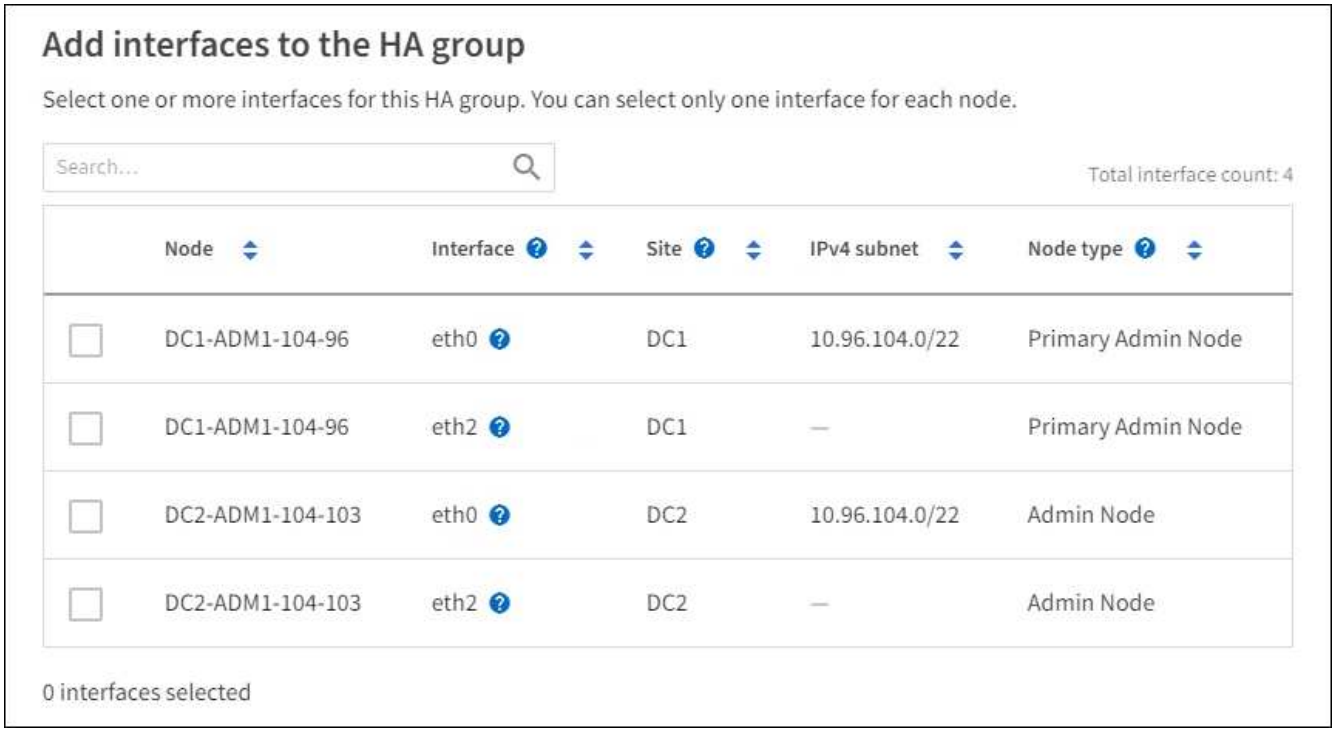
3. Selezionare **continua**.

Aggiungere interfacce al gruppo ha

Fasi

1. Selezionare una o più interfacce da aggiungere a questo gruppo ha.

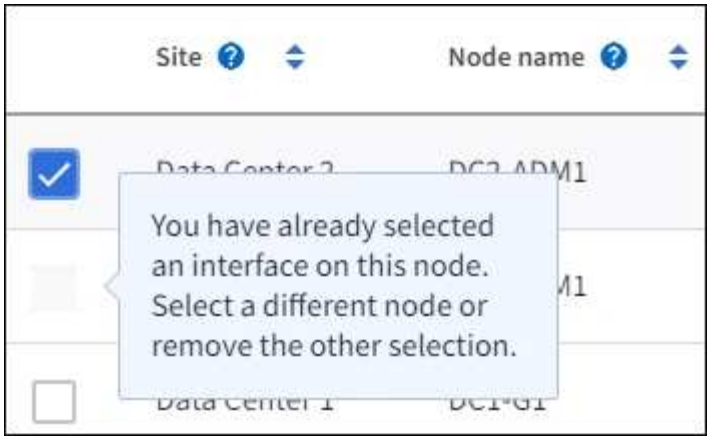
   Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.



> Dopo aver creato un'interfaccia VLAN, attendere fino a 5 minuti per visualizzare la nuova interfaccia nella tabella.

Linee guida per la selezione delle interfacce

- Selezionare almeno un'interfaccia.
- È possibile selezionare una sola interfaccia per un nodo.
- Se il gruppo ha è per la protezione ha dei servizi Admin Node, che includono Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi Admin.
- Se il gruppo ha è per la protezione ha del traffico client S3 o Swift, selezionare le interfacce sui nodi di amministrazione, sui nodi gateway o su entrambi.
- Se si selezionano interfacce su diversi tipi di nodi, viene visualizzata una nota informativa. Si ricorda che, in caso di failover, i servizi forniti dal nodo precedentemente attivo potrebbero non essere disponibili sul nodo appena attivo. Ad esempio, un nodo gateway di backup non può fornire la protezione ha dei servizi del nodo amministratore. Analogamente, un nodo Admin di backup non può eseguire tutte le procedure di manutenzione che il nodo Admin primario può fornire.
- Se non è possibile selezionare un'interfaccia, la relativa casella di controllo è disattivata. Il suggerimento fornisce ulteriori informazioni.



- Non è possibile selezionare un'interfaccia se il relativo valore di sottorete o il gateway è in conflitto con un'altra interfaccia selezionata.
- Non è possibile selezionare un'interfaccia configurata se non dispone di un indirizzo IP statico.

2. Selezionare **continua**.

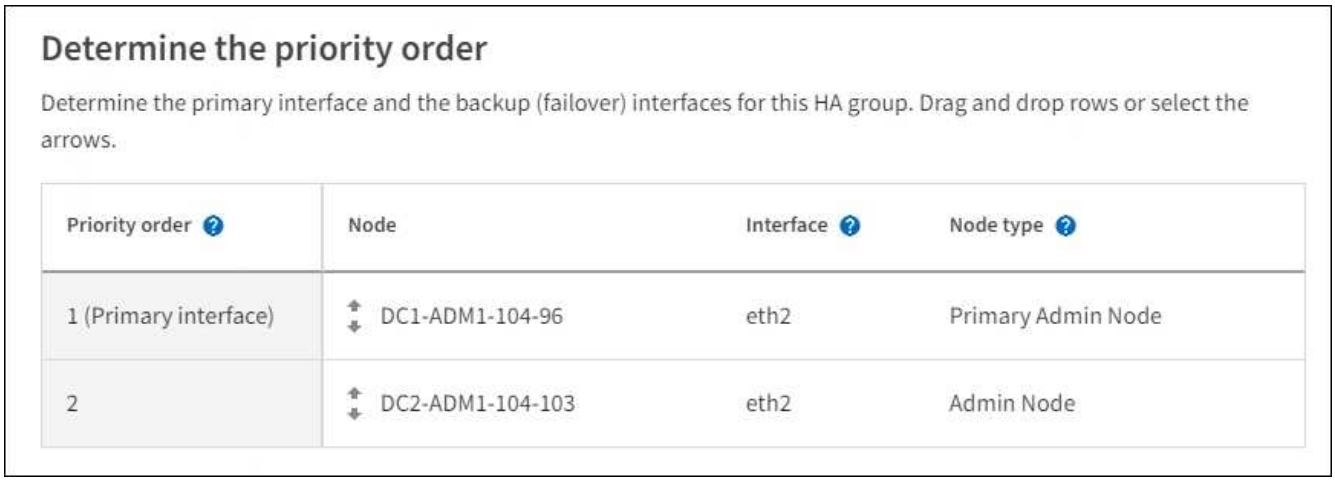
Determinare l'ordine di priorità

Se il gruppo ha include più di un'interfaccia, è possibile determinare quale sia l'interfaccia primaria e quali siano le interfacce di backup (failover). Se l'interfaccia principale non funziona, gli indirizzi VIP passano all'interfaccia con la priorità più alta disponibile. Se l'interfaccia non funziona, gli indirizzi VIP passano alla successiva interfaccia con la priorità più alta disponibile e così via.

Fasi

1. Trascinare le righe nella colonna **Ordine di priorità** per determinare l'interfaccia primaria e le interfacce di backup.

   La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.



> Se il gruppo ha fornisce l'accesso a Grid Manager, è necessario selezionare un'interfaccia sul nodo di amministrazione primario come interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

2. Selezionare **continua**.

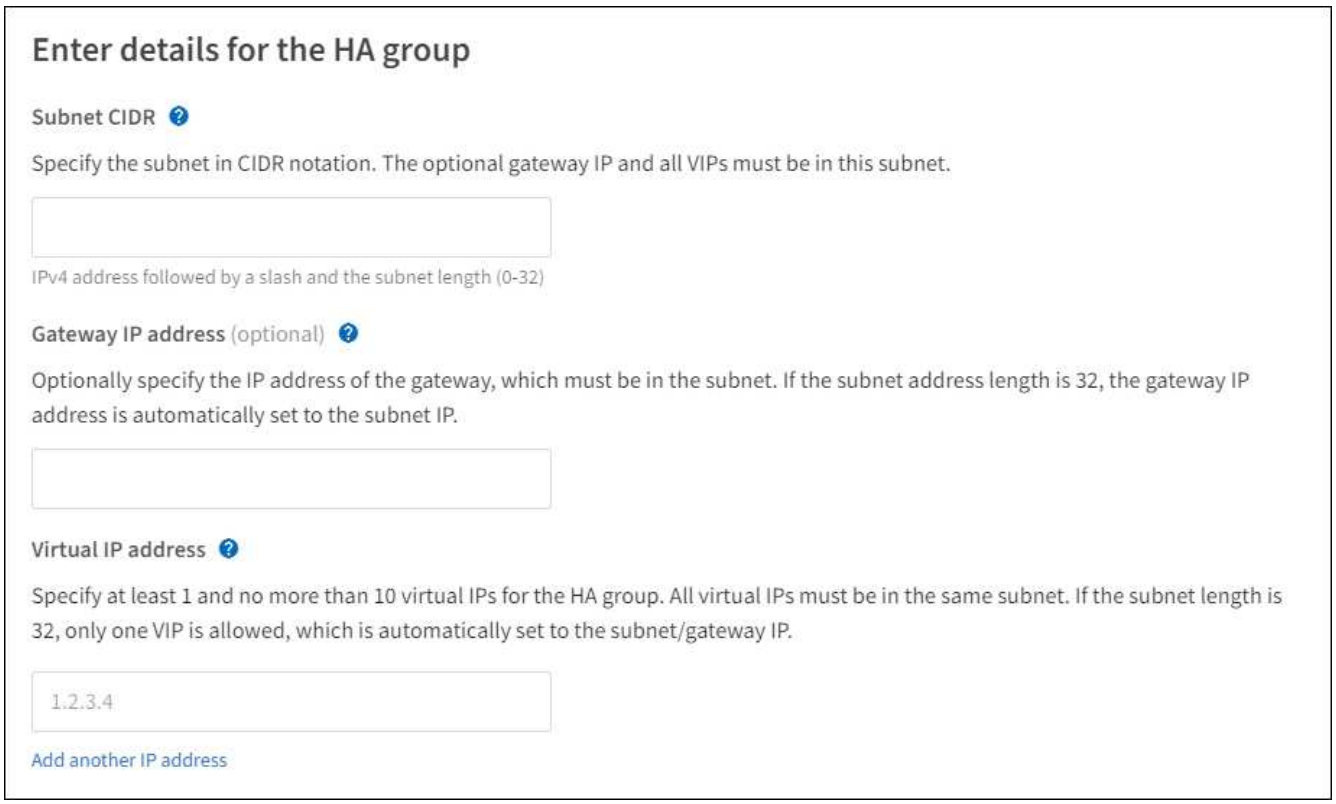
Inserire gli indirizzi IP

Fasi

1. Nel campo **Subnet CIDR**, specificare la subnet VIP nella notazione CIDR: Un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32).

   L'indirizzo di rete non deve avere bit host impostati. Ad esempio, `192.16.0.0/22`.

   > Se si utilizza un prefisso a 32 bit, l'indirizzo di rete VIP funge anche da indirizzo del gateway e da indirizzo VIP.

2. Facoltativamente, se un client S3, Swift, amministrativo o tenant accede a questi indirizzi VIP da una sottorete diversa, immettere l'indirizzo IP del gateway*. L'indirizzo del gateway deve trovarsi all'interno della subnet VIP.

   Gli utenti client e admin utilizzeranno questo gateway per accedere agli indirizzi IP virtuali.

3. Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP e tutti saranno attivi contemporaneamente sull'interfaccia attiva.

   Specificare almeno un indirizzo IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

4. Selezionare **Create ha group** (Crea gruppo ha) e selezionare **Finish** (fine).

   Viene creato il gruppo ha ed è ora possibile utilizzare gli indirizzi IP virtuali configurati.

Passi successivi

Se si utilizza questo gruppo ha per il bilanciamento del carico, creare un endpoint per il bilanciamento del carico per determinare il protocollo di porta e di rete e per allegare eventuali certificati richiesti. Vedere "Configurare gli endpoint del bilanciamento del carico".

Modificare un gruppo ad alta disponibilità

È possibile modificare un gruppo ad alta disponibilità (ha) per modificarne nome e descrizione, aggiungere o rimuovere interfacce, modificare l'ordine di priorità o aggiungere o aggiornare indirizzi IP virtuali.

Ad esempio, potrebbe essere necessario modificare un gruppo ha se si desidera rimuovere il nodo associato a un'interfaccia selezionata in una procedura di decommissionamento del sito o del nodo.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.

   La pagina High Availability groups (gruppi ad alta disponibilità) mostra tutti i gruppi ha esistenti.

2. Selezionare la casella di controllo del gruppo ha che si desidera modificare.
3. Eseguire una delle seguenti operazioni in base a quanto si desidera aggiornare:
   - Selezionare **azioni** > **Modifica indirizzo IP virtuale** per aggiungere o rimuovere indirizzi VIP.
   - Selezionare **azioni** > **Modifica gruppo ha** per aggiornare il nome o la descrizione del gruppo, aggiungere o rimuovere interfacce, modificare l'ordine di priorità o aggiungere o rimuovere indirizzi VIP.
4. Se si seleziona **Modifica indirizzo IP virtuale**:
   a. Aggiornare gli indirizzi IP virtuali per il gruppo ha.
   b. Selezionare **Salva**.
   c. Selezionare **fine**.
5. Se si seleziona **Edit ha group** (Modifica gruppo ha):
   a. Facoltativamente, aggiornare il nome o la descrizione del gruppo.
   b. Facoltativamente, selezionare o deselezionare le caselle di controllo per aggiungere o rimuovere interfacce.

      Se il gruppo ha fornisce l'accesso a Grid Manager, è necessario selezionare un'interfaccia sul nodo di amministrazione primario come interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario

   c. Facoltativamente, trascinare le righe per modificare l'ordine di priorità dell'interfaccia primaria e delle interfacce di backup per questo gruppo ha.
   d. Facoltativamente, aggiornare gli indirizzi IP virtuali.
   e. Selezionare **Salva**, quindi **fine**.

Rimuovere un gruppo ad alta disponibilità

È possibile rimuovere uno o più gruppi ad alta disponibilità (ha) alla volta.

Non è possibile rimuovere un gruppo ha se è associato a un endpoint di bilanciamento del carico. Per eliminare un gruppo ha, è necessario rimuoverlo da tutti gli endpoint del bilanciamento del carico che lo utilizzano.

Per evitare interruzioni del client, aggiornare le applicazioni client S3 o Swift prima di rimuovere un gruppo ha. Aggiornare ciascun client per la connessione utilizzando un altro indirizzo IP, ad esempio l'indirizzo IP virtuale di un gruppo ha diverso o l'indirizzo IP configurato per un'interfaccia durante l'installazione.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.
2. Esaminare la colonna **endpoint del bilanciamento del carico** per ciascun gruppo ha che si desidera rimuovere. Se sono elencati endpoint del bilanciamento del carico:
   a. Andare a **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
   b. Selezionare la casella di controllo per l'endpoint.
   c. Selezionare **azioni** > **Modifica modalità di associazione endpoint**.
   d. Aggiornare la modalità di binding per rimuovere il gruppo ha.
   e. Selezionare **Save Changes** (Salva modifiche).
3. Se non sono elencati endpoint del bilanciamento del carico, selezionare la casella di controllo per ciascun gruppo ha che si desidera rimuovere.
4. Selezionare **azioni** > **Rimuovi gruppo ha**.
5. Esaminare il messaggio e selezionare **Delete ha group** (Elimina gruppo ha) per confermare la selezione.

   Tutti i gruppi ha selezionati vengono rimossi. Nella pagina dei gruppi ad alta disponibilità viene visualizzato un banner verde di successo.

Gestire il bilanciamento del carico

Considerazioni per il bilanciamento del carico

È possibile utilizzare il bilanciamento del carico per gestire i carichi di lavoro di acquisizione e recupero dai client S3 e Swift.

Cos'è il bilanciamento del carico?

Quando un'applicazione client salva o recupera i dati da un sistema StorageGRID, StorageGRID utilizza un sistema di bilanciamento del carico per gestire il carico di lavoro di acquisizione e recupero. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo il carico di lavoro tra più nodi di storage.

Il servizio bilanciamento del carico StorageGRID viene installato su tutti i nodi di amministrazione e su tutti i nodi gateway e fornisce il bilanciamento del carico di livello 7. Esegue la terminazione TLS (Transport Layer Security) delle richieste client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage.

Il servizio Load Balancer su ciascun nodo funziona in modo indipendente quando si inoltra il traffico client ai nodi di storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU.

Anche se il servizio bilanciamento del carico di StorageGRID è il meccanismo di bilanciamento del carico consigliato, potrebbe essere necessario integrare un bilanciamento del carico di terze parti. Per informazioni, contattare il rappresentante commerciale NetApp o visitare il sito Web all'indirizzo "TR-4626: Bilanciatori di carico globali e di terze parti StorageGRID".

Quanti nodi per il bilanciamento del carico sono necessari?

Come Best practice generale, ogni sito del sistema StorageGRID deve includere due o più nodi nel servizio bilanciamento del carico. Ad esempio, un sito potrebbe includere due nodi gateway o sia un nodo amministratore che un nodo gateway. Assicurati che sia disponibile un'infrastruttura di rete, hardware o virtualizzazione adeguata per ogni nodo di bilanciamento del carico, sia che si utilizzino appliance per i servizi, nodi bare metal o nodi basati su macchine virtuali (VM).

Che cos'è un endpoint di bilanciamento del carico?

Un endpoint di bilanciamento del carico definisce la porta e il protocollo di rete (HTTPS o HTTP) che le richieste dell'applicazione client in entrata e in uscita utilizzeranno per accedere ai nodi che contengono il servizio Load Balancer. L'endpoint definisce anche il tipo di client (S3 o Swift), la modalità di binding e, facoltativamente, un elenco di tenant consentiti o bloccati.

Per creare un endpoint di bilanciamento del carico, selezionare **CONFIGURAZIONE** > **rete** > **endpoint di bilanciamento del carico** oppure completare la configurazione guidata di FabricPool e S3. Per istruzioni:

- "Configurare gli endpoint del bilanciamento del carico"
- "Utilizzare l'installazione guidata S3"
- "Utilizzare l'installazione guidata di FabricPool"

Considerazioni per la porta

Per impostazione predefinita, la porta di un endpoint di bilanciamento del carico è 10433 per il primo endpoint creato, ma è possibile specificare qualsiasi porta esterna inutilizzata compresa tra 1 e 65535. Se si utilizza la porta 80 o 443, l'endpoint utilizzerà il servizio Load Balancer solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione. Se si utilizza la stessa porta per più di un endpoint, è necessario specificare una modalità di binding diversa per ciascun endpoint.

Le porte utilizzate da altri servizi di rete non sono consentite. Vedere "Riferimento porta di rete".

Considerazioni sul protocollo di rete

Nella maggior parte dei casi, le connessioni tra le applicazioni client e StorageGRID devono utilizzare la crittografia TLS (Transport Layer Security). La connessione a StorageGRID senza crittografia TLS è supportata ma non consigliata, soprattutto negli ambienti di produzione. Quando si seleziona il protocollo di rete per l'endpoint del bilanciamento del carico StorageGRID, selezionare **HTTPS**.

Considerazioni per i certificati endpoint del bilanciamento del carico

Se si seleziona **HTTPS** come protocollo di rete per l'endpoint del bilanciamento del carico, è necessario fornire un certificato di sicurezza. È possibile utilizzare una di queste tre opzioni quando si crea l'endpoint del bilanciamento del carico:

- **Caricare un certificato firmato (consigliato)**. Il certificato può essere firmato da un'autorità di certificazione pubblica o privata. L'utilizzo di un certificato del server CA pubblicamente attendibile per proteggere la connessione è la procedura consigliata. A differenza dei certificati generati, i certificati firmati

da una CA possono essere ruotati senza interruzioni, in modo da evitare problemi di scadenza.

Prima di creare l'endpoint del bilanciamento del carico, è necessario ottenere i seguenti file:

- Il file di certificato del server personalizzato.
- Il file di chiave privata del certificato del server personalizzato.
- Facoltativamente, un bundle CA dei certificati di ciascuna autorità di certificazione di emissione intermedia.

- **Generare un certificato autofirmato**.
- **Utilizzare il certificato globale StorageGRID S3 e Swift**. È necessario caricare o generare una versione personalizzata del certificato prima di poterla selezionare per l'endpoint del bilanciamento del carico. Vedere "Configurare i certificati API S3 e Swift".

Di quali valori ho bisogno?

Per creare il certificato, è necessario conoscere tutti i nomi di dominio e gli indirizzi IP utilizzati dalle applicazioni client S3 o Swift per accedere all'endpoint.

La voce **Subject DN** (Distinguished Name) per il certificato deve includere il nome di dominio completo che l'applicazione client utilizzerà per StorageGRID. Ad esempio:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Se necessario, il certificato può utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi Admin e Gateway che eseguono il servizio Load Balancer. Ad esempio, `*.storagegrid.example.com` utilizza il carattere jolly * per rappresentare `adm1.storagegrid.example.com` e. `gn1.storagegrid.example.com`.

Se si prevede di utilizzare richieste in stile host virtuali S3, il certificato deve includere anche una voce **Nome alternativo** per ciascuna "Nome di dominio dell'endpoint S3" sono stati configurati, inclusi i nomi con caratteri jolly. Ad esempio:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Se si utilizzano caratteri jolly per i nomi di dominio, consultare "Linee guida per la protezione avanzata dei certificati server".

È inoltre necessario definire una voce DNS per ciascun nome nel certificato di protezione.

Come si gestiscono i certificati in scadenza?

Se il certificato utilizzato per proteggere la connessione tra l'applicazione S3 e StorageGRID scade, l'applicazione potrebbe perdere temporaneamente l'accesso a StorageGRID.

Per evitare problemi di scadenza del certificato, attenersi alle seguenti Best practice:

- Monitorare attentamente gli avvisi che avvisano di avvicinarsi alle date di scadenza del certificato, come ad

esempio **scadenza del certificato endpoint del bilanciamento del carico** e **scadenza del certificato server globale per gli avvisi S3 e Swift API**.

- Mantenere sempre sincronizzate le versioni del certificato delle applicazioni StorageGRID e S3. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint di bilanciamento del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato dall'applicazione S3.
- Utilizzare un certificato CA con firma pubblica. Se si utilizza un certificato firmato da una CA, è possibile sostituire i certificati in scadenza senza interruzioni.
- Se è stato generato un certificato StorageGRID autofirmato e il certificato sta per scadere, è necessario sostituirlo manualmente in StorageGRID e nell'applicazione S3 prima della scadenza del certificato esistente.

Considerazioni per la modalità di binding

La modalità di binding consente di controllare quali indirizzi IP possono essere utilizzati per accedere a un endpoint del bilanciamento del carico. Se un endpoint utilizza una modalità di binding, le applicazioni client possono accedere all'endpoint solo se utilizzano un indirizzo IP consentito o il corrispondente FQDN (Fully Qualified Domain Name). Le applicazioni client che utilizzano qualsiasi altro indirizzo IP o FQDN non possono accedere all'endpoint.

È possibile specificare una delle seguenti modalità di binding:

- **Globale** (impostazione predefinita): Le applicazioni client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare questa impostazione a meno che non sia necessario limitare l'accessibilità di un endpoint.
- **IP virtuali dei gruppi ha**. Le applicazioni client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha.
- **Interfacce nodo**. I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate.
- **Tipo di nodo**. In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway.

Considerazioni sull'accesso al tenant

L'accesso tenant è una funzionalità di sicurezza opzionale che consente di controllare quali account tenant StorageGRID possono utilizzare un endpoint di bilanciamento del carico per accedere ai bucket. È possibile consentire a tutti i tenant di accedere a un endpoint (impostazione predefinita) oppure specificare un elenco dei tenant consentiti o bloccati per ciascun endpoint.

È possibile utilizzare questa funzionalità per fornire un migliore isolamento della sicurezza tra i tenant e i relativi endpoint. Ad esempio, è possibile utilizzare questa funzione per garantire che i materiali top-secret o altamente classificati di proprietà di un tenant rimangano completamente inaccessibili agli altri tenant.

> Ai fini del controllo degli accessi, il tenant viene determinato dalle chiavi di accesso utilizzate nella richiesta del client; se non vengono fornite chiavi di accesso come parte della richiesta (ad esempio con accesso anonimo), il proprietario del bucket viene utilizzato per determinare il tenant.

Esempio di accesso al tenant

Per comprendere il funzionamento di questa funzionalità di sicurezza, si consideri il seguente esempio:

1. Sono stati creati due endpoint di bilanciamento del carico, come segue:
   - Endpoint **Public**: Utilizza la porta 10443 e consente l'accesso a tutti i tenant.
   - Endpoint **Top secret**: Utilizza la porta 10444 e consente l'accesso solo al tenant **Top secret**. Tutti gli altri tenant non possono accedere a questo endpoint.
2. Il `top-secret.pdf` Si trova in un bucket di proprietà del tenant **Top Secret**.

Per accedere a. `top-secret.pdf`, Un utente nel tenant **Top secret** può inviare una richiesta GET a. `https://w.x.y.z:10444/top-secret.pdf`. Poiché a questo tenant è consentito utilizzare l'endpoint 10444, l'utente può accedere all'oggetto. Tuttavia, se un utente appartenente a un altro tenant invia la stessa richiesta allo stesso URL, riceve un messaggio di accesso immediato negato. L'accesso viene negato anche se le credenziali e la firma sono valide.

Disponibilità della CPU

Il servizio Load Balancer su ciascun nodo Admin e nodo Gateway opera in modo indipendente quando inoltra il traffico S3 o Swift ai nodi Storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU. Le informazioni sul carico della CPU del nodo vengono aggiornate ogni pochi minuti, ma la ponderazione potrebbe essere aggiornata più frequentemente. A tutti i nodi di storage viene assegnato un valore minimo di peso di base, anche se un nodo riporta un utilizzo pari al 100% o non ne riporta l'utilizzo.

In alcuni casi, le informazioni sulla disponibilità della CPU sono limitate al sito in cui si trova il servizio Load Balancer.

Configurare gli endpoint del bilanciamento del carico

Gli endpoint del bilanciamento del carico determinano le porte e i protocolli di rete che i client S3 e Swift possono utilizzare per la connessione al bilanciamento del carico StorageGRID sui nodi gateway e di amministrazione. È inoltre possibile utilizzare gli endpoint per accedere a Grid Manager, Tenant Manager o a entrambi.

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Hai esaminato il "considerazioni per il bilanciamento del carico".
- Se in precedenza è stata rimappata una porta che si intende utilizzare per l'endpoint del bilanciamento del carico, è possibile "rimosso il remap della porta".
- Hai creato tutti i gruppi ad alta disponibilità (ha) che intendi utilizzare. I gruppi HA sono consigliati, ma non richiesti. Vedere "Gestire i gruppi ad alta disponibilità".
- Se l'endpoint del bilanciamento del carico verrà utilizzato da "S3 tenant per S3 Select", Non deve utilizzare gli indirizzi IP o FQDN di nodi bare-metal. Per gli endpoint del bilanciamento del carico utilizzati per S3 Select sono consentiti solo le appliance di servizi e i nodi software basati su VMware.
- Sono state configurate le interfacce VLAN che si intende utilizzare. Vedere "Configurare le interfacce

VLAN".

- Se si crea un endpoint HTTPS (consigliato), si dispone delle informazioni per il certificato del server.

  > Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

  - Per caricare un certificato, è necessario disporre del certificato del server, della chiave privata del certificato e, facoltativamente, di un bundle CA.
  - Per generare un certificato, sono necessari tutti i nomi di dominio e gli indirizzi IP utilizzati dai client S3 o Swift per accedere all'endpoint. Devi anche conoscere l'oggetto (Nome distinto).
  - Se si desidera utilizzare il certificato API StorageGRID S3 e Swift (che può essere utilizzato anche per le connessioni dirette ai nodi di storage), il certificato predefinito è già stato sostituito con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere "Configurare i certificati API S3 e Swift".

Creare un endpoint per il bilanciamento del carico

Ogni endpoint del bilanciamento del carico dei client S3 o Swift specifica una porta, un tipo di client (S3 o Swift) e un protocollo di rete (HTTP o HTTPS). Gli endpoint del bilanciamento del carico dell'interfaccia di gestione specificano una porta, un tipo di interfaccia e una rete client non attendibile.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
2. Per creare un endpoint per un client S3 o Swift, selezionare la scheda **S3 o Swift client**.
3. Per creare un endpoint per l'accesso a Grid Manager, Tenant Manager o entrambi, selezionare la scheda **interfaccia di gestione**.
4. Selezionare **Crea**.

Inserire i dettagli dell'endpoint

Fasi

1. Selezionare le istruzioni appropriate per inserire i dettagli per il tipo di endpoint che si desidera creare.

Client S3 o Swift

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è impostato su 10433 per il primo endpoint creato, ma è possibile immettere qualsiasi porta esterna non utilizzata compresa tra 1 e 65535. Se si immette **80** o **8443**, l'endpoint viene configurato solo sui nodi Gateway, a meno che non sia stata liberata la porta 8443. Quindi è possibile utilizzare la porta 8443 come endpoint S3 e la porta verrà configurata su entrambi i nodi Gateway e Admin.
Tipo di client	Il tipo di applicazione client che utilizzerà questo endpoint, **S3** o **Swift**.
Protocollo di rete	Il protocollo di rete che i client utilizzeranno per la connessione a questo endpoint. • Selezionare **HTTPS** per la comunicazione sicura con crittografia TLS (scelta consigliata). È necessario allegare un certificato di sicurezza prima di poter salvare l'endpoint. • Selezionare **HTTP** per comunicazioni meno sicure e non crittografate. Utilizzare HTTP solo per una griglia non di produzione.

Interfaccia di gestione

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	La porta StorageGRID che si desidera utilizzare per accedere a Gestore griglia, Gestore tenant o entrambi. • Gestore griglia: **8443** • Responsabile del tenant: **9443** • Sia Grid Manager che Tenant Manager: **443** **Nota**: È possibile utilizzare queste porte preimpostate o altre porte disponibili.
Tipo di interfaccia	Selezionare il pulsante di opzione per l'interfaccia StorageGRID a cui si accede utilizzando questo endpoint.

Campo	Descrizione
Rete client non attendibile	Selezionare **Sì** se l'endpoint deve essere accessibile alle reti client non attendibili. In caso contrario, selezionare **No**. Quando si seleziona **Sì**, la porta è aperta su tutte le reti client non attendibili. **Nota**: È possibile configurare una porta per essere aperta o chiusa a reti client non attendibili solo quando si crea l'endpoint di bilanciamento del carico.

1. Selezionare **continua**.

Selezionare una modalità di binding

Fasi

1. Selezionare una modalità di associazione per l'endpoint per controllare la modalità di accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

   Alcune modalità di associazione sono disponibili per gli endpoint client o per gli endpoint dell'interfaccia di gestione. Tutte le modalità per entrambi i tipi di endpoint sono elencate di seguito.

Modalità	Descrizione
Globale (impostazione predefinita per gli endpoint client)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione **Globale** a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.
Tipo di nodo (solo endpoint client)	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

Modalità	Descrizione
Tutti i nodi amministrativi (impostazione predefinita per gli endpoint dell'interfaccia di gestione)	I client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo amministrativo per accedere a questo endpoint.

Se più di un endpoint utilizza la stessa porta, StorageGRID utilizza questo ordine di priorità per decidere quale endpoint utilizzare: **IP virtuali dei gruppi ha** > **interfacce nodo** > **tipo di nodo** > **Globale**.

Se si stanno creando endpoint dell'interfaccia di gestione, sono consentiti solo i nodi Admin.

2. Se si seleziona **IP virtuali dei gruppi ha**, selezionare uno o più gruppi ha.

   Se si stanno creando endpoint dell'interfaccia di gestione, selezionare VIP associati solo ai nodi Admin.

3. Se si seleziona **Node interfaces**, selezionare una o più interfacce di nodo per ciascun nodo Admin o nodo gateway che si desidera associare a questo endpoint.
4. Se si seleziona **Node type** (tipo nodo), selezionare Admin Node (nodi amministratore), che include sia l'Admin Node primario che qualsiasi Admin Node non primario, oppure Gateway Node (nodi gateway).

Controllo dell'accesso al tenant

> Un endpoint dell'interfaccia di gestione può controllare l'accesso al tenant solo quando l'endpoint dispone di Tipo di interfaccia di Tenant Manager.

Fasi

1. Per il passaggio **accesso tenant**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket. Selezionare questa opzione se non sono ancora stati creati account tenant. Dopo aver aggiunto account tenant, è possibile modificare l'endpoint del bilanciamento del carico per consentire o bloccare account specifici.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

2. Se si crea un endpoint **HTTP**, non è necessario allegare un certificato. Selezionare **Create** per aggiungere il nuovo endpoint del bilanciamento del carico. Quindi, passare a. Al termine. In caso contrario, selezionare **continua** per allegare il certificato.

Allega certificato

Fasi

1. Se si sta creando un endpoint **HTTPS**, selezionare il tipo di certificato di sicurezza che si desidera allegare all'endpoint.

   Il certificato protegge le connessioni tra i client S3 e Swift e il servizio Load Balancer sui nodi Admin Node o Gateway.

   - **Carica certificato**. Selezionare questa opzione se si dispone di certificati personalizzati da caricare.
   - **Genera certificato**. Selezionare questa opzione se si dispone dei valori necessari per generare un certificato personalizzato.
   - **Utilizzare il certificato StorageGRID S3 e Swift**. Selezionare questa opzione se si desidera utilizzare il certificato globale S3 e Swift API, che può essere utilizzato anche per le connessioni dirette ai nodi di storage.

     Non è possibile selezionare questa opzione a meno che non sia stato sostituito il certificato S3 e Swift API predefinito, firmato dalla CA Grid, con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere "Configurare i certificati API S3 e Swift".

   - **Utilizza certificato interfaccia di gestione**. Selezionare questa opzione se si desidera utilizzare il certificato dell'interfaccia di gestione globale, che può essere utilizzato anche per le connessioni dirette ai nodi amministrativi.
2. Se non si utilizza il certificato StorageGRID S3 e Swift, caricare o generare il certificato.

Carica certificato

a. Selezionare **carica certificato**.

b. Caricare i file dei certificati del server richiesti:

- **Server certificate**: Il file di certificato del server personalizzato in codifica PEM.
- **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (`.key`).

> Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere 2048 bit o superiori.

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

  Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Selezionare **Crea**.
Viene creato l'endpoint del bilanciamento del carico. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 e Swift o l'interfaccia di gestione e l'endpoint.

Generare un certificato

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
IP	Uno o più indirizzi IP da includere nel certificato.

Campo	Descrizione
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Crea**.

   Viene creato l'endpoint del bilanciamento del carico. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 e Swift o l'interfaccia di gestione e questo endpoint.

Al termine

Fasi

1. Se si utilizza un DNS, assicurarsi che il DNS includa un record per associare il nome di dominio completo (FQDN, Fully Qualified Domain Name) di StorageGRID a ciascun indirizzo IP utilizzato dai client per effettuare le connessioni.

   L'indirizzo IP inserito nel record DNS dipende dall'utilizzo di un gruppo ha di nodi per il bilanciamento del carico:

- Se è stato configurato un gruppo ha, i client si connetteranno agli indirizzi IP virtuali di quel gruppo ha.
- Se non si utilizza un gruppo ha, i client si connetteranno al servizio bilanciamento del carico StorageGRID utilizzando l'indirizzo IP di un nodo gateway o di un nodo amministratore.

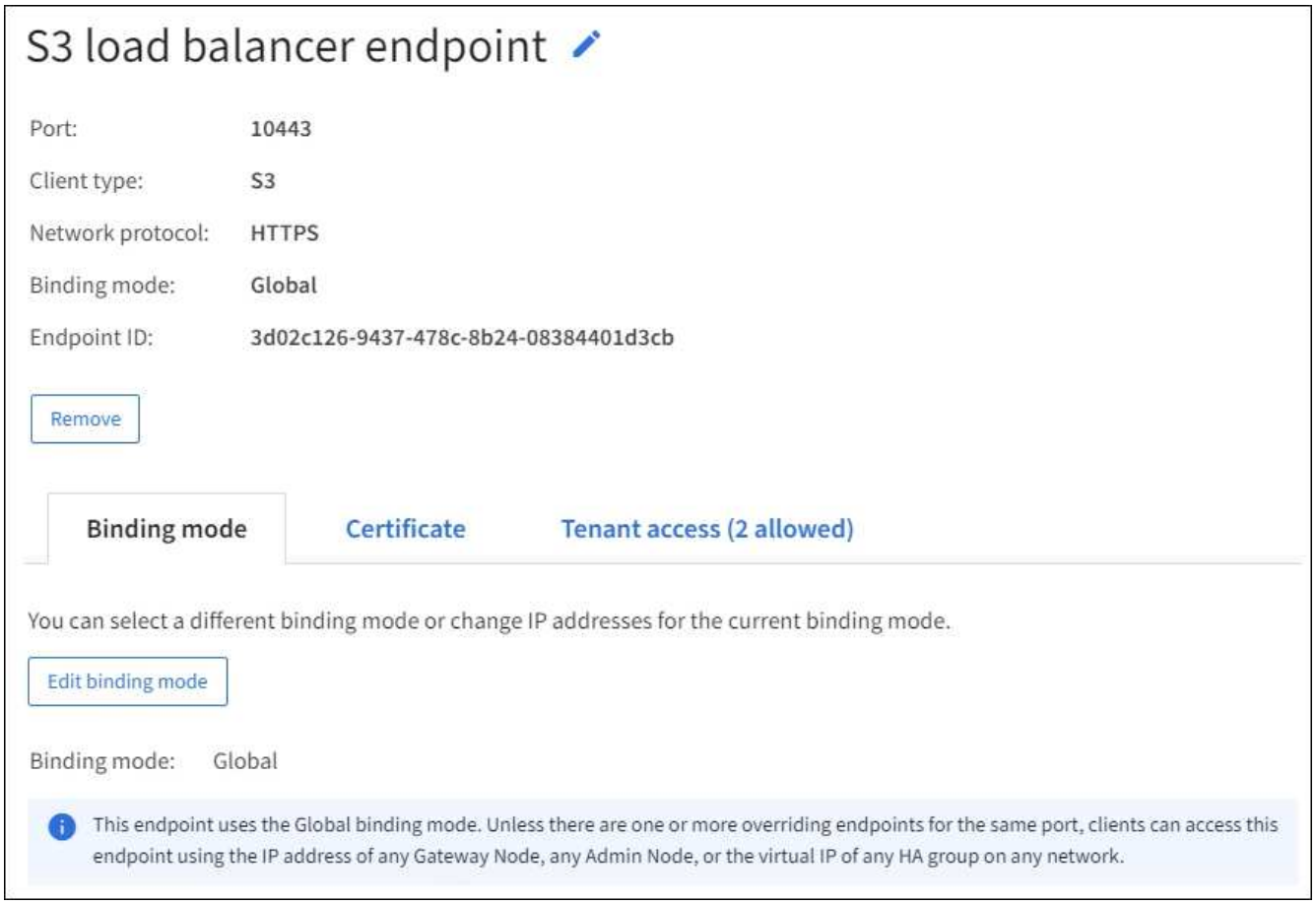
  È inoltre necessario assicurarsi che il record DNS faccia riferimento a tutti i nomi di dominio degli endpoint richiesti, inclusi i nomi con caratteri jolly.

2. Fornire ai client S3 e Swift le informazioni necessarie per connettersi all'endpoint:
   - Numero di porta
   - Nome di dominio completo o indirizzo IP
   - Tutti i dettagli del certificato richiesti

Visualizzare e modificare gli endpoint del bilanciamento del carico

È possibile visualizzare i dettagli degli endpoint del bilanciamento del carico esistenti, inclusi i metadati del certificato per un endpoint protetto. È possibile modificare determinate impostazioni per un endpoint.

- Per visualizzare le informazioni di base per tutti gli endpoint del bilanciamento del carico, esaminare le tabelle nella pagina Endpoints del bilanciamento del carico.
- Per visualizzare tutti i dettagli relativi a un endpoint specifico, inclusi i metadati del certificato, selezionare il nome dell'endpoint nella tabella. Le informazioni visualizzate variano a seconda del tipo di endpoint e della sua configurazione.



- Per modificare un endpoint, utilizzare il menu **azioni** nella pagina Endpoints del bilanciamento del carico.

Se si perde l'accesso a Grid Manager durante la modifica della porta di un endpoint dell'interfaccia di gestione, aggiornare l'URL e la porta per riottenere l'accesso.

Dopo aver modificato un endpoint, potrebbe essere necessario attendere fino a 15 minuti per applicare le modifiche a tutti i nodi.

Attività	Menu delle azioni	Pagina dei dettagli
Modificare il nome dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica nome endpoint**. c. Inserire il nuovo nome. d. Selezionare **Salva**.	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare l'icona di modifica . c. Inserire il nuovo nome. d. Selezionare **Salva**.
Modificare la porta dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica porta endpoint** c. Immettere un numero di porta valido. d. Selezionare **Salva**.	*n/a*
Modificare la modalità di associazione degli endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica modalità di associazione endpoint**. c. Aggiornare la modalità di binding secondo necessità. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare **Edit binding mode** (Modifica modalità di associazione). c. Aggiornare la modalità di binding secondo necessità. d. Selezionare **Save Changes** (Salva modifiche).
Modificare il certificato dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica certificato endpoint**. c. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda **certificato**. c. Selezionare **Modifica certificato**. d. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. e. Selezionare **Save Changes** (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Modificare l'accesso al tenant	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica accesso tenant**. c. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda **accesso tenant**. c. Selezionare **Edit tenant access** (Modifica accesso tenant). d. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni. e. Selezionare **Save Changes** (Salva modifiche).

Rimuovere gli endpoint del bilanciamento del carico

È possibile rimuovere uno o più endpoint dal menu **azioni** oppure rimuovere un singolo endpoint dalla pagina dei dettagli.

> Per evitare interruzioni del client, aggiornare le applicazioni client S3 o Swift interessate prima di rimuovere un endpoint di bilanciamento del carico. Aggiornare ogni client per la connessione utilizzando una porta assegnata a un altro endpoint del bilanciamento del carico. Assicurarsi di aggiornare anche tutte le informazioni di certificato richieste.

> Se si perde l'accesso a Grid Manager durante la rimozione di un endpoint dell'interfaccia di gestione, aggiornare l'URL.

- Per rimuovere uno o più endpoint:
  a. Dalla pagina bilanciamento del carico, selezionare la casella di controllo per ciascun endpoint che si desidera rimuovere.
  b. Selezionare **azioni** > **Rimuovi**.
  c. Selezionare **OK**.
- Per rimuovere un endpoint dalla pagina dei dettagli:
  a. Dalla pagina bilanciamento del carico. selezionare il nome dell'endpoint.
  b. Selezionare **Rimuovi** nella pagina dei dettagli.
  c. Selezionare **OK**.

Configurare i nomi di dominio degli endpoint S3

Per supportare le richieste in stile virtual-hosted S3, è necessario utilizzare Grid Manager per configurare l'elenco dei nomi di dominio degli endpoint S3 a cui si connettono i client S3.

L'utilizzo di un indirizzo IP per un nome di dominio endpoint non è supportato. Le versioni future impediranno questa configurazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai confermato che non è in corso un aggiornamento della griglia.

Non apportare modifiche alla configurazione del nome di dominio quando è in corso un aggiornamento della griglia.

A proposito di questa attività

Per consentire ai client di utilizzare i nomi di dominio degli endpoint S3, è necessario eseguire tutte le seguenti operazioni:

- Utilizzare Grid Manager per aggiungere i nomi di dominio degli endpoint S3 al sistema StorageGRID.
- Assicurarsi che il "Certificato utilizzato dal client per le connessioni HTTPS a StorageGRID" è firmato per tutti i nomi di dominio richiesti dal client.

  Ad esempio, se l'endpoint è `s3.company.com`, È necessario assicurarsi che il certificato utilizzato per le connessioni HTTPS includa `s3.company.com` Endpoint e SAN (Subject alternative Name) con caratteri jolly dell'endpoint: `*.s3.company.com`.

- Configurare il server DNS utilizzato dal client. Includere i record DNS per gli indirizzi IP utilizzati dai client per effettuare le connessioni e assicurarsi che i record riferiscano a tutti i nomi di dominio degli endpoint S3 richiesti, inclusi i nomi con caratteri jolly.

I client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo gateway, di un nodo amministratore o di un nodo di storage oppure connettendosi all'indirizzo IP virtuale di un gruppo ad alta disponibilità. È necessario comprendere il modo in cui le applicazioni client si connettono alla griglia in modo da includere gli indirizzi IP corretti nei record DNS.

I client che utilizzano connessioni HTTPS (consigliate) alla griglia possono utilizzare uno dei seguenti certificati:

- I client che si connettono a un endpoint di bilanciamento del carico possono utilizzare un certificato personalizzato per tale endpoint. Ogni endpoint del bilanciamento del carico può essere configurato per riconoscere diversi nomi di dominio degli endpoint S3.
- I client che si connettono a un endpoint di bilanciamento del carico o direttamente a un nodo di storage possono personalizzare il certificato globale S3 e Swift API per includere tutti i nomi di dominio degli endpoint S3 richiesti.

Se non si aggiungono nomi di dominio degli endpoint S3 e l'elenco è vuoto, il supporto per le richieste in stile virtual-hosted S3 viene disattivato.

Aggiungere un nome di dominio dell'endpoint S3

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **S3 endpoint domain name**.

2. Inserire il nome di dominio nel campo **Domain name 1**. Selezionare **Aggiungi un altro nome di dominio** per aggiungere altri nomi di dominio.
3. Selezionare **Salva**.
4. Assicurarsi che i certificati server utilizzati dai client corrispondano ai nomi di dominio degli endpoint S3 richiesti.
   - Se i client si connettono a un endpoint di bilanciamento del carico che utilizza il proprio certificato, "aggiornare il certificato associato all'endpoint".
   - Se i client si connettono a un endpoint di bilanciamento del carico che utilizza il certificato globale S3 e Swift API o direttamente ai nodi di storage, "Aggiornare il certificato globale S3 e Swift API".
5. Aggiungere i record DNS necessari per garantire che le richieste dei nomi di dominio degli endpoint possano essere risolte.

Risultato

Ora, quando i client utilizzano l'endpoint `bucket.s3.company.com`, Il server DNS si risolve nell'endpoint corretto e il certificato autentica l'endpoint come previsto.

Rinominare un nome di dominio endpoint S3

Se si modifica un nome utilizzato dalle applicazioni S3, le richieste di tipo virtual-hosted non avranno esito positivo.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **S3 endpoint domain name**.
2. Selezionare il campo del nome di dominio che si desidera modificare e apportare le modifiche necessarie.
3. Selezionare **Salva**.
4. Selezionare **Sì** per confermare la modifica.

Eliminare un nome di dominio dell'endpoint S3

Se si rimuove un nome utilizzato dalle applicazioni S3, le richieste di tipo virtual-hosted non avranno esito positivo.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **S3 endpoint domain name**.
2. Selezionare l'icona di eliminazione ✕ accanto al nome di dominio.
3. Selezionare **Sì** per confermare l'eliminazione.

Informazioni correlate

- "UTILIZZARE L'API REST S3"
- "Visualizzare gli indirizzi IP"
- "Configurare i gruppi ad alta disponibilità"

Riepilogo: Indirizzi IP e porte per le connessioni client

Per memorizzare o recuperare oggetti, le applicazioni client S3 e Swift si connettono al servizio Load Balancer, incluso in tutti i nodi Admin e Gateway, o al servizio Local Distribution Router (LDR), incluso in tutti i nodi Storage.

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo Grid e il numero di porta del servizio su tale nodo. Facoltativamente, è possibile creare gruppi ad alta disponibilità (ha) di nodi di bilanciamento del carico per fornire connessioni ad alta disponibilità che utilizzano indirizzi IP virtuali (VIP). Se si desidera connettersi a StorageGRID utilizzando un nome di dominio completo (FQDN) invece di un indirizzo IP o VIP, è possibile configurare le voci DNS.

Questa tabella riassume i diversi modi in cui i client possono connettersi a StorageGRID e gli indirizzi IP e le porte utilizzati per ciascun tipo di connessione. Se sono già stati creati endpoint di bilanciamento del carico e gruppi ad alta disponibilità (ha), vedere Dove trovare gli indirizzi IP Per individuare questi valori in Grid Manager.

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Gruppo HA	Bilanciamento del carico	Indirizzo IP virtuale di un gruppo ha	Porta assegnata all'endpoint del bilanciamento del carico
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	Porta assegnata all'endpoint del bilanciamento del carico
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	Porta assegnata all'endpoint del bilanciamento del carico
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte S3 predefinite: • HTTPS: 18082 • HTTP: 18084 Porte Swift predefinite: • HTTPS: 18083 • HTTP:18085

URL di esempio

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

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

Ad esempio, se l'indirizzo IP virtuale del gruppo ha è 192.0.2.5 e il numero di porta dell'endpoint del bilanciamento del carico è 10443, un'applicazione potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

`https://192.0.2.5:10443`

Dove trovare gli indirizzi IP

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Per trovare l'indirizzo IP di un nodo Grid:
   a. Selezionare **NODI**.
   b. Selezionare il nodo Admin, il nodo gateway o il nodo di storage a cui si desidera connettersi.
   c. Selezionare la scheda **Panoramica**.
   d. Nella sezione Node Information (informazioni sul nodo), annotare gli indirizzi IP del nodo.
   e. Selezionare **Mostra altro** per visualizzare gli indirizzi IPv6 e le mappature dell'interfaccia.

      È possibile stabilire connessioni dalle applicazioni client a uno qualsiasi degli indirizzi IP presenti nell'elenco:

      - **Eth0:** Grid Network
      - **Eth1:** Admin Network (opzionale)
      - **Eth2:** rete client (opzionale)

      > Se si sta visualizzando un nodo Admin o un nodo Gateway e si tratta del nodo attivo di un gruppo ad alta disponibilità, l'indirizzo IP virtuale del gruppo ha viene visualizzato su eth2.

3. Per trovare l'indirizzo IP virtuale di un gruppo ad alta disponibilità:
   a. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.
   b. Nella tabella, annotare l'indirizzo IP virtuale del gruppo ha.
4. Per trovare il numero di porta di un endpoint Load Balancer:
   a. Selezionare **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
   b. Annotare il numero di porta dell'endpoint che si desidera utilizzare.

      > Se il numero di porta è 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché tali porte sono riservate sui nodi Admin. Tutte le altre porte sono configurate sia sui nodi Gateway che sui nodi Admin.

   c. Selezionare il nome dell'endpoint dalla tabella.
   d. Verificare che il **tipo di client** (S3 o Swift) corrisponda all'applicazione client che utilizzerà l'endpoint.

Gestire reti e connessioni

Configurazione delle impostazioni di rete: Panoramica

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

Configurare le interfacce VLAN

È possibile "Creare interfacce LAN virtuale (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.

Policy di classificazione del traffico

È possibile utilizzare "policy di classificazione del traffico" 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.

Linee guida per le reti StorageGRID

È possibile utilizzare Grid Manager per configurare e gestire le reti e le connessioni StorageGRID.

Vedere "Configurare le connessioni client S3 e Swift" Per scoprire come connettere i client S3 o Swift.

Reti StorageGRID predefinite

Per impostazione predefinita, StorageGRID supporta tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.

Per ulteriori informazioni sulla topologia di rete, vedere "Linee guida per il networking".

Grid Network

Obbligatorio. La rete griglia viene utilizzata per tutto il traffico StorageGRID interno. Fornisce connettività tra tutti i nodi della rete, in tutti i siti e le subnet.

Admin Network (rete amministrativa)

Opzionale. La rete di amministrazione viene generalmente utilizzata per l'amministrazione e la manutenzione del sistema. Può essere utilizzato anche per l'accesso al protocollo client. La rete di amministrazione è in genere una rete privata e non deve essere instradabile tra i siti.

Rete client

Opzionale. La rete client è una rete aperta, generalmente utilizzata per fornire l'accesso alle applicazioni client S3 e Swift, in modo che la rete grid possa essere isolata e protetta. La rete client può comunicare con qualsiasi subnet raggiungibile tramite il gateway locale.

Linee guida

- Ogni nodo StorageGRID richiede un'interfaccia di rete dedicata, un indirizzo IP, una subnet mask e un gateway per ogni rete a cui è assegnato.
- Un nodo Grid non può avere più di un'interfaccia su una rete.
- È supportato un singolo gateway, per rete, per nodo di rete, che deve trovarsi sulla stessa sottorete del nodo. Se necessario, è possibile implementare un routing più complesso nel gateway.
- Su ciascun nodo, ogni rete viene mappata a una specifica interfaccia di rete.

Rete	Nome dell'interfaccia
Griglia	eth0

Rete	Nome dell'interfaccia
Admin (opzionale)	eth1
Client (opzionale)	eth2

- Se il nodo è collegato a un'appliance StorageGRID, vengono utilizzate porte specifiche per ciascuna rete. Per ulteriori informazioni, consultare le istruzioni di installazione dell'apparecchio.
- Il percorso predefinito viene generato automaticamente, per nodo. Se eth2 è attivato, 0.0.0.0/0 utilizza la rete client su eth2. Se eth2 non è abilitato, 0.0.0.0/0 utilizza Grid Network su eth0.
- La rete client non diventa operativa fino a quando il nodo grid non si è Unito alla griglia
- La rete amministrativa può essere configurata durante l'implementazione del nodo grid per consentire l'accesso all'interfaccia utente dell'installazione prima che la griglia sia completamente installata.

Interfacce opzionali

In alternativa, è possibile aggiungere interfacce aggiuntive a un nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poterlo utilizzare "Interfacce VLAN" separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in "Gruppo ad alta disponibilità (ha)".

Per aggiungere trunk o interfacce di accesso, vedere quanto segue:

- **VMware (dopo l'installazione del nodo)**: "VMware: Aggiunta di interfacce di accesso o trunk a un nodo"
  - **Red Hat Enterprise Linux (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, Ubuntu o Debian (dopo aver installato il nodo)**: "Linux: Aggiunta di interfacce di accesso o trunk a un nodo"

Visualizzare gli indirizzi IP

È possibile visualizzare l'indirizzo IP di ciascun nodo della griglia nel sistema StorageGRID. È quindi possibile utilizzare questo indirizzo IP per accedere al nodo Grid dalla riga di comando ed eseguire varie procedure di manutenzione.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

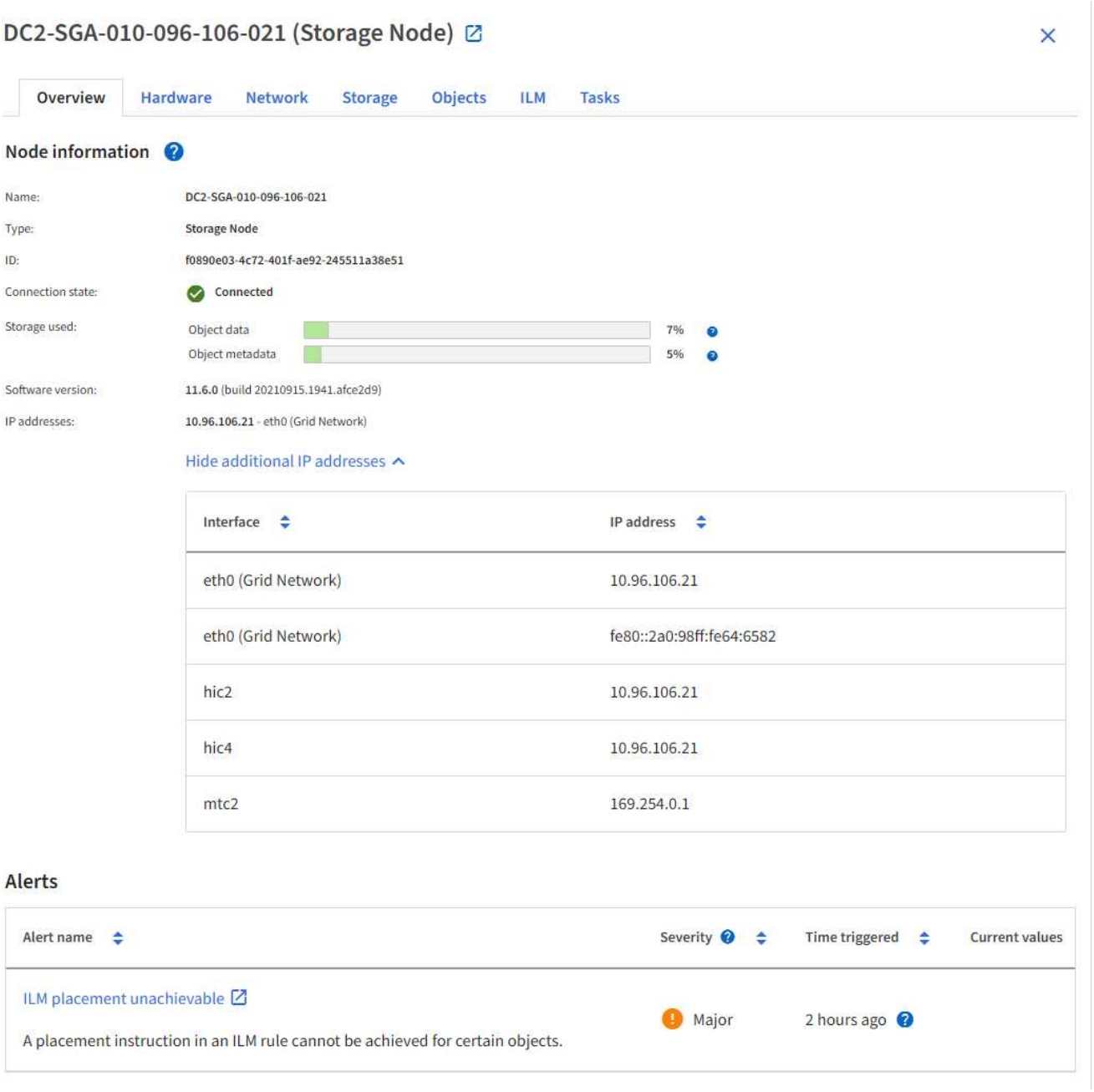
A proposito di questa attività

Per informazioni sulla modifica degli indirizzi IP, vedere "Configurare gli indirizzi IP".

Fasi

1. Selezionare **NODES** > ***Grid Node*** > **Overview**.
2. Selezionare **Mostra altri** a destra del titolo indirizzi IP.

   Gli indirizzi IP per il nodo della griglia sono elencati in una tabella.



Configurare le interfacce VLAN

È possibile creare interfacce LAN virtuale (VLAN) su nodi Admin e nodi Gateway e utilizzarle in gruppi ha ed endpoint di bilanciamento del carico per isolare e partizionare il traffico per garantire sicurezza, flessibilità e performance.

Considerazioni per le interfacce VLAN

- Per creare un'interfaccia VLAN, immettere un ID VLAN e scegliere un'interfaccia principale su uno o più nodi.
- Un'interfaccia principale deve essere configurata come interfaccia di linea sullo switch.
- Un'interfaccia padre può essere Grid Network (eth0), Client Network (eth2) o un'interfaccia trunk aggiuntiva per la macchina virtuale o l'host bare-metal (ad esempio, ens256).

- Per ogni interfaccia VLAN, è possibile selezionare solo un'interfaccia principale per un nodo specifico. Ad esempio, non è possibile utilizzare l'interfaccia Grid Network e l'interfaccia Client Network sullo stesso nodo gateway dell'interfaccia principale per la stessa VLAN.
- Se l'interfaccia VLAN è per il traffico Admin Node, che include il traffico correlato a Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi Admin.
- Se l'interfaccia VLAN è per il traffico client S3 o Swift, selezionare le interfacce sui nodi Admin o Gateway.
- Per ulteriori informazioni sull'aggiunta di interfacce di linea, consultare quanto segue:
  - **VMware (dopo l'installazione del nodo)**: "VMware: Aggiunta di interfacce di accesso o trunk a un nodo"
  - **RHEL (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, Ubuntu o Debian (dopo aver installato il nodo)**: "Linux: Aggiunta di interfacce di accesso o trunk a un nodo"

Creare un'interfaccia VLAN

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Un'interfaccia di linea è stata configurata nella rete e collegata al nodo VM o Linux. Si conosce il nome dell'interfaccia di linea.
- Si conosce l'ID della VLAN che si sta configurando.

A proposito di questa attività

L'amministratore di rete potrebbe aver configurato una o più interfacce di trunk e una o più VLAN per separare il traffico client o amministrativo che appartiene a diverse applicazioni o tenant. Ogni VLAN è identificata da un ID numerico o da un tag. Ad esempio, la rete potrebbe utilizzare la VLAN 100 per il traffico FabricPool e la VLAN 200 per un'applicazione di archiviazione.

È possibile utilizzare Grid Manager per creare interfacce VLAN che consentono ai client di accedere a StorageGRID su una VLAN specifica. Quando si creano interfacce VLAN, specificare l'ID VLAN e selezionare le interfacce principali (trunk) su uno o più nodi.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Selezionare **Crea**.

Inserire i dettagli delle interfacce VLAN

Fasi

1. Specificare l'ID della VLAN nella rete. È possibile immettere un valore compreso tra 1 e 4094.

   Gli ID VLAN non devono essere univoci. Ad esempio, è possibile utilizzare l'ID VLAN 200 per il traffico amministrativo in un sito e lo stesso ID VLAN per il traffico client in un altro sito. È possibile creare interfacce VLAN separate con diversi set di interfacce padre in ogni sito. Tuttavia, due interfacce VLAN con lo stesso ID non possono condividere la stessa interfaccia su un nodo.

Se si specifica un ID già utilizzato, viene visualizzato un messaggio.

2. Facoltativamente, inserire una breve descrizione per l'interfaccia VLAN.
3. Selezionare **continua**.

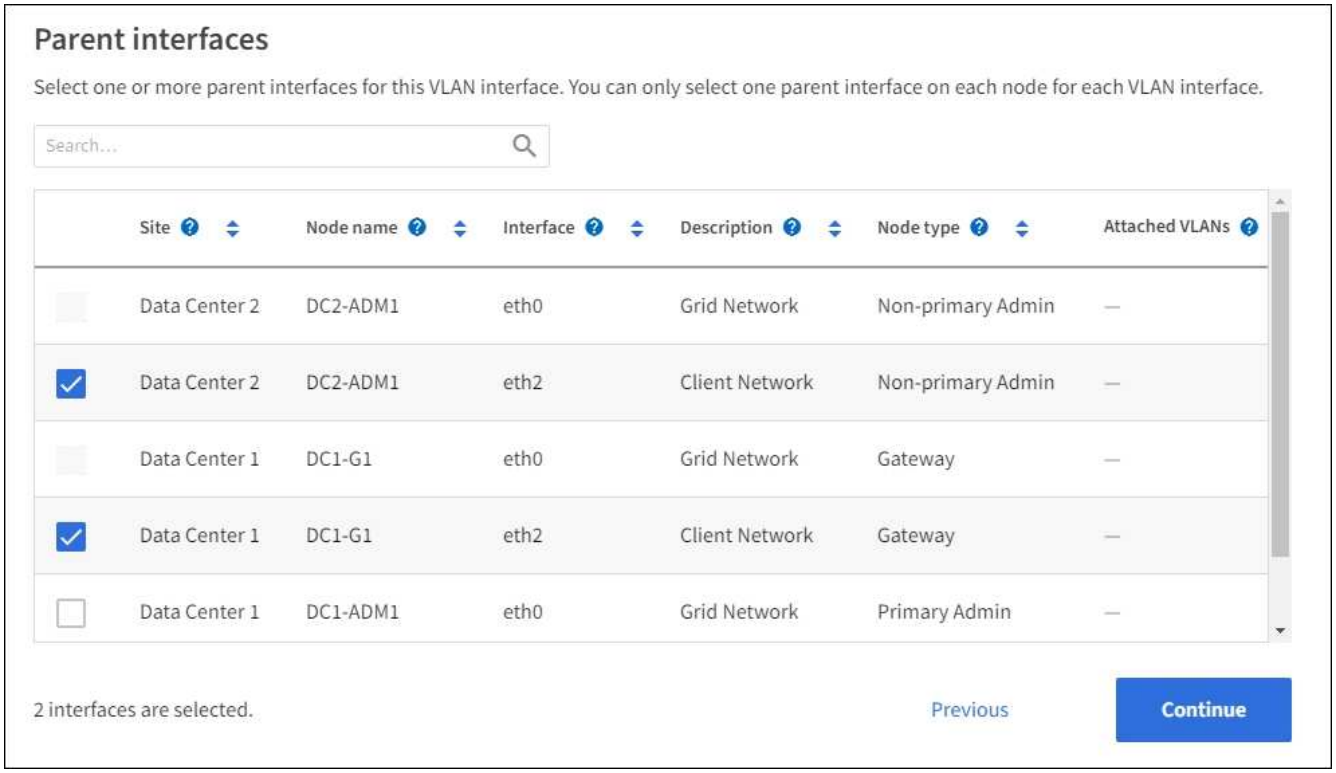
Scegliere le interfacce padre

La tabella elenca le interfacce disponibili per tutti i nodi Admin e Gateway in ogni sito della griglia. Le interfacce Admin Network (eth1) non possono essere utilizzate come interfacce padre e non vengono visualizzate.

Fasi

1. Selezionare una o più interfacce padre a cui collegare questa VLAN.

   Ad esempio, è possibile collegare una VLAN all'interfaccia di rete client (eth2) per un nodo gateway e un nodo amministratore.



2. Selezionare **continua**.

Confermare le impostazioni

Fasi

1. Esaminare la configurazione e apportare eventuali modifiche.
   - Se è necessario modificare l'ID o la descrizione della VLAN, selezionare **Enter VLAN details** (Inserisci dettagli VLAN) nella parte superiore della pagina.
   - Per modificare un'interfaccia padre, selezionare **Choose parent interfaces** (Scegli interfacce padre) nella parte superiore della pagina oppure selezionare **Previous** (precedente).
   - Se è necessario rimuovere un'interfaccia padre, selezionare il cestino .
2. Selezionare **Salva**.

3. Attendere fino a 5 minuti che la nuova interfaccia venga visualizzata come selezione nella pagina High Availability groups (gruppi ad alta disponibilità) e sia elencata nella tabella **Network interfaces** (interfacce di rete) per il nodo (**NODES** > ***parent interface node*** > **Network**).

Modificare un'interfaccia VLAN

Quando si modifica un'interfaccia VLAN, è possibile apportare i seguenti tipi di modifiche:

- Modificare l'ID o la descrizione della VLAN.
- Aggiungere o rimuovere interfacce padre.

Ad esempio, se si intende decommissionare il nodo associato, è possibile rimuovere un'interfaccia principale da un'interfaccia VLAN.

Tenere presente quanto segue:

- Non è possibile modificare un ID VLAN se l'interfaccia VLAN viene utilizzata in un gruppo ha.
- Non è possibile rimuovere un'interfaccia padre se tale interfaccia padre è utilizzata in un gruppo ha.

  Ad esempio, si supponga che la VLAN 200 sia collegata alle interfacce padre sui nodi A e B. Se un gruppo ha utilizza l'interfaccia VLAN 200 per il nodo A e l'interfaccia eth2 per il nodo B, è possibile rimuovere l'interfaccia padre non utilizzata per il nodo B, ma non è possibile rimuovere l'interfaccia padre utilizzata per il nodo A.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Selezionare la casella di controllo dell'interfaccia VLAN che si desidera modificare. Quindi, selezionare **azioni** > **Modifica**.
3. Facoltativamente, aggiornare l'ID VLAN o la descrizione. Quindi, selezionare **continua**.

   Non è possibile aggiornare un ID VLAN se la VLAN viene utilizzata in un gruppo ha.

4. Facoltativamente, selezionare o deselezionare le caselle di controllo per aggiungere interfacce padre o per rimuovere interfacce inutilizzate. Quindi, selezionare **continua**.
5. Esaminare la configurazione e apportare eventuali modifiche.
6. Selezionare **Salva**.

Rimuovere un'interfaccia VLAN

È possibile rimuovere una o più interfacce VLAN.

Non è possibile rimuovere un'interfaccia VLAN se è attualmente utilizzata in un gruppo ha. È necessario rimuovere l'interfaccia VLAN dal gruppo ha prima di poterla rimuovere.

Per evitare interruzioni del traffico client, è consigliabile eseguire una delle seguenti operazioni:

- Aggiungere una nuova interfaccia VLAN al gruppo ha prima di rimuovere questa interfaccia VLAN.
- Creare un nuovo gruppo ha che non utilizzi questa interfaccia VLAN.
- Se l'interfaccia VLAN che si desidera rimuovere è attualmente attiva, modificare il gruppo ha. Spostare l'interfaccia VLAN che si desidera rimuovere in fondo all'elenco delle priorità. Attendere che la comunicazione venga stabilita sulla nuova interfaccia principale, quindi rimuovere la vecchia interfaccia dal

gruppo ha. Infine, eliminare l'interfaccia VLAN su quel nodo.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Selezionare la casella di controllo per ogni interfaccia VLAN che si desidera rimuovere. Quindi, selezionare **azioni** > **Elimina**.
3. Selezionare **Sì** per confermare la selezione.

   Tutte le interfacce VLAN selezionate vengono rimosse. Nella pagina delle interfacce VLAN viene visualizzato un banner verde di successo.

Gestire le policy di classificazione del traffico

Gestire le policy di classificazione del traffico: Panoramica

Per migliorare la qualità del servizio (QoS), è possibile creare policy di classificazione del traffico per identificare e monitorare diversi tipi di traffico di rete. Queste policy possono essere utili per la limitazione e il monitoraggio del traffico.

I criteri di classificazione del traffico vengono applicati agli endpoint del servizio bilanciamento del carico StorageGRID per i nodi gateway e i nodi di amministrazione. Per creare criteri di classificazione del traffico, è necessario aver già creato endpoint di bilanciamento del carico.

Regole corrispondenti

Ogni policy di classificazione del traffico contiene una o più regole corrispondenti per identificare il traffico di rete correlato a una o più delle seguenti entità:

- Bucket
- Subnet
- Tenant
- Endpoint del bilanciamento del carico

StorageGRID monitora il traffico che corrisponde a qualsiasi regola all'interno del criterio in base agli obiettivi della regola. Qualsiasi traffico corrispondente a qualsiasi regola di un criterio viene gestito da tale criterio. Al contrario, è possibile impostare le regole in modo che corrispondano a tutto il traffico ad eccezione di un'entità specificata.

Limitazione del traffico

In alternativa, è possibile aggiungere i seguenti tipi di limite a un criterio:

- Larghezza di banda aggregata
- Larghezza di banda per richiesta
- Richieste simultanee
- Tasso di richiesta

I valori limite vengono applicati in base al bilanciamento del carico. Se il traffico viene distribuito simultaneamente tra più bilanciatori di carico, i tassi massimi totali sono un multiplo dei limiti di velocità specificati.

È possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. I limiti di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul traffico non limitato.

Per i limiti di larghezza di banda aggregati o per richiesta, le richieste vengono trasmesse in streaming alla velocità impostata. StorageGRID può applicare una sola velocità, quindi la corrispondenza di policy più specifica, in base al tipo di matcher, è quella applicata. La larghezza di banda consumata dalla richiesta non viene contata rispetto ad altre policy di corrispondenza meno specifiche contenenti policy di limite della larghezza di banda aggregate. Per tutti gli altri tipi di limite, le richieste client vengono ritardate di 250 millisecondi e ricevono una risposta lenta di 503 per le richieste che superano qualsiasi limite di policy corrispondente.

In Grid Manager, è possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Utilizzare i criteri di classificazione del traffico con gli SLA

È possibile utilizzare le policy di classificazione del traffico insieme ai limiti di capacità e alla protezione dei dati per applicare gli SLA (Service-Level Agreement) che forniscono specifiche per capacità, protezione dei dati e performance.

Nell'esempio riportato di seguito vengono illustrati tre livelli di uno SLA. È possibile creare criteri di classificazione del traffico per raggiungere gli obiettivi di performance di ciascun livello SLA.

Livello di servizio	Capacità	Protezione dei dati	Massime performance consentite	Costo
Oro	1 PB di storage consentito	3 copia regola ILM	25 K richieste/sec 5 GB/sec (40 Gbps) di larghezza di banda	€ al mese
Argento	250 TB di storage consentiti	2 copia regola ILM	10 richieste K/sec Larghezza di banda di 1.25 GB/sec (10 Gbps)	dollari al mese
Bronzo	100 TB di storage consentito	2 copia regola ILM	5 richieste K/sec 1 GB/sec (8 Gbps) di larghezza di banda	dollari al mese

Creare policy di classificazione del traffico

È possibile creare policy di classificazione del traffico se si desidera monitorare e, facoltativamente, limitare il traffico di rete per bucket, bucket regex, CIDR, endpoint del bilanciamento del carico o tenant. Facoltativamente, è possibile impostare limiti per una

policy in base alla larghezza di banda, al numero di richieste simultanee o alla velocità di richiesta.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Sono stati creati endpoint di bilanciamento del carico che si desidera associare.
- Hai creato i tenant che desideri abbinare.

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.
2. Selezionare **Crea**.
3. Inserire un nome e una descrizione (opzionale) per la policy e selezionare **continua**.

   Ad esempio, descrivi a cosa si applica questa policy di classificazione del traffico e a cosa limiterà.

4. Selezionare **Aggiungi regola** e specificare i seguenti dettagli per creare una o più regole corrispondenti per il criterio. I criteri creati devono avere almeno una regola corrispondente. Selezionare **continua**.

Campo	Descrizione
Tipo	Selezionare i tipi di traffico a cui si applica la regola corrispondente. I tipi di traffico sono bucket, bucket regex, CIDR, endpoint del bilanciamento del carico e tenant.
Valore corrispondente	Inserire il valore corrispondente al tipo selezionato. • Bucket: Immettere uno o più nomi di bucket. • Secchio regex: Immettere una o più espressioni regolari utilizzate per far corrispondere un insieme di nomi di bucket. L'espressione regolare non è ancorata. USA l'ancora ^ per trovare la corrispondenza all'inizio del nome del bucket e usa l'ancora per la corrispondenza alla fine del nome. La corrispondenza delle espressioni regolari supporta un sottoinsieme della sintassi PCRE (Perl Compatible Regular Expression). • CIDR: Inserire una o più subnet IPv4, nella notazione CIDR, che corrispondono alla subnet desiderata. • Endpoint del bilanciamento del carico: Selezionare il nome di un endpoint. Questi sono gli endpoint del bilanciamento del carico definiti in "Configurare gli endpoint del bilanciamento del carico". • Tenant: Il tenant matching utilizza l'ID della chiave di accesso. Se la richiesta non contiene un ID della chiave di accesso (ad esempio, l'accesso anonimo), viene utilizzata la proprietà del bucket a cui si accede per determinare il tenant.

Campo	Descrizione
Corrispondenza inversa	Se si desidera far corrispondere tutto il traffico di rete *tranne* coerente con il valore Type and Match appena definito, selezionare la casella di controllo **Inverse Match** (corrispondenza inversa). In caso contrario, lasciare deselezionata la casella di controllo. Ad esempio, se si desidera applicare questo criterio a tutti gli endpoint del bilanciamento del carico tranne uno, specificare l'endpoint del bilanciamento del carico da escludere e selezionare **corrispondenza inversa**. Per un criterio contenente più adattatori in cui almeno uno è un adattatore inverso, fare attenzione a non creare un criterio che corrisponda a tutte le richieste.

5. Facoltativamente, selezionare **Aggiungi un limite** e selezionare i seguenti dettagli per aggiungere uno o più limiti per controllare il traffico di rete associato a una regola.

> StorageGRID raccoglie le metriche anche se non si aggiungono limiti, in modo da poter comprendere le tendenze del traffico.

Campo	Descrizione
Tipo	Il tipo di limite che si desidera applicare al traffico di rete associato alla regola. Ad esempio, è possibile limitare la larghezza di banda o il tasso di richiesta. **Nota**: È possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. Quando la larghezza di banda aggregata è in uso, la larghezza di banda per richiesta non è disponibile. Al contrario, quando viene utilizzata la larghezza di banda per richiesta, la larghezza di banda aggregata non è disponibile. I limiti di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul traffico non limitato. Per i limiti di larghezza di banda, StorageGRID applica la policy che meglio corrisponde al tipo di limite impostato. Ad esempio, se si dispone di una policy che limita il traffico in una sola direzione, il traffico nella direzione opposta sarà illimitato, anche se il traffico corrisponde a criteri aggiuntivi con limiti di larghezza di banda. StorageGRID implementa le corrispondenze "migliori" per i limiti di larghezza di banda nel seguente ordine: • Indirizzo IP esatto (/32 mask) • Nome esatto del bucket • Regex. Bucket • Tenant • Endpoint • Corrispondenze CIDR non esatte (non /32) • Corrispondenze inverse

Campo	Descrizione
Valido per	Se questo limite si applica alle richieste di lettura del client (GET o HEAD) o alle richieste di scrittura (PUT, POST o DELETE).
Valore	Il valore a cui il traffico di rete sarà limitato, in base all'unità selezionata. Ad esempio, immettere 10 e selezionare MiB/s per impedire che il traffico di rete associato a questa regola superi i 10 MiB/s. **Nota**: A seconda dell'impostazione delle unità, le unità disponibili saranno binarie (ad esempio, GiB) o decimali (ad esempio, GB). Per modificare l'impostazione delle unità, selezionare l'elenco a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User Preferences** (Preferenze utente).
Unità	L'unità che descrive il valore immesso.

Ad esempio, se si desidera creare un limite di larghezza di banda di 40 GB/s per un livello SLA, creare due limiti di larghezza di banda aggregati: GET/HEAD a 40 GB/s e PUT/POST/DELETE a 40 GB/s.

6. Selezionare **continua**.
7. Leggere e rivedere la policy di classificazione del traffico. Utilizzare il pulsante **precedente** per tornare indietro e apportare le modifiche necessarie. Quando si è soddisfatti della policy, selezionare **Salva e continua**.

   Il traffico dei client S3 e Swift viene ora gestito in base alla policy di classificazione del traffico.

Al termine

"Visualizzare le metriche del traffico di rete" per verificare che i criteri stiano applicando i limiti di traffico previsti.

Modificare la policy di classificazione del traffico

È possibile modificare un criterio di classificazione del traffico per modificarne il nome o la descrizione oppure per creare, modificare o eliminare eventuali regole o limiti per il criterio.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti vengono elencati in una tabella.

2. Modificare il criterio utilizzando il menu azioni o la pagina dei dettagli. Vedere "creare policy di classificazione del traffico" per cosa partecipare.

Menu delle azioni

a. Selezionare la casella di controllo per la policy.

b. Selezionare **azioni** > **Modifica**.

Pagina dei dettagli

a. Selezionare il nome del criterio.

b. Selezionare il pulsante **Edit** (Modifica) accanto al nome del criterio.

3. Per il passo inserire il nome del criterio, modificare facoltativamente il nome o la descrizione del criterio e selezionare **continua**.
4. Per il passo Add Matching rules (Aggiungi regole di corrispondenza), aggiungere una regola o modificare **Type** e **Match value** della regola esistente, quindi selezionare **Continue** (continua).
5. Per la fase Set Limits (Imposta limiti), aggiungere, modificare o eliminare un limite e selezionare **Continue** (continua).
6. Esaminare la policy aggiornata e selezionare **Salva e continua**.

   Le modifiche apportate alla policy vengono salvate e il traffico di rete viene gestito in base alle policy di classificazione del traffico. È possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Eliminare una policy di classificazione del traffico

È possibile eliminare una policy di classificazione del traffico se non è più necessaria. Assicurarsi di eliminare la policy corretta perché non è possibile recuperare una policy quando viene eliminata.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Criteri di classificazione del traffico con i criteri esistenti elencati in una tabella.

2. Eliminare il criterio utilizzando il menu azioni o la pagina dei dettagli.

Menu delle azioni

a. Selezionare la casella di controllo per la policy.

b. Selezionare **azioni** > **Rimuovi**.

Pagina dei dettagli della policy

a. Selezionare il nome del criterio.

b. Selezionare il pulsante **Remove** accanto al nome del criterio.

3. Selezionare **Sì** per confermare che si desidera eliminare il criterio.

   La policy viene eliminata.

Visualizzare le metriche del traffico di rete

È possibile monitorare il traffico di rete visualizzando i grafici disponibili nella pagina Criteri di classificazione del traffico.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Accesso root o autorizzazione account tenant".

A proposito di questa attività

Per qualsiasi criterio di classificazione del traffico esistente, è possibile visualizzare le metriche per il servizio di bilanciamento del carico per determinare se il criterio limita correttamente il traffico nella rete. I dati nei grafici possono aiutare a determinare se è necessario modificare la policy.

Anche se non vengono impostati limiti per una policy di classificazione del traffico, vengono raccolte le metriche e i grafici forniscono informazioni utili per comprendere le tendenze del traffico.

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti vengono elencati nella tabella.

2. Selezionare il nome del criterio di classificazione del traffico per il quale si desidera visualizzare le metriche.
3. Selezionare la scheda **metriche**.

   Vengono visualizzati i grafici dei criteri di classificazione del traffico. I grafici visualizzano le metriche solo per il traffico corrispondente al criterio selezionato.

   I grafici riportati di seguito sono inclusi nella pagina.

   - Tasso di richiesta: Questo grafico fornisce la quantità di larghezza di banda corrispondente a questa policy gestita da tutti i bilanciatori di carico. I dati ricevuti includono intestazioni di richiesta per tutte le richieste e dimensioni dei dati del corpo per le risposte che hanno dati del corpo. Inviato include le intestazioni delle risposte per tutte le richieste e le dimensioni dei dati del corpo delle risposte per le richieste che includono i dati del corpo nella risposta.

     > Quando le richieste sono complete, questo grafico mostra solo l'utilizzo della larghezza di banda. Per le richieste di oggetti lenti o di grandi dimensioni, la larghezza di banda istantanea effettiva potrebbe differire dai valori riportati in questo grafico.

   - Tasso di risposta agli errori: Questo grafico fornisce una velocità approssimativa alla quale le richieste corrispondenti a questa policy restituiscono errori (codice di stato HTTP >= 400) ai client.
   - Durata media della richiesta (non errore): Questo grafico fornisce una durata media delle richieste riuscite corrispondenti a questa policy.
   - Utilizzo della larghezza di banda della policy: Questo grafico fornisce la quantità di larghezza di banda

corrispondente a questa policy gestita da tutti i bilanciatori di carico. I dati ricevuti includono intestazioni di richiesta per tutte le richieste e dimensioni dei dati del corpo per le risposte che hanno dati del corpo. Inviato include le intestazioni delle risposte per tutte le richieste e le dimensioni dei dati del corpo delle risposte per le richieste che includono i dati del corpo nella risposta.

4. Posizionare il cursore su un grafico a linee per visualizzare una finestra a comparsa di valori su una parte specifica del grafico.
5. Selezionare **Grafana dashboard** sotto il titolo metriche per visualizzare tutti i grafici di una policy. Oltre ai quattro grafici della scheda **metriche**, è possibile visualizzare altri due grafici:
   - Write request rate by object size (tasso di richiesta di scrittura per dimensione oggetto): Tasso di richieste PUT/POST/DELETE corrispondenti a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le velocità mostrate nella vista con il passaggio del mouse sono troncate in conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
   - Read request rate by object size (tasso richiesta di lettura per dimensione oggetto): Il tasso per le richieste GET/HEAD corrispondenti a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le velocità mostrate nella vista con il passaggio del mouse sono troncate in conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
6. In alternativa, accedere ai grafici dal menu **SUPPORT**.
   a. Selezionare **SUPPORT** > **Tools** > **Metrics**.
   b. Selezionare **Traffic Classification Policy** dalla sezione **Grafana**.
   c. Selezionare il criterio dal menu in alto a sinistra della pagina.
   d. Posizionare il cursore su un grafico per visualizzare una finestra a comparsa che mostra la data e l'ora del campione, le dimensioni degli oggetti aggregati nel conteggio e il numero di richieste al secondo durante tale periodo di tempo.

      Le policy di classificazione del traffico sono identificate dal loro ID. Gli ID delle policy sono elencati nella pagina delle policy di classificazione del traffico.
7. Analizzare i grafici per determinare la frequenza con cui il criterio limita il traffico e se è necessario modificare il criterio.

Crittografia supportata per le connessioni TLS in uscita

Il sistema StorageGRID supporta un set limitato di suite di crittografia per le connessioni TLS (Transport Layer Security) ai sistemi esterni utilizzati per la federazione di identità e i pool di storage cloud.

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3 per le connessioni a sistemi esterni utilizzati per la federazione delle identità e i pool di storage cloud.

I cifrari TLS supportati per l'utilizzo con sistemi esterni sono stati selezionati per garantire la compatibilità con una vasta gamma di sistemi esterni. L'elenco è più grande dell'elenco di cifrature supportate per l'utilizzo con le applicazioni client S3 o Swift. Per configurare le crittografia, andare a **CONFIGURATION** > **Security** > **Security settings** e selezionare **TLS and SSH policy**.

Le opzioni di configurazione TLS, come versioni di protocollo, crittografia, algoritmi di scambio delle chiavi e algoritmi MAC, non sono configurabili in StorageGRID. Se hai richieste specifiche su queste impostazioni, contatta il tuo rappresentante NetApp.

Vantaggi delle connessioni HTTP attive, inattive e simultanee

La modalità di configurazione delle connessioni HTTP può influire sulle prestazioni del sistema StorageGRID. Le configurazioni variano a seconda che la connessione HTTP sia attiva o inattiva o che si dispongano di più connessioni simultanee.

È possibile identificare i vantaggi in termini di prestazioni per i seguenti tipi di connessioni HTTP:

- Connessioni HTTP inattive
- Connessioni HTTP attive
- Connessioni HTTP simultanee

I vantaggi di mantenere aperte le connessioni HTTP inattive

È necessario mantenere aperte le connessioni HTTP anche quando le applicazioni client sono inattive per consentire alle applicazioni client di eseguire transazioni successive sulla connessione aperta. In base alle misurazioni del sistema e all'esperienza di integrazione, è necessario mantenere aperta una connessione HTTP inattiva per un massimo di 10 minuti. StorageGRID potrebbe chiudere automaticamente una connessione HTTP che rimane aperta e inattiva per più di 10 minuti.

Le connessioni HTTP aperte e inattive offrono i seguenti vantaggi:

- Latenza ridotta dal momento in cui il sistema StorageGRID stabilisce di eseguire una transazione HTTP al momento in cui il sistema StorageGRID può eseguire la transazione

  La latenza ridotta è il vantaggio principale, in particolare per il tempo necessario per stabilire connessioni TCP/IP e TLS.

- Aumento della velocità di trasferimento dei dati mediante l'attivazione dell'algoritmo di avvio lento TCP/IP con i trasferimenti eseguiti in precedenza
- Notifica istantanea di diverse classi di condizioni di errore che interrompono la connettività tra l'applicazione client e il sistema StorageGRID

Determinare per quanto tempo mantenere aperta una connessione inattiva è un compromesso tra i benefici dell'avvio lento associati alla connessione esistente e l'allocazione ideale della connessione alle risorse di sistema interne.

Vantaggi delle connessioni HTTP attive

Per le connessioni dirette ai nodi di storage, è necessario limitare la durata di una connessione HTTP attiva a un massimo di 10 minuti, anche se la connessione HTTP esegue continuamente transazioni.

La determinazione della durata massima per cui una connessione deve essere mantenuta aperta è un compromesso tra i benefici della persistenza della connessione e l'allocazione ideale della connessione alle risorse di sistema interne.

Per le connessioni client ai nodi di storage, la limitazione delle connessioni HTTP attive offre i seguenti vantaggi:

- Consente un bilanciamento ottimale del carico nel sistema StorageGRID.

  Con il passare del tempo, una connessione HTTP potrebbe non essere più ottimale con il variare dei requisiti di bilanciamento del carico. Il sistema esegue il miglior bilanciamento del carico quando le applicazioni client stabiliscono una connessione HTTP separata per ciascuna transazione, ma questo nega i guadagni molto più preziosi associati alle connessioni persistenti.

- Consente alle applicazioni client di indirizzare le transazioni HTTP ai servizi LDR che dispongono di spazio disponibile.
- Consente l'avvio delle procedure di manutenzione.

  Alcune procedure di manutenzione vengono avviate solo dopo il completamento di tutte le connessioni HTTP in corso.

Per le connessioni client al servizio Load Balancer, la limitazione della durata delle connessioni aperte può essere utile per consentire l'avvio tempestivo di alcune procedure di manutenzione. Se la durata delle connessioni client non è limitata, potrebbero essere necessari alcuni minuti per terminare automaticamente le connessioni attive.

Vantaggi delle connessioni HTTP simultanee

Tenere aperte più connessioni TCP/IP al sistema StorageGRID per consentire il parallelismo, aumentando così le performance. Il numero ottimale di connessioni parallele dipende da diversi fattori.

Le connessioni HTTP simultanee offrono i seguenti vantaggi:

- Latenza ridotta

  Le transazioni possono iniziare immediatamente invece di attendere il completamento di altre transazioni.

- Maggiore throughput

  Il sistema StorageGRID può eseguire transazioni parallele e aumentare il throughput delle transazioni aggregate.

Le applicazioni client devono stabilire più connessioni HTTP. Quando un'applicazione client deve eseguire una transazione, può selezionare e utilizzare immediatamente qualsiasi connessione stabilita che non sta elaborando una transazione.

La topologia di ciascun sistema StorageGRID presenta un throughput di picco diverso per le transazioni e le connessioni simultanee prima che le performance comincino a degradarsi. Il throughput massimo dipende da fattori quali risorse di calcolo, risorse di rete, risorse di storage e collegamenti WAN. Anche il numero di server e servizi e il numero di applicazioni supportate dal sistema StorageGRID sono fattori.

I sistemi StorageGRID spesso supportano più applicazioni client. Tenere presente questo aspetto quando si determina il numero massimo di connessioni simultanee utilizzate da un'applicazione client. Se l'applicazione client è costituita da più entità software che stabiliscono connessioni al sistema StorageGRID, è necessario sommare tutte le connessioni tra le entità. Potrebbe essere necessario regolare il numero massimo di connessioni simultanee nelle seguenti situazioni:

- La topologia del sistema StorageGRID influisce sul numero massimo di transazioni e connessioni simultanee supportate dal sistema.
- Le applicazioni client che interagiscono con il sistema StorageGRID su una rete con larghezza di banda limitata potrebbero dover ridurre il grado di concorrenza per garantire che le singole transazioni vengano

completate in un tempo ragionevole.

- Quando molte applicazioni client condividono il sistema StorageGRID, potrebbe essere necessario ridurre il grado di concorrenza per evitare di superare i limiti del sistema.

Separazione dei pool di connessione HTTP per le operazioni di lettura e scrittura

È possibile utilizzare pool separati di connessioni HTTP per le operazioni di lettura e scrittura e controllare la quantità di un pool da utilizzare per ciascuno di essi. I pool separati di connessioni HTTP consentono di controllare meglio le transazioni e bilanciare i carichi.

Le applicazioni client possono creare carichi dominanti dal recupero (lettura) o dominanti dal negozio (scrittura). Con pool separati di connessioni HTTP per le transazioni di lettura e scrittura, è possibile regolare la quantità di ciascun pool da dedicare alle transazioni di lettura o scrittura.

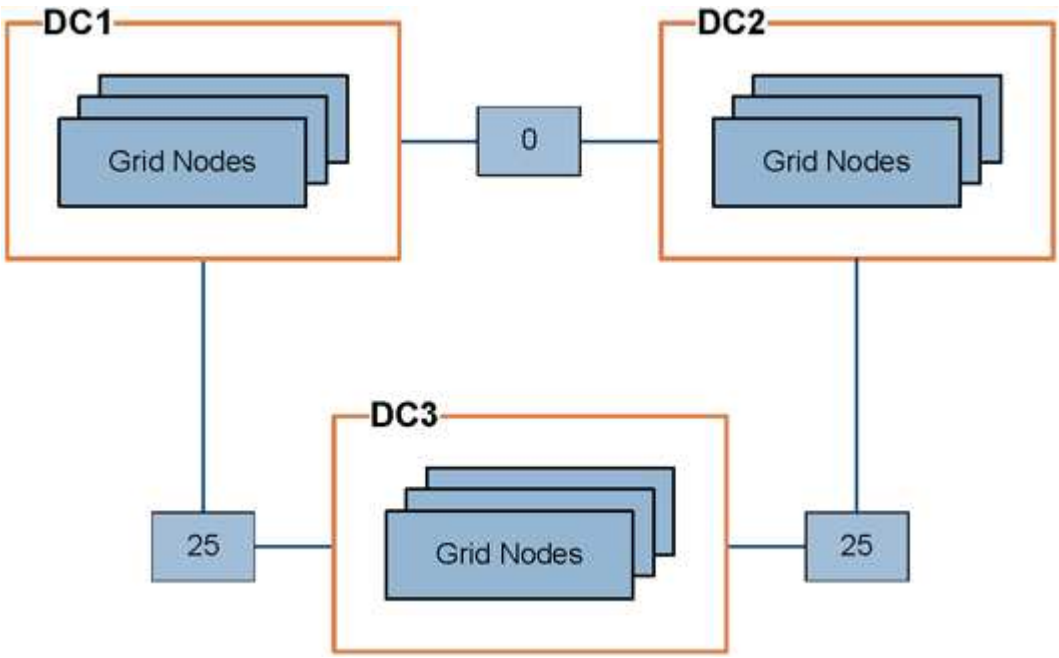
Gestire i costi di collegamento

I costi di collegamento consentono di assegnare la priorità al sito del data center che fornisce un servizio richiesto quando esistono due o più siti del data center. È possibile regolare i costi di collegamento in modo da riflettere la latenza tra i siti.

Quali sono i costi di collegamento?

- I costi di collegamento vengono utilizzati per assegnare la priorità alla copia oggetto utilizzata per soddisfare i recuperi di oggetti.
- I costi di collegamento vengono utilizzati dall'API di gestione del grid e dall'API di gestione del tenant per determinare i servizi StorageGRID interni da utilizzare.
- I costi di collegamento vengono utilizzati dal servizio Load Balancer sui nodi Admin e sui nodi Gateway per indirizzare le connessioni client. Vedere "Considerazioni per il bilanciamento del carico".

Il diagramma mostra una griglia a tre siti con costi di collegamento configurati tra i siti:



- Il servizio Load Balancer sui nodi Admin e Gateway distribuisce in modo uguale le connessioni client a tutti i nodi Storage nello stesso sito del data center e a qualsiasi sito del data center con un costo di

collegamento pari a 0.

Nell'esempio, un nodo gateway nel sito 1 del data center (DC1) distribuisce in modo uguale le connessioni client ai nodi di storage in DC1 e ai nodi di storage in DC2. Un nodo gateway in DC3 invia le connessioni client solo ai nodi di storage in DC3.

- Quando si recupera un oggetto che esiste come copie replicate multiple, StorageGRID recupera la copia nel data center che ha il costo di collegamento più basso.

  Nell'esempio, se un'applicazione client in DC2 recupera un oggetto memorizzato sia in DC1 che in DC3, l'oggetto viene recuperato da DC1, poiché il costo di collegamento da DC1 a DC2 è 0, che è inferiore al costo di collegamento da DC3 a DC2 (25).

I costi di collegamento sono numeri relativi arbitrari senza unità di misura specifica. Ad esempio, un costo di collegamento di 50 viene utilizzato in modo meno preferenziale rispetto a un costo di collegamento di 25. La tabella mostra i costi di collegamento comunemente utilizzati.

Collegamento	Costo del collegamento	Note
Tra siti fisici di data center	25 (impostazione predefinita)	Data center connessi tramite un collegamento WAN.
Tra i siti del data center logico nella stessa posizione fisica	0	Data center logici nello stesso edificio fisico o campus connessi da una LAN.

Aggiornare i costi dei collegamenti

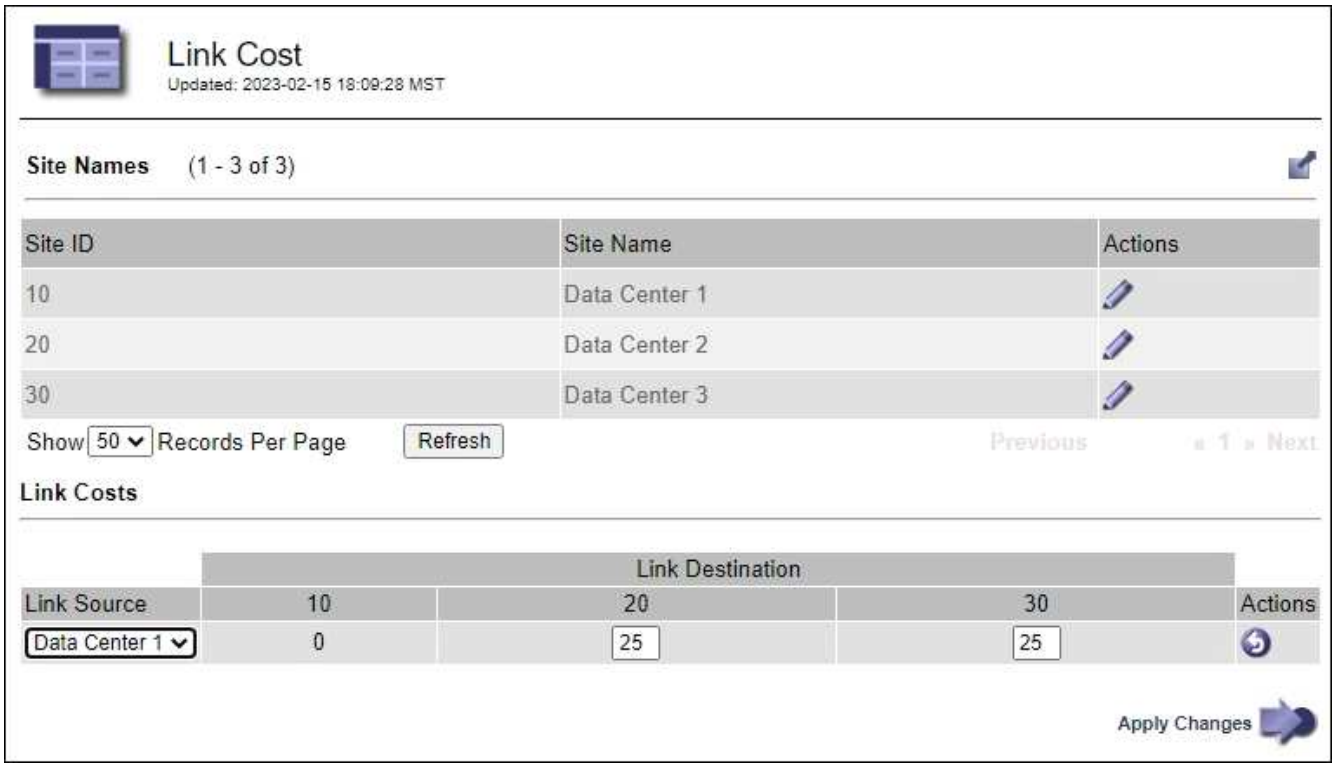
È possibile aggiornare i costi di collegamento tra i siti del data center per riflettere la latenza tra i siti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di configurazione della pagina della topologia della griglia".

Fasi

1. Selezionare **SUPPORTO** > **Altro** > **costo collegamento**.



2. Selezionare un sito in **link Source** (origine collegamento) e immettere un valore di costo compreso tra 0 e 100 in **link Destination** (destinazione collegamento).

   Non puoi modificare il costo del collegamento se l'origine è la stessa della destinazione.

   Per annullare le modifiche, selezionare **Ripristina**.

3. Selezionare **Applica modifiche**.

USA AutoSupport

Use AutoSupport: Panoramica

La funzione AutoSupport consente a StorageGRID di inviare pacchetti di stato e integrità al supporto tecnico NetApp.

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 pacchetti AutoSupport da inviare a una destinazione aggiuntiva.

StorageGRID dispone di due tipi di AutoSupport:

StorageGRID AutoSupport

Segnala problemi relativi al software StorageGRID. Attivato per impostazione predefinita quando si installa StorageGRID per la prima volta. È possibile "Modificare la configurazione AutoSupport predefinita" se necessario.

Se StorageGRID AutoSupport non è abilitato, viene visualizzato un messaggio sul dashboard di Gestione griglia. Il messaggio include un collegamento alla pagina di configurazione di AutoSupport. Se si chiude il messaggio, questo non viene visualizzato fino a quando la cache del browser non viene cancellata, anche se AutoSupport rimane disattivato.

AutoSupport dell'hardware di appliance

Segnala problemi relativi all'appliance StorageGRID. È necessario "Configura AutoSupport hardware su ogni appliance".

Che cos'è 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 nel sito di supporto NetApp, è necessario attivare AutoSupport.

"Documentazione di Active IQ Digital Advisor"

Informazioni incluse nel pacchetto AutoSupport

Un pacchetto AutoSupport contiene i seguenti file XML e dettagli.

Nome del file	Campi	Descrizione
AUTOSUPPORT-HISTORY.XML	Numero di sequenza AutoSupport Destinazione per questo AutoSupport Evento trigger Stato di consegna Tentativi di consegna Oggetto AutoSupport URI di consegna Ultimo errore AutoSupport INSERISCI nome file Ora di generazione Dimensione compressa AutoSupport Dimensioni decompresse AutoSupport Tempo totale di raccolta (ms)	File di cronologia AutoSupport.

Nome del file	Campi	Descrizione
AUTOSUPPORT.XML	Nodo Protocollo per contattare il supporto URL di supporto per HTTP/HTTPS Indirizzo di assistenza Stato OnDemand AutoSupport URL server OnDemand AutoSupport Intervallo di polling su richiesta AutoSupport	File di stato AutoSupport. Fornisce i dettagli del protocollo utilizzato, dell'URL e dell'indirizzo del supporto tecnico, dell'intervallo di polling e di OnDemand AutoSupport, se attivato o disattivato.
BUCKET.XML	ID benna ID account Versione build Configurazione vincolo posizione Conformità abilitata Configurazione conformità Blocco oggetto S3 abilitato S3 Configurazione blocco oggetto Configurazione di coerenza CORS abilitato Configurazione CORS Ora ultimo accesso attivata Criterio attivato Configurazione dei criteri Notifiche attivate Configurazione notifiche Cloud Mirror abilitato Configurazione del mirror cloud Ricerca abilitata Cerca configurazione Accesso rapido ACL di lettura attivato Configurazione ACL lettura rapida Swift Write ACL attivato Configurazione Swift Write ACL Etichettatura bucket abilitata Configurazione etichettatura bucket Configurazione delle versioni	Fornisce dettagli di configurazione e statistiche a livello di bucket. Esempi di configurazioni bucket includono servizi di piattaforma, conformità e coerenza dei bucket.

Nome del file	Campi	Descrizione
GRID-CONFIGURATIONS.XML	ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di informazioni sulla configurazione a livello di griglia. Contiene informazioni sui certificati Grid, sullo spazio riservato ai metadati, sulle impostazioni di configurazione a livello di grid (compliance, blocco degli oggetti S3, compressione degli oggetti, avvisi, syslog, e configurazione ILM), dettagli del profilo di erasure coding, nome DNS, "Nome NMS"e molto altro ancora.
GRID-SPEC.XML	Specifiche della griglia, XML non elaborato	Utilizzato per la configurazione e la distribuzione di StorageGRID. Contiene le specifiche della griglia, l'IP del server NTP, l'IP del server DNS, la topologia di rete e i profili hardware dei nodi.
GRID-TASKS.XML	Nodo Percorso di assistenza ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di stato delle attività della griglia (procedure di manutenzione). Fornisce i dettagli delle attività attive, terminate, completate, non riuscite e in sospeso della griglia.
GRID.JSON	Griglia + Revisione + versione software + Descrizione + licenza + password + DNS + NTP + Siti + nodi	Informazioni sulla griglia.
ILM-CONFIGURATION.XML	ID attributo Nome attributo Valore Indice ID tabella Nome tabella	Elenco degli attributi per le configurazioni ILM.
ILM-STATUS.XML	Nodo Percorso di servizio ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di informazioni sulle metriche ILM. Contiene le velocità di valutazione ILM per ogni nodo e le metriche a livello di grid.

Nome del file	Campi	Descrizione
ILM.XML	XML raw ILM	File di criteri ILM attivo. Contiene dettagli sulle policy ILM attive, come ID del pool di storage, comportamento di acquisizione, filtri, regole e descrizione. Contiene inoltre l'XML per il criterio ILM predefinito.
LOG.TGZ	*n/a*	File di registro scaricabile. Contiene `bycast-err.log` e. `servermanager.log` da ogni nodo.
MANIFEST.XML	Ordine di ritiro Nome file contenuto AutoSupport per questi dati Descrizione di questa voce di dati Numero di byte raccolti Tempo impiegato per la raccolta Stato di questa voce dati Descrizione dell'errore Tipo di contenuto AutoSupport per questi dati +	Contiene metadati AutoSupport e brevi descrizioni di tutti i file XML AutoSupport.
NMS-ENTITIES.XML	Indice attributo Entità OID ID nodo ID modello dispositivo Versione del modello del dispositivo Nome entità	Raggruppa e service entities in "Albero NMS". Fornisce dettagli sulla topologia della griglia. Il nodo può essere determinato in base ai servizi in esecuzione sul nodo.
OBJECTS-STATUS.XML	Nodo Percorso di servizio ID attributo Nome attributo Valore Indice ID tabella Nome tabella	Stato dell'oggetto, incluso lo stato della scansione in background, il trasferimento attivo, la velocità di trasferimento, i trasferimenti totali, la velocità di eliminazione, frammenti corrotti, oggetti smarriti, oggetti mancanti, tentativo di riparazione, velocità di scansione, periodo di scansione stimato, stato di completamento della riparazione e altro ancora.

Nome del file	Campi	Descrizione
SERVER-STATUS.XML	Nodo Percorso di servizio ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di eventi e configurazioni del server. Contiene i seguenti dettagli per ogni nodo: Tipo di piattaforma, sistema operativo, memoria installata, memoria disponibile, connettività storage, numero di serie dello chassis dell'appliance di storage, numero di dischi guasti dello storage controller, temperatura dello chassis del controller di calcolo, hardware di calcolo, numero di serie del controller di calcolo, alimentatore, dimensioni dei dischi, tipo di disco e altro ancora.
SERVICE-STATUS.XML	Nodo Percorso di servizio ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di informazioni sul nodo di servizio. Contiene dettagli quali spazio allocato nella tabella, spazio libero nella tabella, metriche del piano d'esame del database, durata della riparazione dei segmenti, durata del processo di riparazione, riavvii automatici del processo, interruzione automatica del processo, e molto altro ancora.
STORAGE-GRADE.XML	ID grado archiviazione Nome grado storage ID nodo storage Percorso del nodo storage	File di definizioni di livello di archiviazione per ogni nodo di archiviazione.
SUMMARY-ATTRIBUTES.XML	OID gruppo Percorso gruppo ID attributo riepilogo Nome attributo riepilogo Valore Indice ID tabella Nome tabella	Dati di stato del sistema di alto livello che riassumono le informazioni sull'utilizzo di StorageGRID. Fornisce dettagli quali nome della griglia, nomi dei siti, numero di nodi storage per grid e per sito, tipo di licenza, capacità e utilizzo della licenza, termini di supporto software e dettagli sulle operazioni di S3 e Swift.
SYSTEM-ALARMS.XML	Nodo Percorso di servizio Gravità Attributo allarme Nome attributo Stato Valore Tempo di attivazione Conferma ora	Allarmi di livello di sistema (deprecati) e dati di stato utilizzati per indicare attività anomale o potenziali problemi.

Nome del file	Campi	Descrizione
SYSTEM-ALERTS.XML	Nome Gravità Nome del nodo Stato avviso Nome sito Tempo di attivazione allarme Tempo risoluzione avviso ID regola ID nodo ID sito Silenziato Altre annotazioni Altre etichette	Avvisi di sistema correnti che indicano potenziali problemi nel sistema StorageGRID.
USERAGENTS.XML	Agente utente Numero di giorni Richieste HTTP totali Byte totali acquisiti Byte totali recuperati INSERIRE le richieste Richiedi ELIMINA richieste Richieste HEAD INVIA richieste OPZIONI richieste Tempo medio richiesta (ms) Tempo medio di richiesta PUT (ms) Tempo medio di richiesta di RECUPERO (ms) Tempo medio di richiesta di ELIMINAZIONE (ms) Tempo medio di richiesta TESTINA (ms) Tempo medio POST-richiesta (ms) Tempo medio richiesta OPZIONI (ms)	Statistiche basate sugli agenti utente dell'applicazione. Ad esempio, il numero di operazioni PUT/GET/DELETE/HEAD per agente utente e la dimensione totale dei byte di ciascuna operazione.
X-HEADER-DATA	X-NetApp-asup-generated-on X-NetApp-asup-hostname X-NetApp-asup-os-version X-NetApp-asup-serial-num X-NetApp-asup-subject X-NetApp-asup-system-id X-NetApp-asup-model-name +	Dati di intestazione AutoSupport.

Configurare AutoSupport

Per impostazione predefinita, la funzione StorageGRID AutoSupport è attivata quando si installa StorageGRID per la prima volta. Tuttavia, è necessario configurare AutoSupport hardware su ogni appliance. Se necessario, è possibile modificare la configurazione di AutoSupport.

Se si desidera modificare la configurazione di StorageGRID AutoSupport, apportare le modifiche solo al nodo amministrativo primario. È necessario Configurare l'AutoSupport dell'hardware su ciascun apparecchio.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Se si utilizza HTTPS per l'invio di pacchetti AutoSupport, è stato fornito l'accesso Internet in uscita al nodo amministrativo principale, direttamente o. "utilizzando un server proxy" (non sono richieste connessioni in entrata).
- Se nella pagina StorageGRID AutoSupport è selezionato HTTP, è stato configurato un server proxy per inoltrare i pacchetti AutoSupport come HTTPS. I server AutoSupport di NetApp rifiuteranno i pacchetti inviati utilizzando il protocollo HTTP.

  "Informazioni sulla configurazione delle impostazioni proxy dell'amministratore".

- Se si utilizza SMTP come protocollo per i pacchetti AutoSupport, è stato configurato un server di posta SMTP. La stessa configurazione del server di posta viene utilizzata per le notifiche e-mail di allarme (sistema legacy).

A proposito di questa attività

È possibile utilizzare qualsiasi combinazione delle seguenti opzioni per inviare i pacchetti AutoSupport al supporto tecnico:

- **Settimanale**: Invia automaticamente i pacchetti AutoSupport una volta alla settimana. Impostazione predefinita: Enabled (attivato).
- **Evento attivato**: Invia automaticamente pacchetti AutoSupport ogni ora o quando si verificano eventi di sistema significativi. Impostazione predefinita: Enabled (attivato).
- **Su richiesta**: Consente al supporto tecnico di richiedere che il sistema StorageGRID invii automaticamente i pacchetti AutoSupport, il che è utile quando stanno lavorando attivamente a un problema (richiede il protocollo di trasmissione HTTPS AutoSupport). Impostazione predefinita: Disattivata.
- **Attivato dall'utente**: Inviare manualmente i pacchetti AutoSupport in qualsiasi momento.

specifica il protocollo per i pacchetti AutoSupport

È possibile utilizzare uno dei seguenti protocolli per l'invio di pacchetti AutoSupport:

- **HTTPS**: Impostazione predefinita e consigliata per le nuove installazioni. Questo protocollo utilizza la porta 443. Se lo si desidera Attivare la funzione AutoSupport on Demand, È necessario utilizzare HTTPS.
- **HTTP**: Se si seleziona HTTP, è necessario configurare un server proxy per inoltrare i pacchetti AutoSupport come HTTPS. I server AutoSupport di NetApp rifiutano i pacchetti inviati mediante HTTP. Questo protocollo utilizza la porta 80.
- **SMTP**: Utilizzare questa opzione se si desidera che i pacchetti AutoSupport vengano inviati tramite e-mail. Se si utilizza SMTP come protocollo per i pacchetti AutoSupport, è necessario configurare un server di

posta SMTP nella pagina di configurazione della posta elettronica precedente (**SUPPORT** > **Allarmi (legacy)** > **impostazione della posta elettronica precedente**).

Il protocollo impostato viene utilizzato per l'invio di tutti i tipi di pacchetti AutoSupport.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Selezionare il protocollo che si desidera utilizzare per inviare pacchetti AutoSupport.
3. Se è stato selezionato **HTTPS**, selezionare se utilizzare un certificato di supporto NetApp (certificato TLS) per proteggere la connessione al server del supporto tecnico.
   - **Verify certificate** (verifica certificato*) (impostazione predefinita): Garantisce che la trasmissione dei pacchetti AutoSupport sia sicura. Il certificato di supporto NetApp è già installato con il software StorageGRID.
   - **Non verificare il certificato**: Selezionare questa opzione solo se si dispone di un buon motivo per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.
4. Selezionare **Salva**. Tutti i pacchetti settimanali, attivati dall'utente e attivati da eventi vengono inviati utilizzando il protocollo selezionato.

Disattiva AutoSupport settimanale

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport all'assistenza tecnica una volta alla settimana.

Per determinare quando verrà inviato il pacchetto settimanale AutoSupport, andare alla scheda **AutoSupport** > **Results**. Nella sezione **AutoSupport settimanale**, osservare il valore per **ora pianificata successiva**.

È possibile disattivare l'invio automatico di pacchetti AutoSupport settimanali in qualsiasi momento.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Deselezionare la casella di controllo **Enable Weekly AutoSupport** (Abilita aggiornamento settimanale).
3. Selezionare **Salva**.

Disattiva AutoSupport attivato dagli eventi

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport all'assistenza tecnica ogni ora.

È possibile disattivare AutoSupport attivato da eventi in qualsiasi momento.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Deselezionare la casella di controllo **attiva AutoSupport attivato da eventi**.
3. Selezionare **Salva**.

Attiva AutoSupport on Demand

AutoSupport on Demand può aiutare a risolvere i problemi sui quali il supporto tecnico sta lavorando attivamente.

Per impostazione predefinita, AutoSupport on Demand è disattivato. L'attivazione di questa funzione consente al supporto tecnico di richiedere che il sistema StorageGRID invii automaticamente i pacchetti AutoSupport. Il supporto tecnico può anche impostare l'intervallo di tempo di polling per le query AutoSupport on Demand.

Il supporto tecnico non può attivare o disattivare AutoSupport on Demand.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Selezionare **HTTPS** per il protocollo.
3. Selezionare la casella di controllo **Enable Weekly AutoSupport** (Abilita aggiornamento settimanale).
4. Selezionare la casella di controllo **attiva AutoSupport su richiesta**.
5. Selezionare **Salva**.

   AutoSupport on Demand è attivato e il supporto tecnico può inviare richieste AutoSupport on Demand a StorageGRID.

Disattiva i controlli per gli aggiornamenti software

Per impostazione predefinita, StorageGRID contatta NetApp per determinare se sono disponibili aggiornamenti software per il sistema. Se è disponibile una correzione rapida StorageGRID o una nuova versione, la nuova versione viene visualizzata nella pagina aggiornamento StorageGRID.

Se necessario, è possibile disattivare la verifica degli aggiornamenti software. Ad esempio, se il sistema non dispone di accesso WAN, disattivare il controllo per evitare errori di download.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Deselezionare la casella di controllo **Controlla aggiornamenti software**.
3. Selezionare **Salva**.

Aggiungere una destinazione AutoSupport aggiuntiva

Quando si attiva AutoSupport, i pacchetti di stato e di integrità vengono inviati al supporto tecnico. È possibile specificare una destinazione aggiuntiva per tutti i pacchetti AutoSupport.

Per verificare o modificare il protocollo utilizzato per inviare pacchetti AutoSupport, vedere le istruzioni a. Specificare il protocollo per i pacchetti AutoSupport.

> Non è possibile utilizzare il protocollo SMTP per inviare pacchetti AutoSupport a una destinazione aggiuntiva.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Selezionare **attiva destinazione AutoSupport aggiuntiva**.
3. Specificare quanto segue:

   Nome host
   Il nome host del server o l'indirizzo IP di un server di destinazione AutoSupport aggiuntivo.

È possibile inserire solo una destinazione aggiuntiva.

Porta

Porta utilizzata per connettersi a un server di destinazione AutoSupport aggiuntivo. L'impostazione predefinita è la porta 80 per HTTP o la porta 443 per HTTPS.

Convalida del certificato

Se viene utilizzato un certificato TLS per proteggere la connessione alla destinazione aggiuntiva.

- Selezionare **verifica certificato** per utilizzare la convalida del certificato.
- Selezionare **non verificare il certificato** per inviare i pacchetti AutoSupport senza la convalida del certificato.

  Selezionare questa opzione solo se si dispone di un buon motivo per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.

4. Se è stato selezionato **verifica certificato**, procedere come segue:
   a. Individuare la posizione del certificato CA.
   b. Caricare il file del certificato CA.

   Vengono visualizzati i metadati del certificato CA.
5. Selezionare **Salva**.

   Tutti i futuri pacchetti AutoSupport settimanali, attivati da eventi e attivati dall'utente verranno inviati alla destinazione aggiuntiva.

Configurazione di AutoSupport per le appliance

AutoSupport per appliance segnala problemi di hardware StorageGRID e StorageGRID AutoSupport segnala problemi di software StorageGRID, con una sola eccezione: Per SGF6112, StorageGRID AutoSupport segnala problemi di hardware e software. È necessario configurare AutoSupport su ogni appliance, ad eccezione di SGF6112, che non richiede configurazione aggiuntiva. AutoSupport viene implementato in maniera differente per le appliance di servizi e di storage.

Puoi utilizzare SANtricity per abilitare AutoSupport per ciascuna appliance di storage. È possibile configurare SANtricity AutoSupport durante la configurazione iniziale dell'appliance o dopo l'installazione di un'appliance:

- Per le appliance SG6000 e SG5700, "Configurare AutoSupport in Gestore di sistema di SANtricity"

È possibile includere in StorageGRID AutoSupport i pacchetti AutoSupport delle appliance e-Series configurando l'erogazione di AutoSupport in base al proxy "Gestore di sistema di SANtricity".

StorageGRID AutoSupport non segnala problemi di hardware, ad esempio errori DIMM o HIC (host Interface Card). Tuttavia, potrebbero verificarsi alcuni guasti ai componenti "avvisi hardware". Per le appliance StorageGRID con un controller di gestione baseboard (BMC) è possibile configurare trap e-mail e SNMP per segnalare errori hardware:

- "Impostare le notifiche e-mail per gli avvisi BMC"
- "Configurare le impostazioni SNMP per BMC"

Informazioni correlate

"Supporto NetApp"

Attivare manualmente un pacchetto AutoSupport

Per assistere il supporto tecnico nella risoluzione dei problemi del sistema StorageGRID, è possibile attivare manualmente l'invio di un pacchetto AutoSupport.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- È necessario disporre dell'autorizzazione di accesso root o di altra configurazione della griglia.

Fasi

1. Selezionare **SUPPORTO** > **Strumenti** > **AutoSupport**.
2. Nella scheda **azioni**, selezionare **Invia AutoSupport** attivato dall'utente.

   StorageGRID tenta di inviare un pacchetto AutoSupport al sito di supporto NetApp. Se il tentativo ha esito positivo, i valori **risultato più recente** e **tempo ultimo successo** nella scheda **risultati** vengono aggiornati. Se si verifica un problema, il valore **risultato più recente** viene aggiornato a "non riuscito" e StorageGRID non tenta di inviare nuovamente il pacchetto AutoSupport.

   > Dopo aver inviato un pacchetto AutoSupport attivato dall'utente, aggiornare la pagina AutoSupport nel browser dopo 1 minuto per accedere ai risultati più recenti.

Risolvere i problemi relativi ai pacchetti AutoSupport

Se un tentativo di invio di un pacchetto AutoSupport non riesce, il sistema StorageGRID esegue azioni diverse a seconda del tipo di pacchetto AutoSupport. È possibile controllare lo stato dei pacchetti AutoSupport selezionando **SUPPORT** > **Tools** > **AutoSupport** > **Results**.

Quando il pacchetto AutoSupport non riesce a inviare, viene visualizzato "non riuscito" nella scheda **risultati** della pagina **AutoSupport**.

> Se è stato configurato un server proxy per l'inoltro dei pacchetti AutoSupport a NetApp, è necessario "verificare che le impostazioni di configurazione del server proxy siano corrette".

Errore settimanale del pacchetto AutoSupport

Se un pacchetto AutoSupport settimanale non viene inviato, il sistema StorageGRID esegue le seguenti operazioni:

1. Aggiorna l'attributo dei risultati più recenti in Riprova.
2. Tenta di inviare nuovamente il pacchetto AutoSupport 15 volte ogni quattro minuti per un'ora.
3. Dopo un'ora di errori di invio, aggiorna l'attributo dei risultati più recenti su non riuscito.
4. Tenta di inviare nuovamente un pacchetto AutoSupport all'ora pianificata successiva.
5. Mantiene la normale pianificazione AutoSupport se il pacchetto non riesce perché il servizio NMS non è disponibile e se un pacchetto viene inviato prima del termine di sette giorni.
6. Quando il servizio NMS è nuovamente disponibile, invia immediatamente un pacchetto AutoSupport se

non è stato inviato per sette giorni o più.

Errore del pacchetto AutoSupport attivato dall'utente o dagli eventi

Se un pacchetto AutoSupport attivato dall'utente o da un evento non riesce a inviare, il sistema StorageGRID esegue le seguenti operazioni:

1. Visualizza un messaggio di errore se l'errore è noto. Ad esempio, se un utente seleziona il protocollo SMTP senza fornire le corrette impostazioni di configurazione dell'e-mail, viene visualizzato il seguente messaggio di errore: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Non tenta di inviare nuovamente il pacchetto.
3. Registra l'errore in `nms.log`.

Se si verifica un errore e SMTP è il protocollo selezionato, verificare che il server e-mail del sistema StorageGRID sia configurato correttamente e che il server e-mail sia in esecuzione (**SUPPORT** > **Alarms (legacy)** > **> Configurazione e-mail legacy**). Nella pagina AutoSupport potrebbe essere visualizzato il seguente messaggio di errore: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Scopri come "configurare le impostazioni del server di posta elettronica".

Correggere un errore del pacchetto AutoSupport

Se si verifica un errore e il protocollo SMTP è selezionato, verificare che il server e-mail del sistema StorageGRID sia configurato correttamente e che il server e-mail sia in esecuzione. Nella pagina AutoSupport potrebbe essere visualizzato il seguente messaggio di errore: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Invio dei pacchetti e-Series AutoSupport tramite StorageGRID

Puoi inviare pacchetti AutoSupport di e-Series SANtricity System Manager al supporto tecnico tramite un nodo amministrativo StorageGRID piuttosto che la porta di gestione dell'appliance di storage.

Vedere "AutoSupport hardware e-Series" Per ulteriori informazioni sull'utilizzo di AutoSupport con le appliance e-Series.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root o amministratore dell'appliance di storage".
- Hai configurato SANtricity AutoSupport:
  - Per le appliance SG6000 e SG5700, "Configurare AutoSupport in Gestore di sistema di SANtricity"

> È necessario disporre del firmware SANtricity 8.70 o superiore per accedere a Gestione di sistema di SANtricity utilizzando Gestione griglia.

A proposito di questa attività

I pacchetti e-Series AutoSupport contengono dettagli sull'hardware di storage e sono più specifici degli altri pacchetti AutoSupport inviati dal sistema StorageGRID.

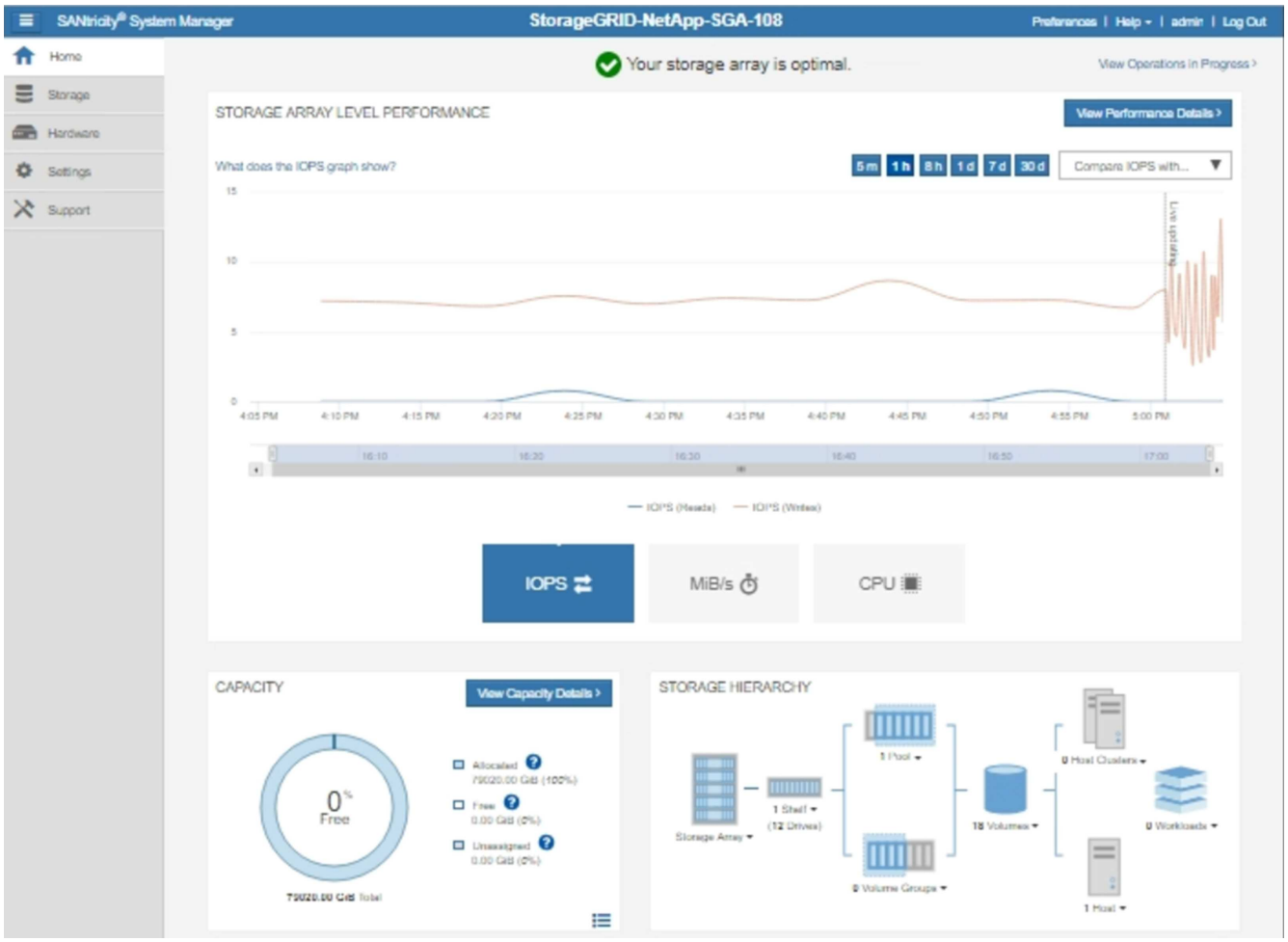
È possibile configurare un indirizzo speciale del server proxy in Gestione di sistema SANtricity per trasmettere pacchetti AutoSupport tramite un nodo amministrativo StorageGRID senza l'utilizzo della porta di gestione dell'appliance. I pacchetti AutoSupport trasmessi in questo modo vengono inviati dal "Nodo Admin mittente preferito"e ne utilizzano uno "impostazioni proxy amministratore" Che sono stati configurati in Grid Manager.

> Questa procedura si applica solo alla configurazione di un server proxy StorageGRID per i pacchetti AutoSupport e-Series. Per ulteriori informazioni sulla configurazione di e-Series AutoSupport, consultare "Documentazione NetApp e-Series e SANtricity".

Fasi

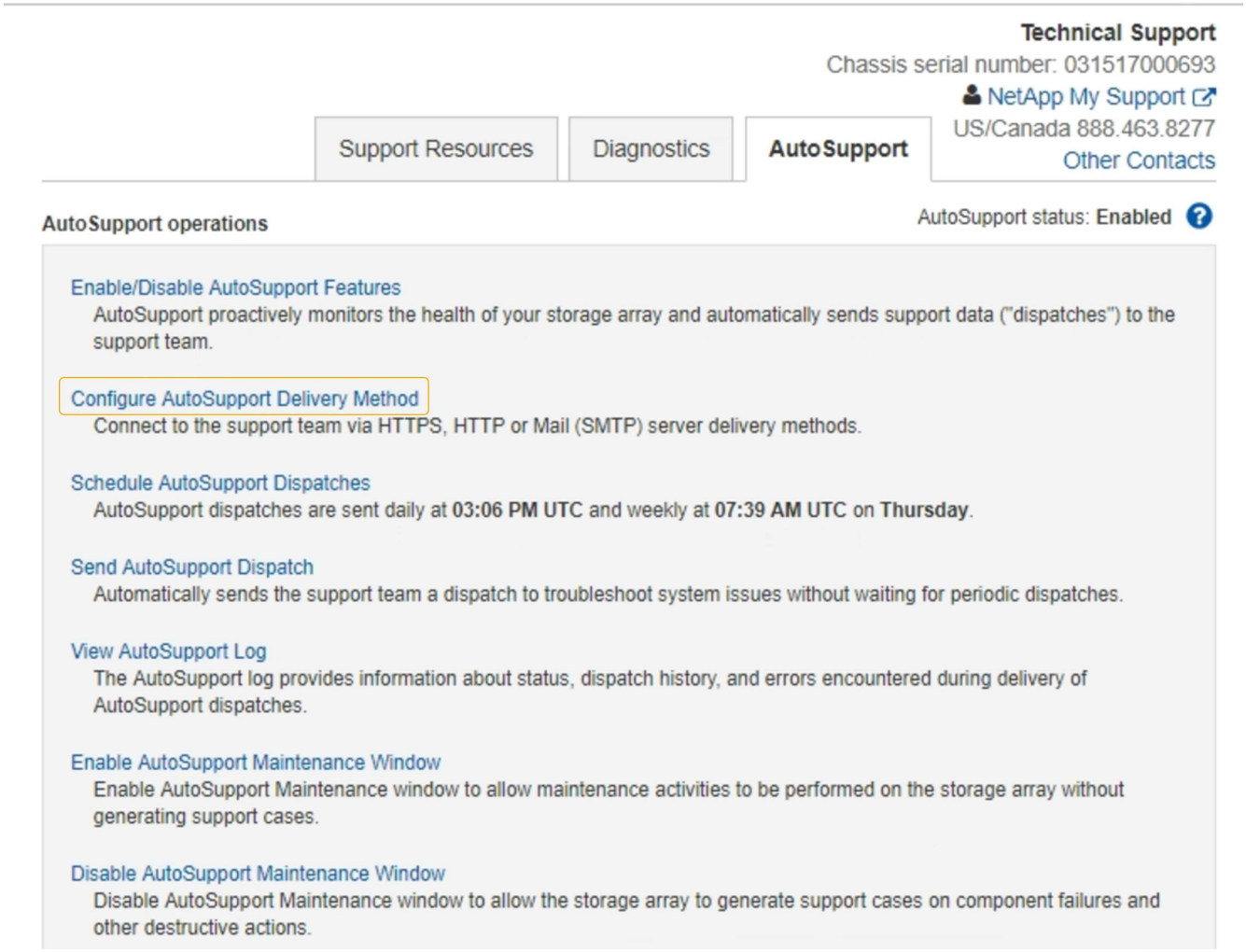
1. In Grid Manager, selezionare **NODES**.
2. Dall'elenco dei nodi a sinistra, selezionare il nodo dell'appliance di storage che si desidera configurare.
3. Selezionare **Gestore di sistema SANtricity**.

   Viene visualizzata la home page di Gestore di sistema di SANtricity.



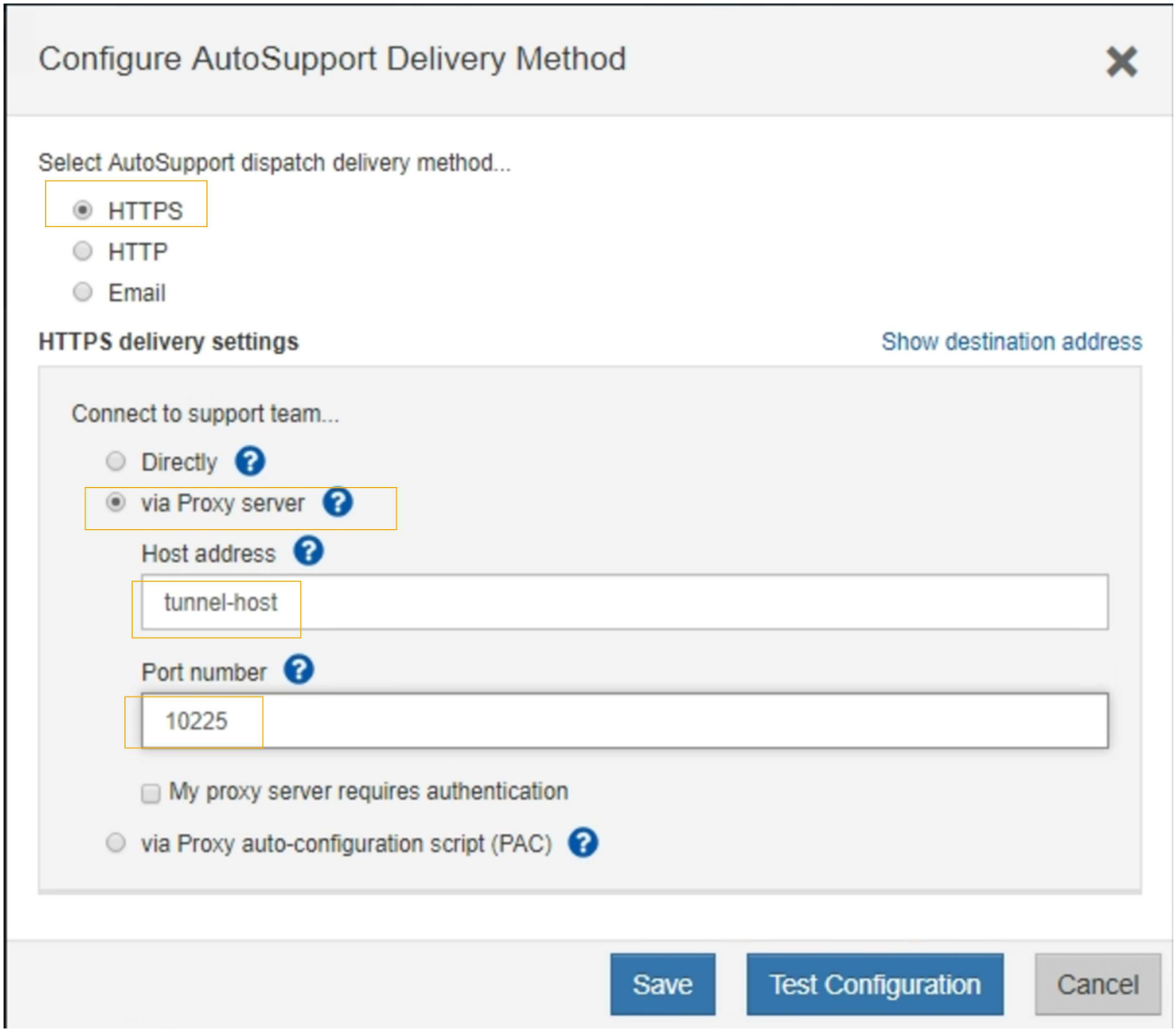
4. Selezionare **SUPPORT** > **Support Center** > **AutoSupport**.

   Viene visualizzata la pagina AutoSupport Operations.



5. Selezionare **Configura metodo di erogazione AutoSupport**.

   Viene visualizzata la pagina Configura metodo di erogazione AutoSupport.



6. Selezionare **HTTPS** per il metodo di consegna.

   Il certificato che abilita HTTPS è preinstallato.

7. Selezionare **via Proxy server**.
8. Invio `tunnel-host` Per l'indirizzo **host**.

   `tunnel-host` È l'indirizzo speciale che consente di utilizzare un nodo amministrativo per inviare pacchetti AutoSupport e-Series.

9. Invio `10225` Per il numero di porta *.

   `10225` È il numero di porta sul server proxy StorageGRID che riceve i pacchetti AutoSupport dal controller e-Series dell'appliance.

10. Selezionare **verifica configurazione** per verificare l'instradamento e la configurazione del server proxy AutoSupport.

    Se corretto, viene visualizzato un messaggio in un banner verde: "La configurazione AutoSupport è stata

verificata."

Se il test ha esito negativo, viene visualizzato un messaggio di errore su un banner rosso. Verificare le impostazioni DNS e la rete StorageGRID, quindi verificare "Nodo Admin mittente preferito" Può connettersi al sito di supporto NetApp e riprovare il test.

11. Selezionare **Salva**.

La configurazione viene salvata e viene visualizzato un messaggio di conferma: "Il metodo di consegna AutoSupport è stato configurato".

Gestire i nodi di storage

Gestione dei nodi di storage: Panoramica

I nodi di storage forniscono servizi e capacità di storage su disco. La gestione dei nodi di storage comporta quanto segue:

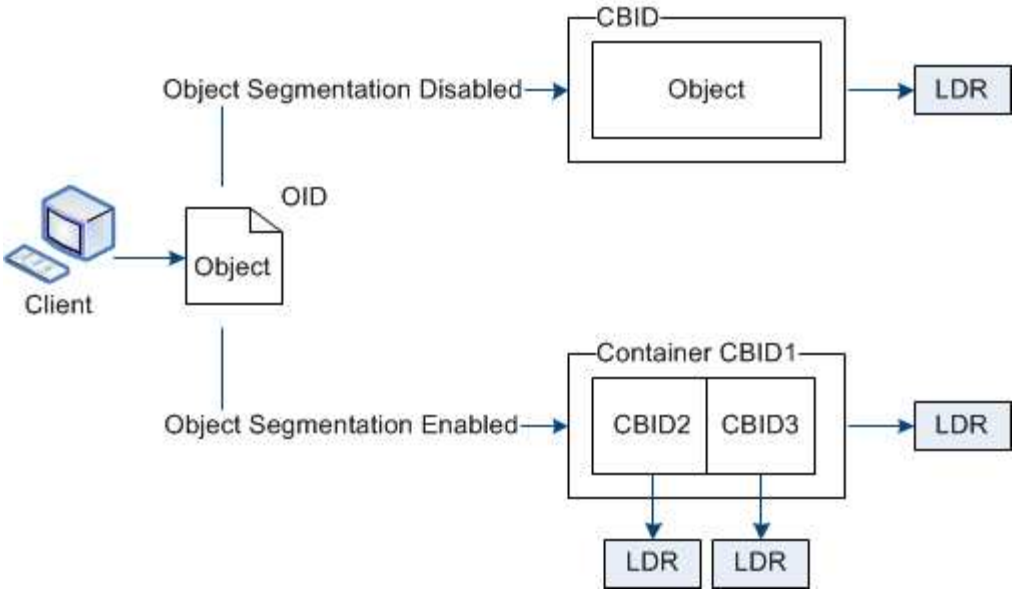
- Gestione delle opzioni di storage
- Comprendere quali sono le filigrane dei volumi di storage e come è possibile utilizzare le sovrascritture dei watermark per controllare quando i nodi di storage diventano di sola lettura
- Monitoraggio e gestione dello spazio utilizzato per i metadati degli oggetti
- Configurazione delle impostazioni globali per gli oggetti memorizzati
- Applicazione delle impostazioni di configurazione del nodo di storage
- Gestione dei nodi di storage completi

Utilizzare le opzioni di storage

Che cos'è la segmentazione degli oggetti?

La segmentazione degli oggetti è il processo di suddivisione di un oggetto in un insieme di oggetti di dimensioni fisse più piccole per ottimizzare l'utilizzo dello storage e delle risorse per oggetti di grandi dimensioni. Il caricamento multiparte S3 crea anche oggetti segmentati, con un oggetto che rappresenta ciascuna parte.

Quando un oggetto viene acquisito nel sistema StorageGRID, il servizio LDR suddivide l'oggetto in segmenti e crea un container di segmenti che elenca le informazioni di intestazione di tutti i segmenti come contenuto.



Al momento del recupero di un container di segmenti, il servizio LDR assembla l'oggetto originale dai suoi segmenti e lo restituisce al client.

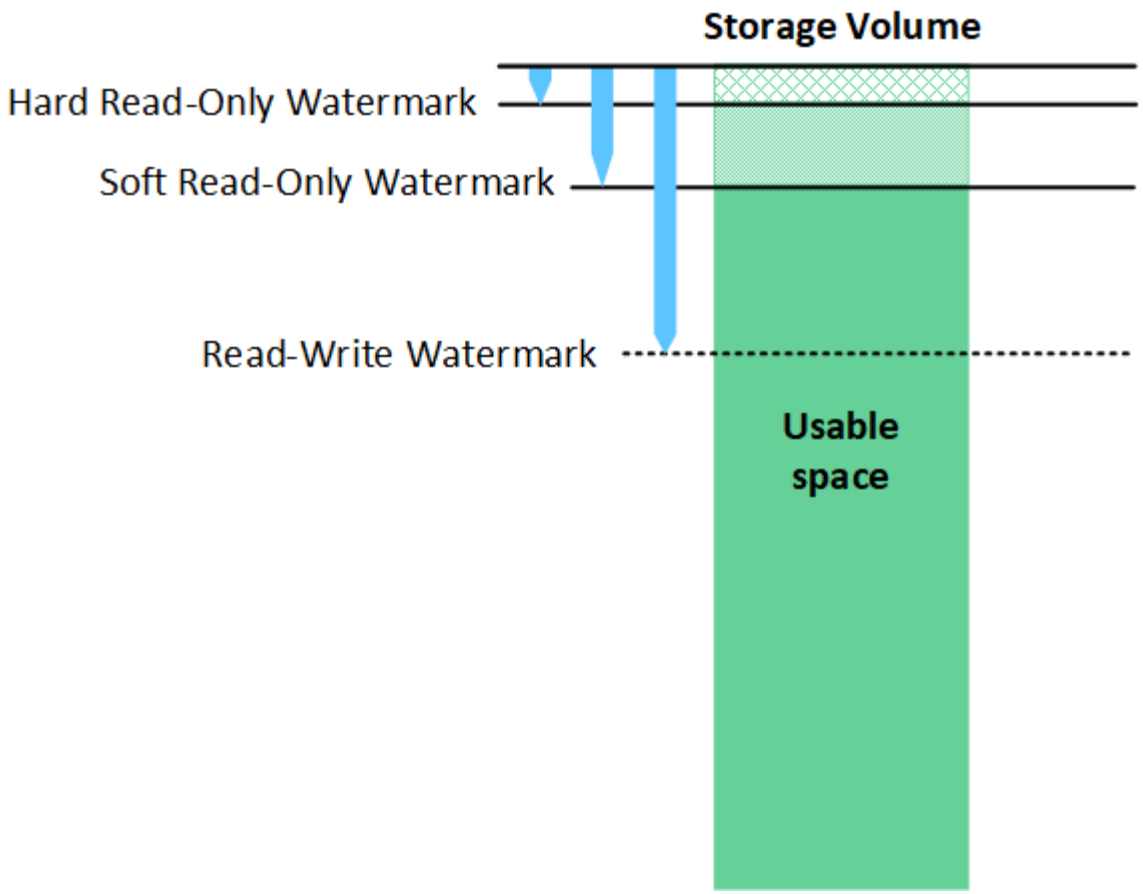
Il container e i segmenti non sono necessariamente memorizzati sullo stesso nodo di storage. Container e segmenti possono essere memorizzati in qualsiasi nodo di storage all'interno del pool di storage specificato nella regola ILM.

Ogni segmento viene trattato dal sistema StorageGRID in modo indipendente e contribuisce al conteggio di attributi come oggetti gestiti e oggetti memorizzati. Ad esempio, se un oggetto memorizzato nel sistema StorageGRID viene suddiviso in due segmenti, il valore degli oggetti gestiti aumenta di tre dopo il completamento dell'acquisizione, come segue:

```
segment container + segment 1 + segment 2 = three stored objects
```

Cosa sono le filigrane dei volumi di storage?

StorageGRID utilizza tre filigrane dei volumi di storage per garantire che i nodi di storage vengano trasferiti in modo sicuro in uno stato di sola lettura prima che lo spazio sia estremamente ridotto e per consentire ai nodi di storage che sono stati trasferiti in uno stato di sola lettura di tornare in lettura e scrittura.



Le filigrane dei volumi di storage si applicano solo allo spazio utilizzato per i dati degli oggetti replicati e codificati in cancellazione. Per ulteriori informazioni sullo spazio riservato ai metadati degli oggetti sul volume 0, visitare il sito Web "Gestire lo storage dei metadati degli oggetti".

Che cos'è la filigrana di sola lettura?

La filigrana **Storage Volume Soft Read-Only** è la prima filigrana a indicare che lo spazio utilizzabile di un nodo di storage per i dati dell'oggetto sta diventando pieno.

Se ogni volume in un nodo di storage ha meno spazio libero rispetto alla filigrana di sola lettura soft del volume, il nodo di storage passa alla *modalità di sola lettura*. La modalità di sola lettura indica che il nodo di storage annuncia servizi di sola lettura al resto del sistema StorageGRID, ma soddisfa tutte le richieste di scrittura in sospeso.

Ad esempio, si supponga che ogni volume in un nodo di storage abbia un watermark di sola lettura soft di 10 GB. Non appena ogni volume dispone di meno di 10 GB di spazio libero, il nodo di storage passa alla modalità di sola lettura.

Che cos'è la filigrana di sola lettura?

La filigrana **Storage Volume Hard Read-Only** è la filigrana successiva per indicare che lo spazio utilizzabile di un nodo per i dati dell'oggetto sta diventando pieno.

Se lo spazio libero su un volume è inferiore a quello della filigrana di sola lettura del volume, la scrittura sul volume non avrà esito positivo. Tuttavia, le scritture su altri volumi possono continuare fino a quando lo spazio libero su tali volumi non è inferiore alle filigrane di sola lettura.

Ad esempio, si supponga che ogni volume in un nodo di storage abbia un watermark di sola lettura hard di 5 GB. Non appena ogni volume dispone di meno di 5 GB di spazio libero, Storage Node non accetta più richieste di scrittura.

La filigrana hard Read-only è sempre inferiore alla filigrana soft Read-only.

Che cos'è la filigrana Read-Write?

Il watermark **Storage Volume Read-Write** si applica solo ai nodi di storage che sono passati alla modalità di sola lettura. Determina quando il nodo può diventare di nuovo in lettura/scrittura. Quando lo spazio libero su un volume di storage in un nodo di storage è superiore al watermark Read-Write di quel volume, il nodo ritorna automaticamente allo stato Read-write.

Ad esempio, supponiamo che il nodo di storage sia passato alla modalità di sola lettura. Si supponga inoltre che ogni volume abbia un watermark Read-Write di 30 GB. Non appena lo spazio libero per qualsiasi volume aumenta fino a 30 GB, il nodo diventa di nuovo in lettura/scrittura.

La filigrana Read-Write è sempre più grande della filigrana di sola lettura e della filigrana di sola lettura.

Visualizzare le filigrane dei volumi di storage

È possibile visualizzare le impostazioni correnti del watermark e i valori ottimizzati per il sistema. Se non si utilizzano filigrane ottimizzate, è possibile determinare se è possibile o necessario regolare le impostazioni.

Prima di iniziare

- L'aggiornamento a StorageGRID 11.6 o versione successiva è stato completato.
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Consente di visualizzare le impostazioni correnti del watermark

È possibile visualizzare le impostazioni correnti del filigrana dello storage in Grid Manager.

Fasi

1. Selezionare **SUPPORT** > **other** > **Storage Watermarks**.
2. Nella pagina Storage Watermark (Filigrane di archiviazione), controllare la casella di controllo Use Optimized Values (Usa valori ottimizzati).
   - Se la casella di controllo è selezionata, tutte e tre le filigrane sono ottimizzate per ogni volume di archiviazione su ogni nodo di archiviazione, in base alle dimensioni del nodo di archiviazione e alla capacità relativa del volume.

     Questa è l'impostazione predefinita e consigliata. Non aggiornare questi valori. Se lo si desidera, è possibile Visualizza filigrane di storage ottimizzate.

   - Se la casella di controllo Usa valori ottimizzati non è selezionata, vengono utilizzate filigrane personalizzate (non ottimizzate). Si sconsiglia di utilizzare le impostazioni personalizzate della filigrana. Seguire le istruzioni per "Risoluzione dei problemi gli avvisi di override del watermark di sola lettura bassa" per determinare se è possibile o necessario regolare le impostazioni.

     Quando si specificano le impostazioni personalizzate della filigrana, è necessario immettere valori superiori a 0.

Visualizza filigrane di memorizzazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati che ha calcolato per la filigrana di sola lettura del volume di storage **Soft Read-only**. È possibile visualizzare i valori minimi e massimi ottimizzati per ciascun nodo di storage nella griglia.

1. Selezionare **SUPPORT** > **Tools** > **Metrics**.
2. Nella sezione Prometheus, selezionare il collegamento per accedere all'interfaccia utente Prometheus.
3. Per visualizzare la filigrana minima di sola lettura soft consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   L'ultima colonna mostra il valore minimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage. Se questo valore è superiore all'impostazione personalizzata per **Storage Volume Soft Read-Only Watermark**, viene attivato l'avviso **Low Read-only watermark override** per il nodo di storage.

4. Per visualizzare la filigrana di sola lettura soft massima consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   L'ultima colonna mostra il valore massimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage.

Gestire lo storage dei metadati degli oggetti

La capacità dei metadati degli oggetti di un sistema StorageGRID controlla il numero massimo di oggetti che possono essere memorizzati in tale sistema. Per garantire che il sistema StorageGRID disponga di spazio sufficiente per memorizzare nuovi oggetti, è necessario comprendere dove e come StorageGRID memorizza i metadati degli oggetti.

Che cos'è il metadata a oggetti?

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.

Per un oggetto in StorageGRID, i metadati dell'oggetto includono i seguenti tipi di informazioni:

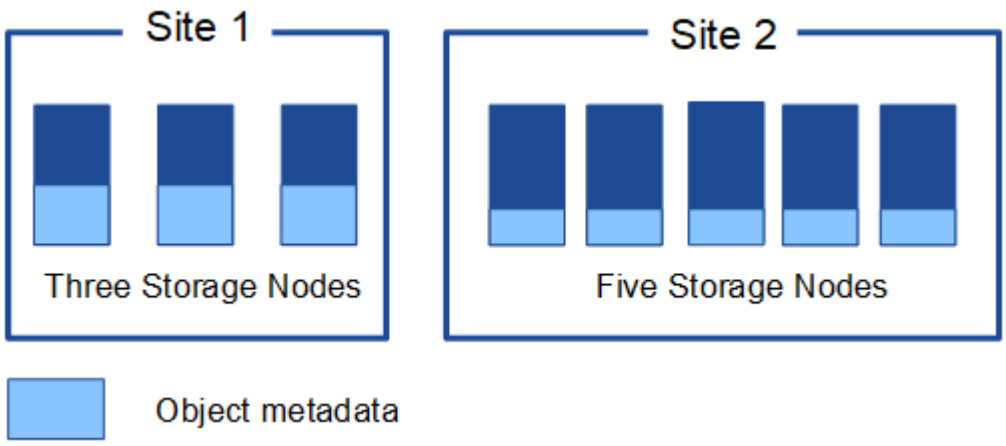
- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3 o del container Swift, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora in cui l'oggetto è stato creato per la prima volta, e la data e l'ora dell'ultima modifica dell'oggetto.
- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
- Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.

- Per oggetti segmentati e multiparte, identificatori di segmenti e dimensioni dei dati.

Come vengono memorizzati i metadati degli oggetti?

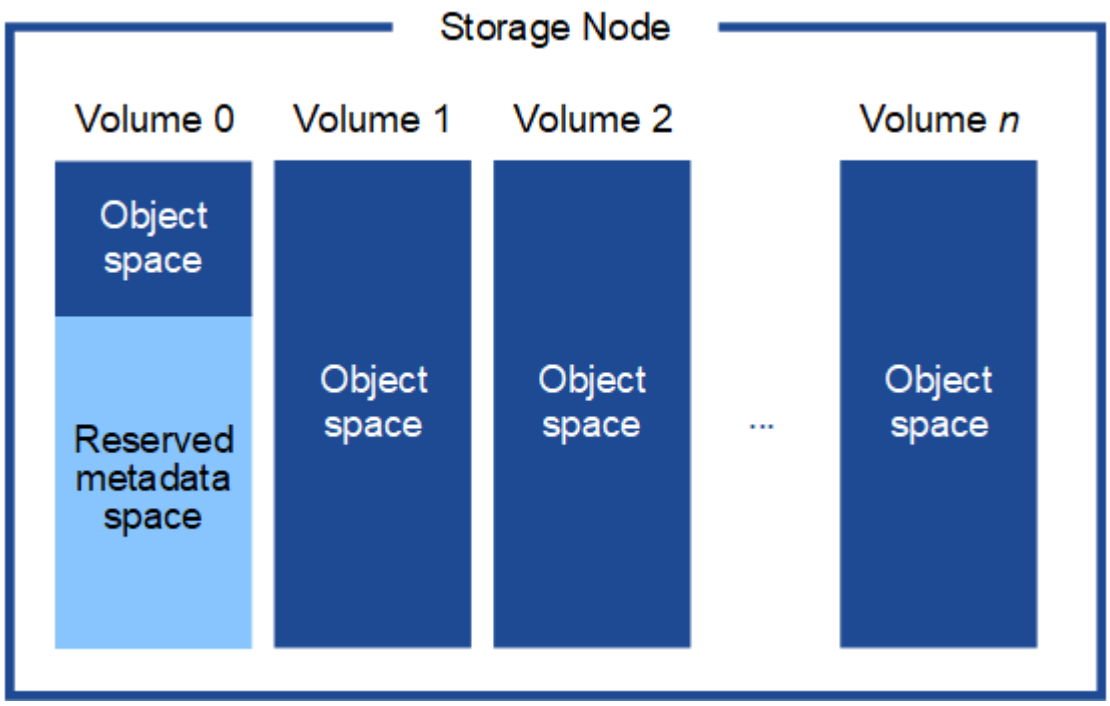
StorageGRID mantiene i metadati degli oggetti in un database Cassandra, che viene memorizzato indipendentemente dai dati degli oggetti. Per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti del sistema in ogni sito.

Questa figura rappresenta i nodi di storage in due siti. Ogni sito ha la stessa quantità di metadati oggetto e i metadati di ciascun sito sono suddivisi tra tutti i nodi di storage di quel sito.



Dove sono memorizzati i metadati degli oggetti?

Questa figura rappresenta i volumi di storage per un singolo nodo di storage.



Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di storage 0 di ciascun nodo di storage. Utilizza lo spazio riservato per memorizzare i metadati degli oggetti e per eseguire le operazioni essenziali del database. Qualsiasi spazio rimanente sul volume di storage 0 e tutti gli altri volumi di storage nel nodo di storage vengono utilizzati esclusivamente per i dati a oggetti (copie replicate e frammenti

con codifica di cancellazione).

La quantità di spazio riservato ai metadati degli oggetti su un nodo di storage specifico dipende da diversi fattori, descritti di seguito.

Impostazione dello spazio riservato dei metadati

Lo *spazio riservato metadati* è un'impostazione a livello di sistema che rappresenta la quantità di spazio che sarà riservata ai metadati sul volume 0 di ogni nodo di archiviazione. Come mostrato nella tabella, il valore predefinito di questa impostazione si basa su:

- La versione software utilizzata al momento dell'installazione iniziale di StorageGRID.
- La quantità di RAM su ciascun nodo di storage.

Versione utilizzata per l'installazione iniziale di StorageGRID	Quantità di RAM sui nodi di storage	Impostazione predefinita spazio riservato metadati
da 11,5 a 11,8	128 GB o più su ciascun nodo di storage nella griglia	8 TB (8,000 GB)
	Meno di 128 GB su qualsiasi nodo di storage nel grid	3 TB (3.000 GB)
da 11,1 a 11,4	128 GB o più su ciascun nodo di storage in un sito qualsiasi	4 TB (4.000 GB)
	Meno di 128 GB su qualsiasi nodo di storage in ogni sito	3 TB (3.000 GB)
11,0 o precedente	Qualsiasi importo	2 TB (2.000 GB)

Visualizza impostazione spazio riservato metadati

Per visualizzare l'impostazione dello spazio riservato ai metadati per il sistema StorageGRID, procedere come segue.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Impostazioni archiviazione**.
2. Nella pagina Impostazioni archiviazione, espandere la sezione **spazio riservato metadati**.

Per StorageGRID 11,8 o versione successiva, il valore dello spazio riservato dei metadati deve essere almeno 100 GB e non più di 1 PB.

L'impostazione predefinita per una nuova installazione di StorageGRID 11,6 o superiore in cui ogni nodo di archiviazione ha 128 GB o più di RAM è 8.000 GB (8 TB).

Spazio riservato effettivo per i metadati

A differenza dell'impostazione dello spazio riservato ai metadati a livello di sistema, per ogni nodo di archiviazione viene determinato lo *spazio riservato effettivo* per i metadati dell'oggetto. Per qualsiasi nodo di

archiviazione, lo spazio riservato effettivo per i metadati dipende dalla dimensione del volume 0 per il nodo e dall'impostazione dello spazio riservato metadati a livello di sistema.

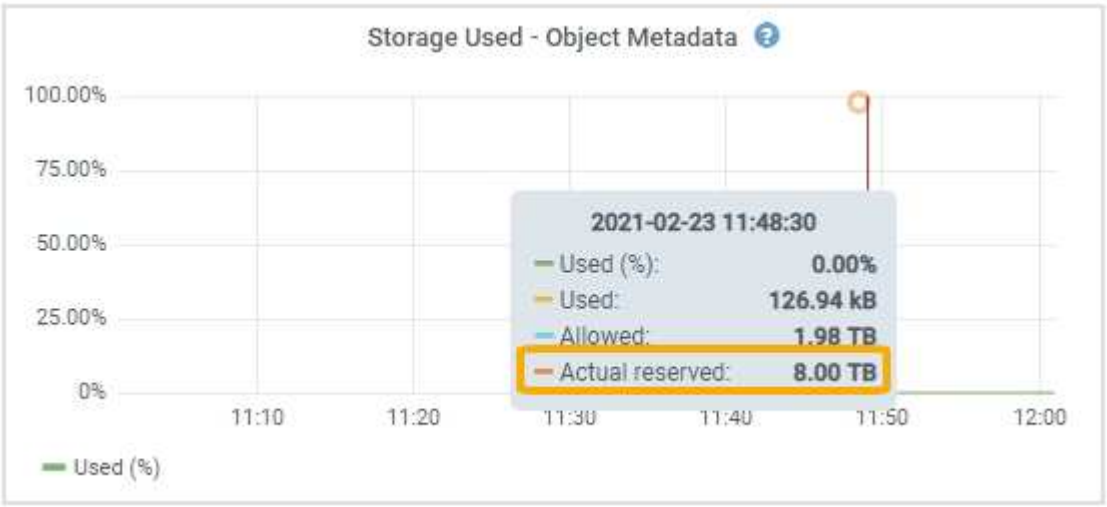
Dimensione del volume 0 per il nodo	Spazio riservato effettivo per i metadati
Meno di 500 GB (non in produzione)	10% del volume 0
500 GB o più o Nodi di storage solo metadati	Il minore di questi valori: • Volume 0 • Impostazione dello spazio riservato dei metadati **Nota**: È richiesto un solo rangedb per i nodi di archiviazione di solo metadati.

Visualizzare lo spazio riservato effettivo per i metadati

Per visualizzare lo spazio riservato effettivo per i metadati su un nodo di storage specifico, procedere come segue.

Fasi

1. Da Grid Manager, selezionare **NODES** > ***Storage Node***.
2. Selezionare la scheda **Storage**.
3. Posizionare il cursore sul grafico Storage used - Object Metadata (Storage utilizzato - metadati oggetto) e individuare il valore **Actual reserved** (riservato).



Nella schermata, il valore **effettivo riservato** è 8 TB. Questa schermata riguarda un nodo di storage di grandi dimensioni in una nuova installazione di StorageGRID 11.6. Poiché l'impostazione dello spazio riservato ai metadati a livello di sistema è inferiore al volume 0 per questo nodo di archiviazione, lo spazio riservato effettivo per questo nodo è uguale all'impostazione dello spazio riservato ai metadati.

Esempio di spazio riservato effettivo dei metadati

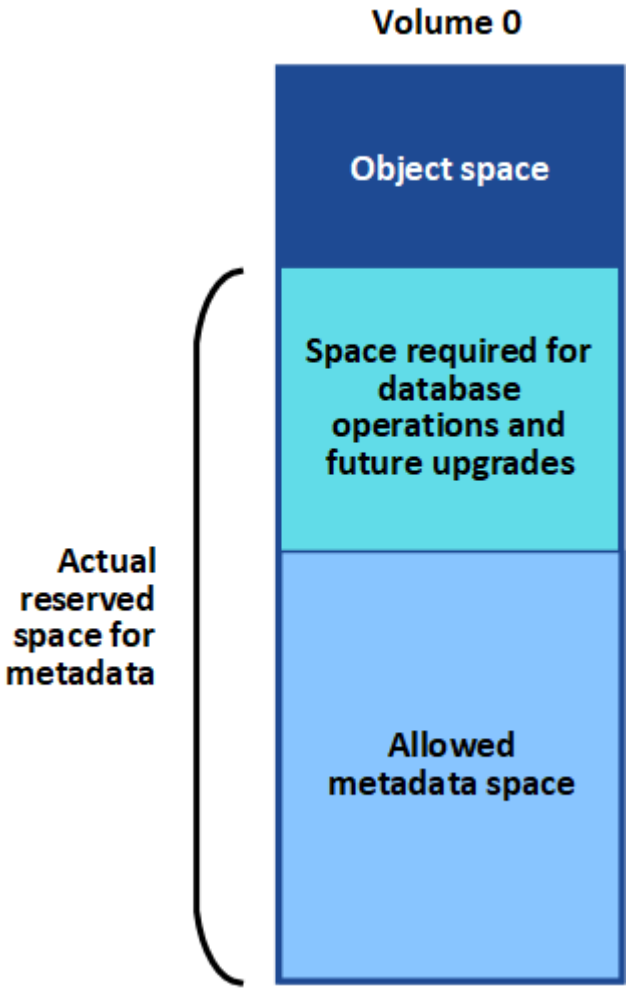
Si supponga di installare un nuovo sistema StorageGRID utilizzando la versione 11,7 o successiva. In questo esempio, si supponga che ogni nodo di storage abbia più di 128 GB di RAM e che il volume 0 del nodo di

storage 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo spazio riservato * dei metadati a livello di sistema è impostato su 8 TB. (Questo è il valore predefinito per una nuova installazione di StorageGRID 11.6 o superiore se ogni nodo di storage ha più di 128 GB di RAM).
- Lo spazio riservato effettivo per i metadati per SN1 è di 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione **spazio riservato metadati**).

Spazio consentito di metadati

Lo spazio riservato effettivo di ciascun nodo di storage per i metadati viene suddiviso nello spazio disponibile per i metadati dell'oggetto (il *spazio consentito per i metadati*) e nello spazio necessario per le operazioni essenziali del database (come la compattazione e la riparazione) e per i futuri aggiornamenti hardware e software. Lo spazio consentito per i metadati regola la capacità complessiva degli oggetti.



La seguente tabella mostra come StorageGRID calcola lo spazio di metadati consentito* per diversi nodi di storage, in base alla quantità di memoria per il nodo e allo spazio riservato effettivo per i metadati.

		Quantità di memoria sul nodo di storage	
	≪ 128 GB	>= 128 GB	**Spazio riservato effettivo per i metadati**

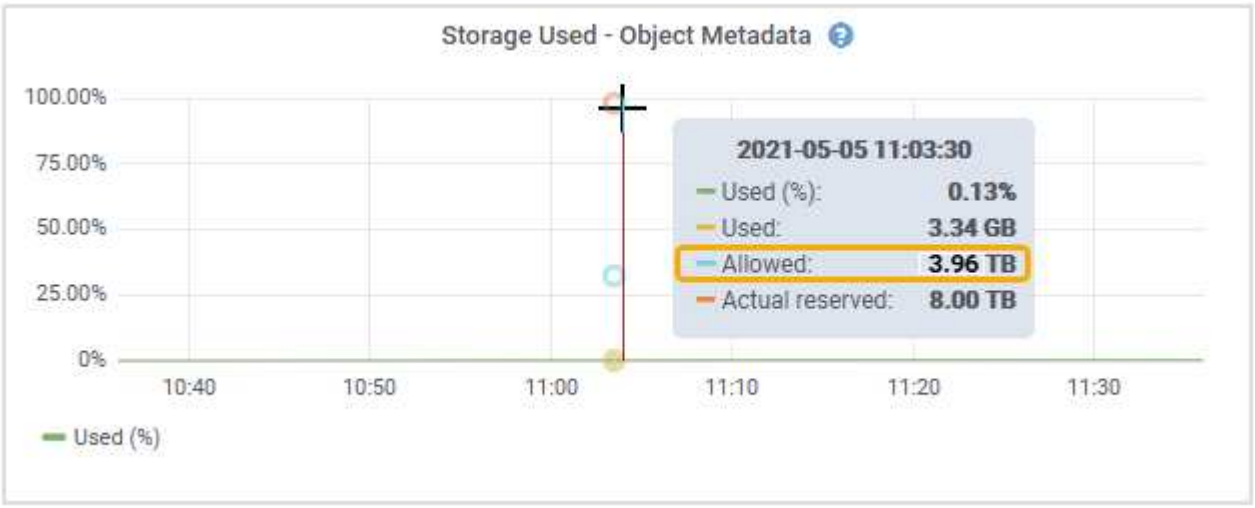
≪= 4 TB	60% dello spazio riservato effettivo per i metadati, fino a un massimo di 1.32 TB	60% dello spazio riservato effettivo per i metadati, fino a un massimo di 1,98 TB	4 TB

Visualizzare lo spazio consentito per i metadati

Per visualizzare lo spazio di metadati consentito per un nodo di storage, procedere come segue.

Fasi

1. Da Grid Manager, selezionare **NODES**.
2. Selezionare il nodo di storage.
3. Selezionare la scheda **Storage**.
4. Posizionare il cursore sul grafico dei metadati Storage used - Object e individuare il valore **Allowed**.



Nella schermata, il valore **Allowed** è 3,96 TB, che è il valore massimo per un nodo di archiviazione il cui spazio riservato effettivo per i metadati è superiore a 4 TB.

Il valore **Allowed** corrisponde a questa metrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Esempio di spazio consentito per i metadati

Si supponga di installare un sistema StorageGRID utilizzando la versione 11.6. In questo esempio, si supponga che ogni nodo di storage abbia più di 128 GB di RAM e che il volume 0 del nodo di storage 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo spazio riservato * dei metadati a livello di sistema è impostato su 8 TB. (Questo è il valore predefinito per StorageGRID 11.6 o superiore quando ogni nodo di storage ha più di 128 GB di RAM).
- Lo spazio riservato effettivo per i metadati per SN1 è di 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione **spazio riservato metadati**).

- Lo spazio consentito per i metadati su SN1 è di 3 TB, in base al calcolo mostrato nella tabella per lo spazio consentito per i metadati: (Spazio riservato effettivo per i metadati − 1 TB) × 60%, fino a un massimo di 3.96 TB.

In che modo i nodi di storage di diverse dimensioni influiscono sulla capacità degli oggetti

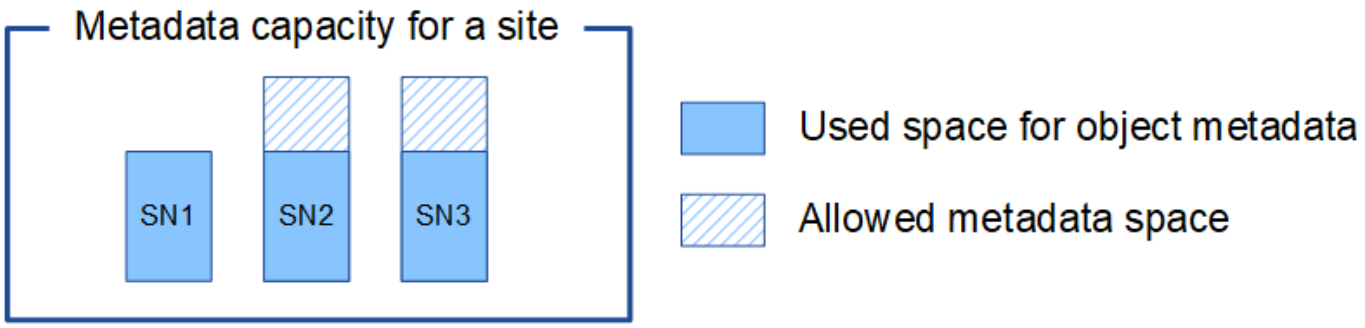
Come descritto in precedenza, StorageGRID distribuisce uniformemente i metadati degli oggetti nei nodi di storage di ciascun sito. Per questo motivo, se un sito contiene nodi di storage di dimensioni diverse, il nodo più piccolo del sito determina la capacità di metadati del sito.

Si consideri il seguente esempio:

- Si dispone di un grid a sito singolo contenente tre nodi di storage di dimensioni diverse.
- L'impostazione **spazio riservato metadati** è 4 TB.
- I nodi di storage hanno i seguenti valori per lo spazio riservato effettivo dei metadati e per lo spazio consentito dei metadati.

Nodo di storage	Dimensione del volume 0	Spazio riservato effettivo dei metadati	Spazio consentito di metadati
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Poiché i metadati degli oggetti sono distribuiti in modo uniforme tra i nodi di storage di un sito, ciascun nodo di questo esempio può contenere solo 1.32 TB di metadati. I 0.66 TB aggiuntivi di spazio consentito per i metadati SN2 e SN3 non possono essere utilizzati.



Analogamente, poiché StorageGRID gestisce tutti i metadati degli oggetti per un sistema StorageGRID in ogni sito, la capacità complessiva dei metadati di un sistema StorageGRID è determinata dalla capacità dei metadati degli oggetti del sito più piccolo.

Inoltre, poiché la capacità dei metadati degli oggetti controlla il numero massimo di oggetti, quando un nodo esaurisce la capacità dei metadati, la griglia è effettivamente piena.

Informazioni correlate

- Per informazioni su come monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage, vedere le istruzioni per "Monitoraggio di StorageGRID".

- Per aumentare la capacità dei metadati degli oggetti per il sistema, "espandere una griglia" Aggiungendo nuovi nodi di storage.

Aumentare l'impostazione spazio riservato metadati

È possibile aumentare l'impostazione del sistema spazio riservato metadati se i nodi di archiviazione soddisfano requisiti specifici per la RAM e lo spazio disponibile.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root o configurazione pagina topologia griglia e altre autorizzazioni di configurazione griglia".

A proposito di questa attività

Potrebbe essere possibile aumentare manualmente l'impostazione dello spazio riservato dei metadati a livello di sistema fino a 8 TB.

È possibile aumentare il valore dell'impostazione spazio riservato metadati a livello di sistema solo se entrambe le istruzioni sono vere:

- I nodi di storage di qualsiasi sito del sistema dispongono ciascuno di almeno 128 GB di RAM.
- I nodi di storage di qualsiasi sito del sistema dispongono ciascuno di spazio disponibile sufficiente sul volume di storage 0.

Se si aumenta questa impostazione, si riduce contemporaneamente lo spazio disponibile per lo storage a oggetti sul volume di storage 0 di tutti i nodi di storage. Per questo motivo, potrebbe essere preferibile impostare Metadata Reserved Space su un valore inferiore a 8 TB, in base ai requisiti previsti per i metadati degli oggetti.

> In generale, è meglio utilizzare un valore più alto invece di un valore più basso. Se l'impostazione spazio riservato metadati è troppo grande, è possibile ridurla in un secondo momento. Al contrario, se si aumenta il valore in un secondo momento, il sistema potrebbe dover spostare i dati dell'oggetto per liberare spazio.

Per una spiegazione dettagliata di come l'impostazione spazio riservato metadati influisce sullo spazio consentito per l'archiviazione dei metadati dell'oggetto su un nodo di archiviazione specifico, vedere "Gestire lo storage dei metadati degli oggetti".

Fasi

1. Determinare l'impostazione corrente di Metadata Reserved Space.
   a. Selezionare **CONFIGURATION** > **System** > **Storage options**.
   b. Nella sezione Storage Watermarks (Filigrane di archiviazione), annotare il valore **Metadata Reserved Space** (spazio riservato metadati).
2. Assicurarsi di disporre di spazio disponibile sufficiente sul volume di storage 0 di ciascun nodo di storage per aumentare questo valore.
   a. Selezionare **NODI**.
   b. Selezionare il primo nodo di storage nella griglia.
   c. Selezionare la scheda Storage (archiviazione).
   d. Nella sezione Volumes (volumi), individuare la voce **/var/local/rangedb/0**.

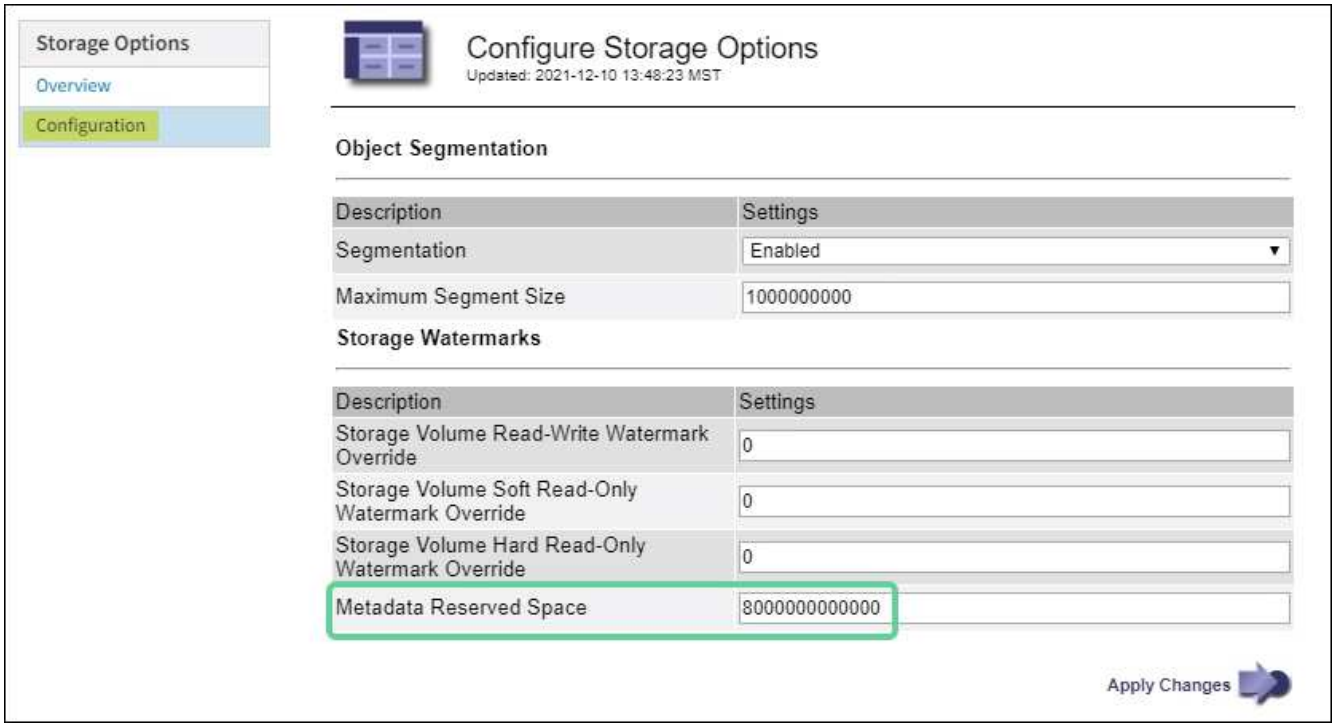
e. Verificare che il valore disponibile sia uguale o superiore alla differenza tra il nuovo valore che si desidera utilizzare e il valore corrente dello spazio riservato dei metadati.

   Ad esempio, se l'impostazione spazio riservato metadati è attualmente di 4 TB e si desidera aumentarla a 6 TB, il valore disponibile deve essere pari o superiore a 2 TB.

f. Ripetere questi passaggi per tutti i nodi di storage.
   - Se uno o più nodi di storage non dispongono di spazio disponibile sufficiente, non è possibile aumentare il valore Metadata Reserved Space (spazio riservato metadati). Non continuare con questa procedura.
   - Se ogni nodo di storage dispone di spazio disponibile sufficiente sul volume 0, passare alla fase successiva.

3. Assicurarsi di disporre di almeno 128 GB di RAM su ciascun nodo di storage.
   a. Selezionare **NODI**.
   b. Selezionare il primo nodo di storage nella griglia.
   c. Selezionare la scheda **hardware**.
   d. Posizionare il cursore del mouse sul grafico utilizzo memoria. Assicurarsi che la memoria totale sia di almeno 128 GB.
   e. Ripetere questi passaggi per tutti i nodi di storage.
      - Se uno o più nodi di storage non dispongono di memoria totale sufficiente, non è possibile aumentare il valore Metadata Reserved Space (spazio riservato metadati). Non continuare con questa procedura.
      - Se ciascun nodo di storage dispone di almeno 128 GB di memoria totale, passare alla fase successiva.
4. Aggiornare l'impostazione Metadata Reserved Space (spazio riservato metadati).
   a. Selezionare **CONFIGURATION** > **System** > **Storage options**.
   b. Selezionare la scheda Configurazione.
   c. Nella sezione Storage Watermarks (Filigrane di archiviazione), selezionare **Metadata Reserved Space** (spazio riservato metadati).
   d. Inserire il nuovo valore.

      Ad esempio, per inserire 8 TB, che è il valore massimo supportato, inserire **8000000000000** (8, seguito da 12 zeri)



a. Selezionare **Applica modifiche**.

Compressione degli oggetti memorizzati

È possibile attivare la compressione degli oggetti per ridurre le dimensioni degli oggetti memorizzati in StorageGRID, in modo che gli oggetti consumino meno spazio di storage.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Per impostazione predefinita, la compressione degli oggetti è disattivata. Se si attiva la compressione, StorageGRID tenta di comprimere ogni oggetto durante il salvataggio, utilizzando la compressione senza perdita di dati.

> Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

Prima di attivare la compressione degli oggetti, tenere presente quanto segue:

- Non selezionare **compress stored objects** a meno che non si sappia che i dati memorizzati sono comprimibili.
- Le applicazioni che salvano oggetti in StorageGRID potrebbero comprimere gli oggetti prima di salvarli. Se un'applicazione client ha già compresso un oggetto prima di salvarlo in StorageGRID, selezionando questa opzione non si ridurrà ulteriormente la dimensione di un oggetto.
- Non selezionare **compress stored objects** se si utilizza NetApp FabricPool con StorageGRID.
- Se si seleziona **compress stored objects**, le applicazioni client S3 e Swift devono evitare di eseguire operazioni GetObject che specificano un intervallo di byte da restituire. Queste operazioni di "lettura

dell'intervallo" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. Le operazioni GetObject che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è inefficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

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

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

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Impostazioni archiviazione** > **compressione oggetti**.
2. Selezionare la casella di controllo **Comprimi oggetti memorizzati**.
3. Selezionare **Salva**.

Impostazioni di configurazione del nodo di storage

Ogni nodo di storage utilizza diverse impostazioni di configurazione e contatori. Potrebbe essere necessario visualizzare le impostazioni correnti o reimpostare i contatori per cancellare gli allarmi (sistema precedente).

> Ad eccezione di quando espressamente indicato nella documentazione, è necessario consultare il supporto tecnico prima di modificare le impostazioni di configurazione di Storage Node. Se necessario, è possibile reimpostare i contatori degli eventi per cancellare gli allarmi legacy.

Per accedere alle impostazioni di configurazione e ai contatori di un nodo di storage, procedere come segue.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > ***Storage Node***.
3. Espandere il nodo di storage e selezionare il servizio o il componente.
4. Selezionare la scheda **Configurazione**.

Le seguenti tabelle riassumono le impostazioni di configurazione del nodo di storage.

LDR

Nome attributo	Codice	Descrizione
HTTP state (Stato HTTP)	HSTE	Lo stato corrente di HTTP per S3, Swift e altro traffico StorageGRID interno: • Offline: Non sono consentite operazioni e qualsiasi applicazione client che tenta di aprire una sessione HTTP al servizio LDR riceve un messaggio di errore. Le sessioni attive vengono normalmente chiuse. • Online: Il funzionamento continua normalmente

Nome attributo	Codice	Descrizione
Avvio automatico HTTP	HTA	• Se selezionata, lo stato del sistema al riavvio dipende dallo stato del componente **LDR** > **Storage**. Se il componente **LDR** > **Storage** è di sola lettura al riavvio, anche l'interfaccia HTTP è di sola lettura. Se il componente **LDR** > **Storage** è Online, anche HTTP è Online. In caso contrario, l'interfaccia HTTP rimane in stato Offline. • Se l'opzione non è selezionata, l'interfaccia HTTP rimane offline fino a quando non viene attivata esplicitamente.

LDR > Archivio dati

Nome attributo	Codice	Descrizione
Ripristina conteggio oggetti persi	RCOR	Ripristina il contatore per il numero di oggetti persi su questo servizio.

LDR > Storage (Storage)

Nome attributo	Codice	Descrizione
Stato di storage — desiderato	SSD	Un'impostazione configurabile dall'utente per lo stato desiderato del componente di storage. Il servizio LDR legge questo valore e tenta di corrispondere allo stato indicato da questo attributo. Il valore è persistente durante i riavvii. Ad esempio, è possibile utilizzare questa impostazione per forzare lo storage a diventare di sola lettura anche in presenza di ampio spazio di storage disponibile. Questo può essere utile per la risoluzione dei problemi. L'attributo può assumere uno dei seguenti valori: • Offline: Quando lo stato desiderato è offline, il servizio LDR porta il componente **LDR** > **Storage** offline. • Sola lettura: Quando lo stato desiderato è di sola lettura, il servizio LDR sposta lo stato di archiviazione in sola lettura e interrompe l'accettazione del nuovo contenuto. Tuttavia, il servizio LDR continua ad accettare richieste di eliminazione e eliminazione S3 o gestite da ILM. Tenere presente che il contenuto potrebbe continuare a essere salvato nel nodo di storage per un breve periodo di tempo fino alla chiusura delle sessioni aperte. • Online: Lasciare il valore in Online durante le normali operazioni di sistema. Lo stato di storage — corrente del componente di storage viene impostato dinamicamente dal servizio in base alle condizioni del servizio LDR, ad esempio la quantità di spazio di storage a oggetti disponibile. Se lo spazio è basso, il componente diventa di sola lettura.
Timeout controllo stato di salute	STC	Il limite di tempo in secondi entro il quale deve essere completato un test di controllo dello stato di salute per poter considerare un volume di storage integro. Modificare questo valore solo se richiesto dal supporto.

LDR > verifica

Nome attributo	Codice	Descrizione
Ripristina numero oggetti mancanti	VCMI	Ripristina il numero di oggetti mancanti rilevati (OMIS). Utilizzare solo dopo il completamento del controllo dell'esistenza dell'oggetto. I dati degli oggetti replicati mancanti vengono ripristinati automaticamente dal sistema StorageGRID.
Tasso di verifica	VPRI	Imposta la velocità con cui avviene la verifica in background. Vedere le informazioni sulla configurazione della velocità di verifica in background.
Ripristina numero oggetti corrotti	VCCR	Ripristinare il contatore per i dati degli oggetti replicati danneggiati rilevati durante la verifica in background. Questa opzione può essere utilizzata per eliminare la condizione di allarme OCOR (Corrupt Objects Detected).
Elimina oggetti in quarantena	OQRT	Eliminare gli oggetti corrotti dalla directory di quarantena, azzerare il numero di oggetti in quarantena e annullare l'allarme di rilevamento oggetti in quarantena (OQRT). Questa opzione viene utilizzata dopo il ripristino automatico degli oggetti corrotti da parte del sistema StorageGRID. Se viene attivato un allarme oggetti persi, il supporto tecnico potrebbe voler accedere agli oggetti in quarantena. In alcuni casi, gli oggetti in quarantena potrebbero essere utili per il ripristino dei dati o per il debug dei problemi sottostanti che hanno causato le copie degli oggetti corrotte.

LDR > Erasure coding (codifica cancellazione)

Nome attributo	Codice	Descrizione
Azzera conteggio errori di scrittura	RSWF	Reimpostare il contatore per gli errori di scrittura dei dati degli oggetti con codifica erasure sul nodo di storage.
Il ripristino legge il numero di errori	RSRF	Reimpostare il contatore per gli errori di lettura dei dati degli oggetti con codifica erasure dal nodo di storage.
Ripristina Elimina numero di errori	RSDF	Reimpostare il contatore per gli errori di eliminazione dei dati degli oggetti con codifica erasure dal nodo di storage.

Nome attributo	Codice	Descrizione
Ripristina numero copie corrotte rilevate	RSCC	Reimpostare il contatore per il numero di copie corrotte dei dati degli oggetti con codifica di cancellazione sul nodo di storage.
Ripristina numero di frammenti corrotti rilevati	RSCD	Reimpostare il contatore per i frammenti corrotti di dati di oggetti con codifica di cancellazione sul nodo di storage.
Ripristina numero frammenti mancanti rilevati	RSMD	Reimpostare il contatore per i frammenti mancanti di dati di oggetti con codifica di cancellazione sul nodo di storage. Utilizzare solo dopo il completamento del controllo dell'esistenza dell'oggetto.

LDR > Replica

Nome attributo	Codice	Descrizione
Ripristina conteggio errori replica in entrata	RIC	Reimpostare il contatore per gli errori di replica in entrata. Questa opzione può essere utilizzata per cancellare l'allarme RIRF (Inbound Replication — Failed).
Ripristina conteggio errori replica in uscita	ROCR	Reimpostare il contatore per gli errori di replica in uscita. Questa opzione può essere utilizzata per cancellare l'allarme RORF (Outbound Replications — Failed).
Disattiva replica in entrata	DSIR	Selezionare questa opzione per disattivare la replica in entrata come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento. Quando la replica in entrata è disattivata, gli oggetti possono essere recuperati dal nodo di storage per la copia in altre posizioni nel sistema StorageGRID, ma gli oggetti non possono essere copiati in questo nodo di storage da altre posizioni: Il servizio LDR è di sola lettura.

Nome attributo	Codice	Descrizione
Disattiva la replica in uscita	DSOR	Selezionare questa opzione per disattivare la replica in uscita (incluse le richieste di contenuto per i retrievals HTTP) come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento. Quando la replica in uscita è disattivata, gli oggetti possono essere copiati in questo nodo di storage, ma gli oggetti non possono essere recuperati dal nodo di storage per essere copiati in altre posizioni nel sistema StorageGRID. Il servizio LDR è di sola scrittura.

Gestire nodi storage completi

Man mano che i nodi di storage raggiungono la capacità, è necessario espandere il sistema StorageGRID con l'aggiunta di nuovo storage. Sono disponibili tre opzioni: Aggiunta di volumi di storage, aggiunta di shelf di espansione dello storage e aggiunta di nodi di storage.

Aggiungere volumi di storage

Ciascun nodo di storage supporta un numero massimo di volumi di storage. Il valore massimo definito varia in base alla piattaforma. Se un nodo di storage contiene meno del numero massimo di volumi di storage, è possibile aggiungere volumi per aumentarne la capacità. Consultare le istruzioni per "Espansione di un sistema StorageGRID".

Aggiungere shelf di espansione dello storage

Alcuni nodi di storage delle appliance StorageGRID, come SG6060 o SG6160, sono in grado di supportare shelf di storage aggiuntivi. Se si dispone di appliance StorageGRID con funzionalità di espansione che non sono già state estese alla capacità massima, è possibile aggiungere shelf di storage per aumentare la capacità. Consultare le istruzioni per "Espansione di un sistema StorageGRID".

Aggiungere nodi storage

È possibile aumentare la capacità dello storage aggiungendo nodi di storage. Quando si aggiunge lo storage, è necessario prendere in considerazione le regole ILM attualmente attive e i requisiti di capacità. Consultare le istruzioni per "Espansione di un sistema StorageGRID".

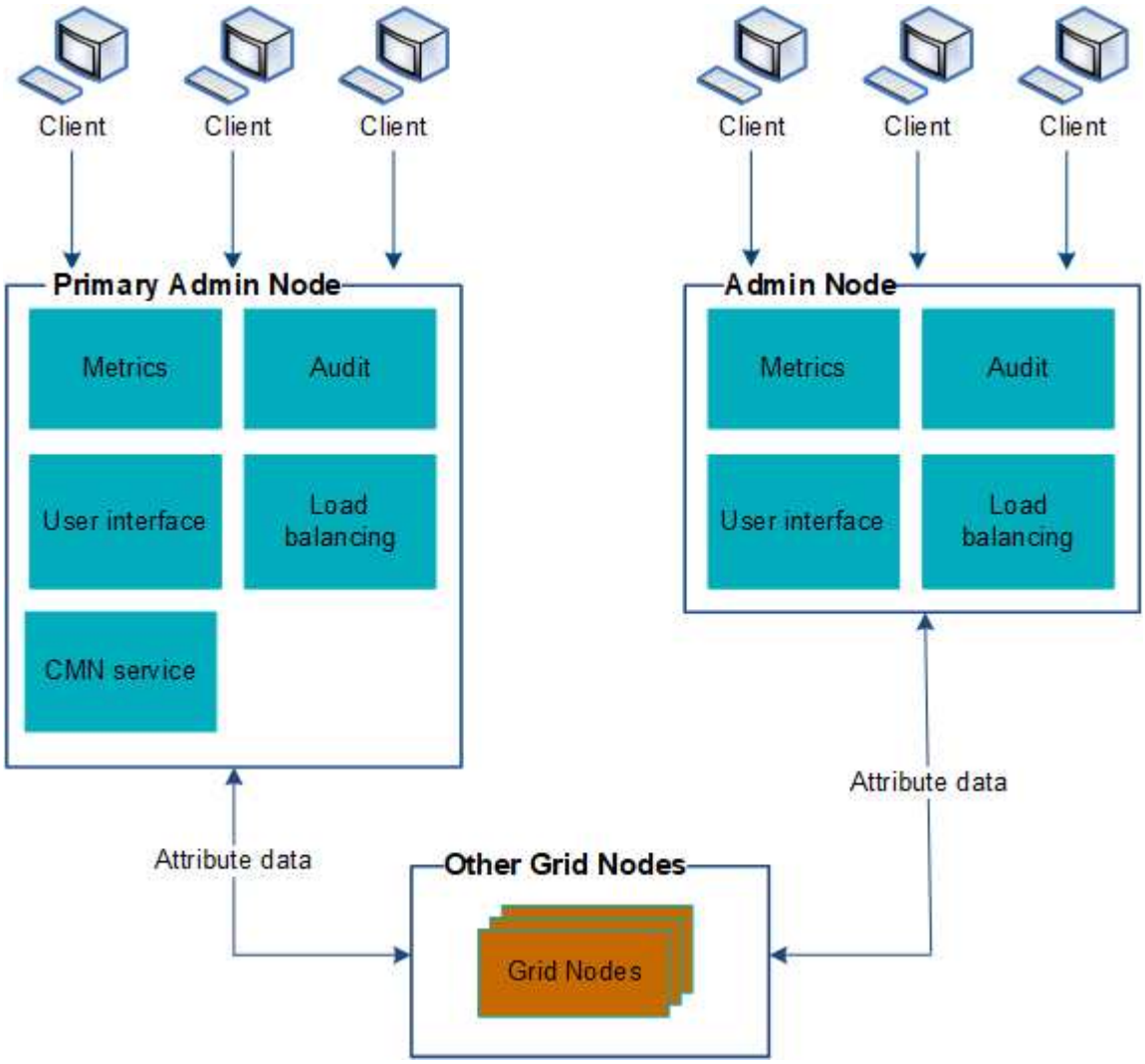
Gestire i nodi di amministrazione

Utilizzare più nodi di amministrazione

Un sistema StorageGRID può includere più nodi di amministrazione per consentire di monitorare e configurare continuamente il sistema StorageGRID anche in caso di guasto di un nodo di amministrazione.

Se un nodo amministrativo non è disponibile, l'elaborazione degli attributi continua, gli avvisi e gli allarmi (sistema legacy) vengono ancora attivati e le notifiche e-mail e i pacchetti AutoSupport vengono ancora inviati.

Tuttavia, la disponibilità di più nodi amministrativi non fornisce protezione dal failover, ad eccezione delle notifiche e dei pacchetti AutoSupport. In particolare, le conferme di allarme effettuate da un nodo di amministrazione non vengono copiate in altri nodi di amministrazione.



Sono disponibili due opzioni per continuare a visualizzare e configurare il sistema StorageGRID in caso di errore di un nodo di amministrazione:

- I client Web possono riconnettersi a qualsiasi altro nodo Admin disponibile.
- Se un amministratore di sistema ha configurato un gruppo di nodi di amministrazione ad alta disponibilità, i client Web possono continuare ad accedere a Grid Manager o a Tenant Manager utilizzando l'indirizzo IP virtuale del gruppo ha. Vedere "Gestire i gruppi ad alta disponibilità".

> Quando si utilizza un gruppo ha, l'accesso viene interrotto in caso di errore del nodo Admin attivo. Gli utenti devono effettuare nuovamente l'accesso dopo il failover dell'indirizzo IP virtuale del gruppo ha verso un altro nodo amministratore del gruppo.

Alcune attività di manutenzione possono essere eseguite solo utilizzando il nodo di amministrazione primario. In caso di guasto del nodo amministratore primario, è necessario ripristinarlo prima che il sistema StorageGRID funzioni nuovamente.

Identificare il nodo di amministrazione principale

Il nodo di amministrazione primario ospita il servizio CMN. Alcune procedure di manutenzione possono essere eseguite solo utilizzando il nodo di amministrazione primario.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > **Admin Node**, quindi scegliere ➕ Per espandere la struttura della topologia e mostrare i servizi ospitati su questo nodo di amministrazione.

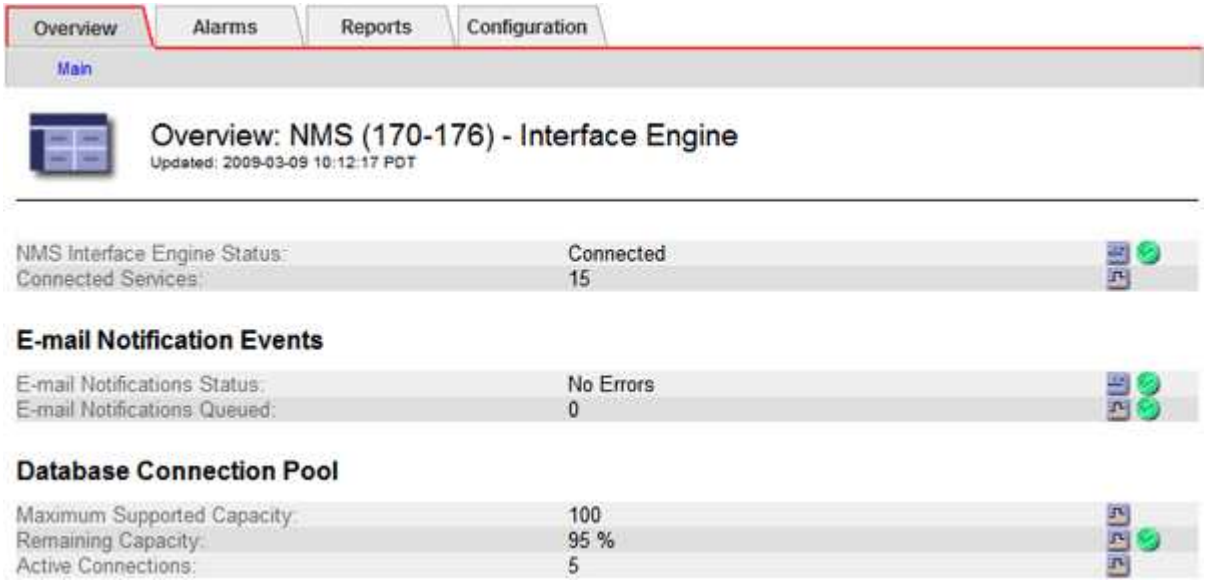
   Il nodo di amministrazione primario ospita il servizio CMN.

3. Se questo nodo di amministrazione non ospita il servizio CMN, controllare gli altri nodi di amministrazione.

Visualizzare lo stato delle notifiche e le code

Il servizio NMS (Network Management System) sui nodi di amministrazione invia notifiche al server di posta. È possibile visualizzare lo stato corrente del servizio NMS e le dimensioni della relativa coda di notifica nella pagina motore interfaccia.

Per accedere alla pagina Interface Engine, selezionare **SUPPORT** > **Tools** > **Grid topology**. Infine, selezionare ***Site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



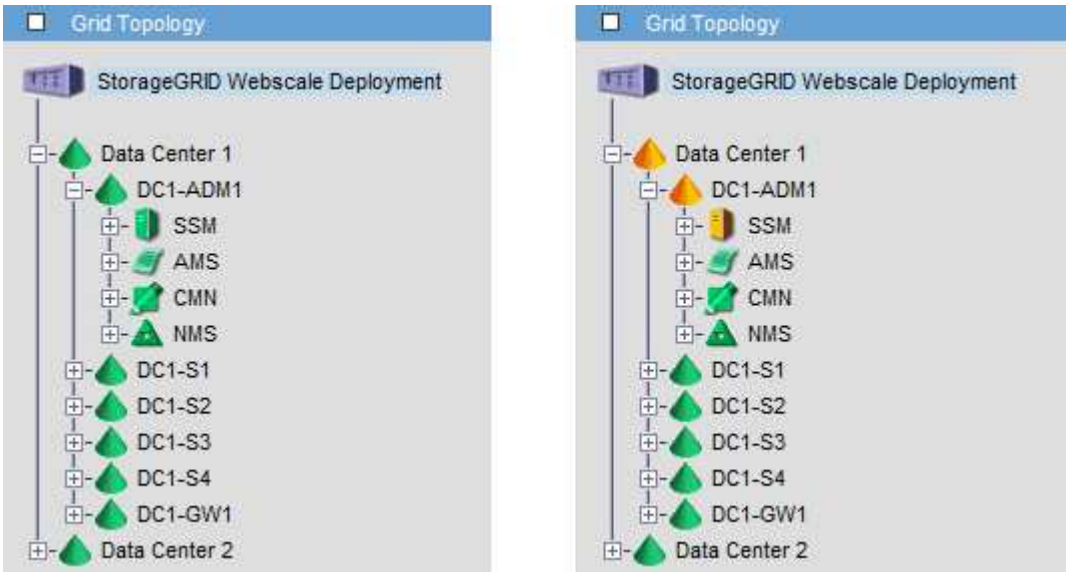
Le notifiche vengono elaborate tramite la coda di notifica e-mail e inviate al server di posta una dopo l'altra nell'ordine in cui vengono attivate. Se si verifica un problema (ad esempio, un errore di connessione di rete) e il server di posta non è disponibile quando si tenta di inviare la notifica, il tentativo più efficace di inviare nuovamente la notifica al server di posta continua per un periodo di 60 secondi. Se la notifica non viene inviata al server di posta dopo 60 secondi, la notifica viene interrotta dalla coda di notifica e viene eseguito un tentativo di invio della notifica successiva nella coda.

Poiché le notifiche possono essere interrotte dalla coda delle notifiche senza essere inviate, è possibile che un allarme possa essere attivato senza l'invio di una notifica. Se una notifica viene interrotta dalla coda senza essere inviata, viene attivato l'allarme minore MINUTI (Stato notifica e-mail).

Modalità di visualizzazione degli allarmi riconosciuti da Admin Node (sistema legacy)

Quando si riconosce un allarme su un nodo di amministrazione, l'allarme confermato non viene copiato in nessun altro nodo di amministrazione. Poiché i riconoscimenti non vengono copiati in altri nodi di amministrazione, l'albero topologia griglia potrebbe non avere lo stesso aspetto per ciascun nodo di amministrazione.

Questa differenza può essere utile quando si connettono client web. I client Web possono avere viste diverse del sistema StorageGRID in base alle esigenze dell'amministratore.



Si noti che le notifiche vengono inviate dal nodo di amministrazione in cui si verifica la conferma.

Configurare l'accesso al client di audit

Configurare l'accesso client di audit per NFS

Il nodo di amministrazione, tramite il servizio Audit Management System (AMS), registra tutti gli eventi di sistema controllati in un file di registro disponibile attraverso la condivisione dell'audit, che viene aggiunto a ciascun nodo di amministrazione al momento dell'installazione. La condivisione di controllo viene attivata automaticamente come condivisione di sola lettura.

> Il supporto per NFS è stato obsoleto e verrà rimosso in una versione futura.

Per accedere ai registri di audit, è possibile configurare l'accesso client per controllare le condivisioni per NFS. In alternativa, è possibile "utilizzare un server syslog esterno".

Il sistema StorageGRID utilizza il riconoscimento positivo per impedire la perdita dei messaggi di audit prima che vengano scritti nel file di log. Un messaggio rimane in coda in un servizio fino a quando il servizio AMS o un servizio di inoltro di audit intermedio non ne ha riconosciuto il controllo. Per ulteriori informazioni, vedere "Esaminare i registri di audit".

Prima di iniziare

- Hai il `Passwords.txt` file con la password root/admin.
- Hai il `Configuration.txt` File (disponibile nel pacchetto di ripristino).
- Il client di audit utilizza NFS versione 3 (NFSv3).

A proposito di questa attività

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato. Inserire: `storagegrid-status`

   Se alcuni servizi non sono elencati come in esecuzione o verificati, risolvere i problemi prima di continuare.
3. Tornare alla riga di comando. Premere **Ctrl+C**.
4. Avviare l'utility di configurazione NFS. Inserire: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

5. Aggiungere il client di audit: `add-audit-share`
   a. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: `client_IP_address`
   b. Quando richiesto, premere **Invio**.
6. Se più di un client di audit è autorizzato ad accedere alla condivisione di audit, aggiungere l'indirizzo IP dell'utente aggiuntivo: `add-ip-to-share`
   a. Inserire il numero della condivisione di controllo: *`audit_share_number`*
   b. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: *`client_IP_address`*

c. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione NFS.

d. Ripetere questi passaggi secondari per ogni client di audit aggiuntivo che ha accesso alla condivisione di audit.

7. Se si desidera, verificare la configurazione.

   a. Immettere quanto segue: `validate-config`

      I servizi vengono controllati e visualizzati.

   b. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione NFS.

   c. Chiudere l'utility di configurazione NFS: `exit`

8. Determinare se è necessario abilitare le condivisioni di audit in altri siti.
   - Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.
   - Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare queste condivisioni di controllo come richiesto:
     i. Accedere in remoto al nodo Admin del sito:
        A. Immettere il seguente comando: `ssh admin@grid_node_IP`
        B. Immettere la password elencata in `Passwords.txt` file.
        C. Immettere il seguente comando per passare a root: `su -`
        D. Immettere la password elencata in `Passwords.txt` file.
     ii. Ripetere questi passaggi per configurare le condivisioni di controllo per ogni nodo amministrativo aggiuntivo.
     iii. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto. Inserire: `exit`

9. Disconnettersi dalla shell dei comandi: `exit`

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. Concedere l'accesso alla condivisione di controllo a un nuovo client di audit NFS aggiungendo il proprio indirizzo IP alla condivisione oppure rimuovere un client di audit esistente rimuovendo il relativo indirizzo IP.

Aggiungere un client di audit NFS a una condivisione di audit

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. Concedere l'accesso alla condivisione di audit a un nuovo client di audit NFS aggiungendo il proprio indirizzo IP alla condivisione di audit.

Il supporto per NFS è stato obsoleto e verrà rimosso in una versione futura.

Prima di iniziare

- Hai il `Passwords.txt` file con la password dell'account root/admin.

- Hai il `Configuration.txt` File (disponibile nel pacchetto di ripristino).
- Il client di audit utilizza NFS versione 3 (NFSv3).

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Avviare l'utility di configurazione NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Inserire: `add-ip-to-share`

   Viene visualizzato un elenco di condivisioni di controllo NFS attivate nel nodo di amministrazione. La condivisione dell'audit è elencata come: `/var/local/log`

4. Inserire il numero della condivisione di controllo: *`audit_share_number`*
5. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: *`client_IP_address`*

   Il client di audit viene aggiunto alla condivisione di audit.

6. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione NFS.

7. Ripetere i passaggi per ogni client di audit da aggiungere alla condivisione di audit.
8. In alternativa, verificare la configurazione: `validate-config`

   I servizi vengono controllati e visualizzati.

   a. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione NFS.

9. Chiudere l'utility di configurazione NFS: `exit`
10. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

    In caso contrario, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, attivare facoltativamente queste condivisioni di controllo come richiesto:

    a. Accedere in remoto al nodo di amministrazione di un sito:
        i. Immettere il seguente comando: `ssh admin@grid_node_IP`
        ii. Immettere la password elencata in `Passwords.txt` file.
        iii. Immettere il seguente comando per passare a root: `su -`
        iv. Immettere la password elencata in `Passwords.txt` file.
    b. Ripetere questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
    c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`
11. Disconnettersi dalla shell dei comandi: `exit`

Verificare l'integrazione dell'audit NFS

Dopo aver configurato una condivisione di audit e aggiunto un client di audit NFS, è possibile montare la condivisione del client di audit e verificare che i file siano disponibili dalla condivisione di audit.

> Il supporto per NFS è stato obsoleto e verrà rimosso in una versione futura.

Fasi

1. Verificare la connettività (o la variante per il sistema client) utilizzando l'indirizzo IP lato client del nodo di amministrazione che ospita il servizio AMS. Inserire: `ping IP_address`

   Verificare che il server risponda, indicando la connettività.

2. Montare la condivisione di sola lettura dell'audit utilizzando un comando appropriato per il sistema operativo del client. Un esempio di comando Linux è (invio su una riga):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/log myAudit`

   Utilizzare l'indirizzo IP del nodo di amministrazione che ospita il servizio AMS e il nome di condivisione predefinito per il sistema di audit. Il punto di montaggio può essere qualsiasi nome selezionato dal client (ad esempio, *`myAudit`* nel comando precedente).

3. Verificare che i file siano disponibili dalla condivisione dell'audit. Inserire: `ls myAudit /*`

   dove *`myAudit`* è il punto di montaggio della condivisione dell'audit. Dovrebbe essere presente almeno un file di log.

Rimuovere un client di audit NFS dalla condivisione di audit

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al

proprio indirizzo IP. È possibile rimuovere un client di audit esistente rimuovendo il relativo indirizzo IP.

Prima di iniziare

- Hai il `Passwords.txt` file con la password dell'account root/admin.
- Hai il `Configuration.txt` File (disponibile nel pacchetto di ripristino).

A proposito di questa attività

Non è possibile rimuovere l'ultimo indirizzo IP consentito per accedere alla condivisione dell'audit.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Avviare l'utility di configurazione NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Rimuovere l'indirizzo IP dalla condivisione dell'audit: `remove-ip-from-share`

   Viene visualizzato un elenco numerato di condivisioni di controllo configurate sul server. La condivisione dell'audit è elencata come: `/var/local/log`

4. Inserire il numero corrispondente alla condivisione di audit: *`audit_share_number`*

   Viene visualizzato un elenco numerato di indirizzi IP autorizzati ad accedere alla condivisione dell'audit.

5. Inserire il numero corrispondente all'indirizzo IP che si desidera rimuovere.

   La condivisione di audit viene aggiornata e l'accesso non è più consentito da alcun client di audit con questo indirizzo IP.

6. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione NFS.

7. Chiudere l'utility di configurazione NFS: `exit`
8. Se l'implementazione di StorageGRID è un'implementazione di più siti di data center con nodi amministrativi aggiuntivi negli altri siti, disattivare queste condivisioni di controllo secondo necessità:
   a. Accedere in remoto al nodo di amministrazione di ciascun sito:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file.
   b. Ripetere questi passaggi per configurare le condivisioni di controllo per ogni nodo amministrativo aggiuntivo.
   c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`
9. Disconnettersi dalla shell dei comandi: `exit`

Modificare l'indirizzo IP di un client di audit NFS

Se si desidera modificare l'indirizzo IP di un client di audit NFS, attenersi alla procedura descritta di seguito.

Fasi

1. Aggiungere un nuovo indirizzo IP a una condivisione di audit NFS esistente.
2. Rimuovere l'indirizzo IP originale.

Informazioni correlate

- "Aggiungere un client di audit NFS a una condivisione di audit"
- "Rimuovere un client di audit NFS dalla condivisione di audit"

Gestire i nodi di archiviazione

Archiviazione nel cloud tramite l'API S3

È possibile configurare un nodo di archiviazione per la connessione diretta ai servizi Web Amazon o a qualsiasi altro sistema in grado di interfacciarsi con il sistema StorageGRID tramite l'API S3.

> Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura. Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità.
>
> Anche l'opzione Cloud Tiering - Simple Storage Service (S3) è obsoleta. Se si utilizza attualmente un nodo di archiviazione con questa opzione, "Migrare gli oggetti in un pool di storage cloud" invece.
>
> Inoltre, è necessario rimuovere i nodi di archiviazione dal criterio ILM attivo in StorageGRID 11,7 o versioni precedenti. La rimozione dei dati degli oggetti memorizzati nei nodi di archiviazione semplificherà gli aggiornamenti futuri. Vedere "Utilizzo delle regole ILM e delle policy ILM".

Configurare le impostazioni di connessione per l'API S3

Se si sta effettuando la connessione a un nodo di archiviazione utilizzando l'interfaccia S3, è necessario configurare le impostazioni di connessione per l'API S3. Fino a quando queste impostazioni non vengono configurate, il servizio ARC rimane in uno stato di allarme principale in quanto non è in grado di comunicare con il sistema di storage di archiviazione esterno.

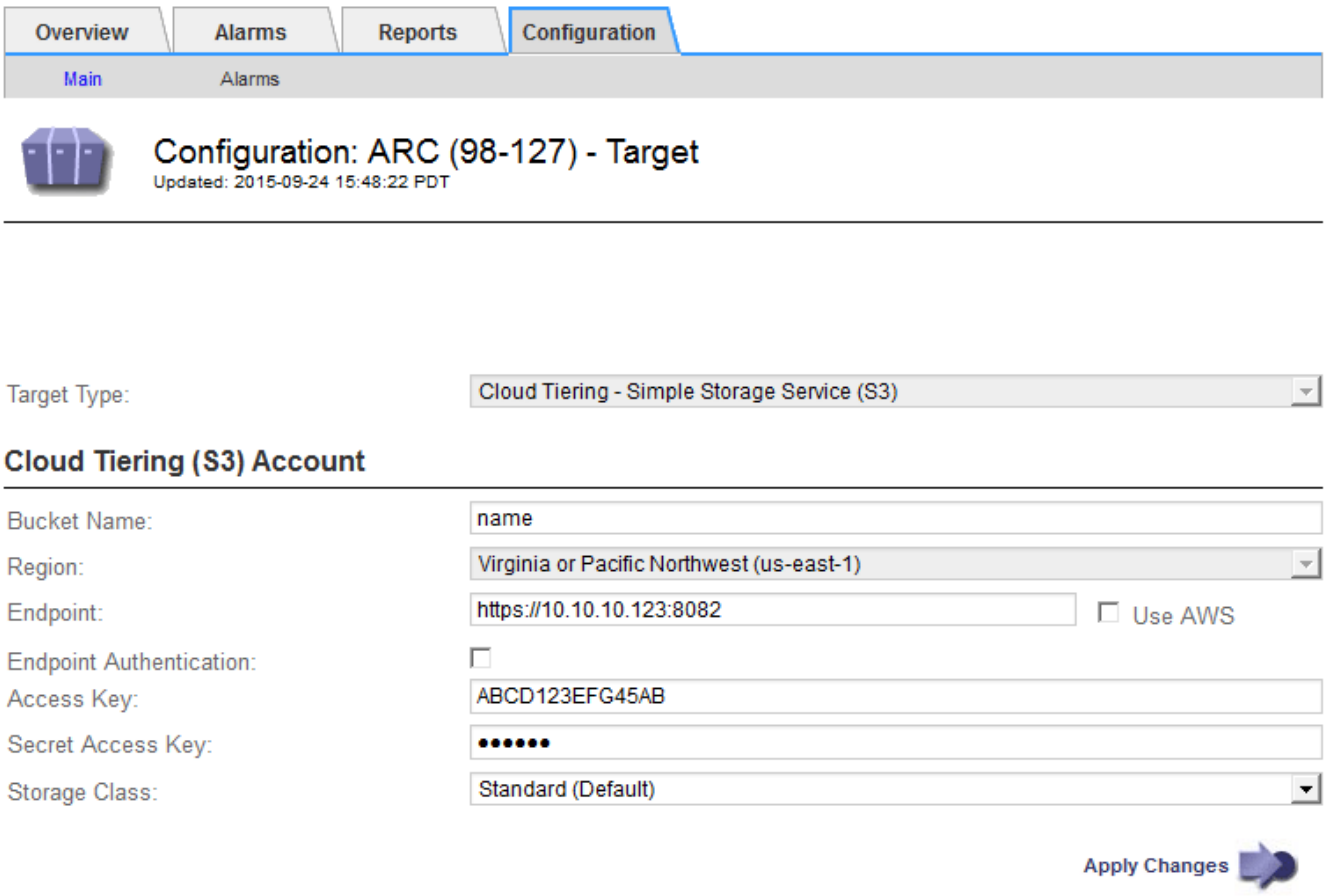
> Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura. Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità.
>
> Anche l'opzione Cloud Tiering - Simple Storage Service (S3) è obsoleta. Se si utilizza attualmente un nodo di archiviazione con questa opzione, "Migrare gli oggetti in un pool di storage cloud" invece.
>
> Inoltre, è necessario rimuovere i nodi di archiviazione dal criterio ILM attivo in StorageGRID 11,7 o versioni precedenti. La rimozione dei dati degli oggetti memorizzati nei nodi di archiviazione semplificherà gli aggiornamenti futuri. Vedere "Utilizzo delle regole ILM e delle policy ILM".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai creato un bucket sul sistema storage di archiviazione di destinazione:
  - Il bucket è dedicato a un singolo nodo di archiviazione. Non può essere utilizzato da altri nodi di archiviazione o altre applicazioni.
  - Nel bucket è stata selezionata la regione appropriata per la propria posizione.
  - Il bucket deve essere configurato con la versione sospesa.
- La segmentazione degli oggetti è attivata e la dimensione massima dei segmenti è inferiore o uguale a 4.5 GiB (4,831,838,208 byte). Le richieste API S3 che superano questo valore non avranno esito positivo se S3 viene utilizzato come sistema di storage di archiviazione esterno.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare **Archive Node** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.



4. Selezionare **Cloud Tiering - Simple Storage Service (S3)** dall'elenco a discesa Target Type (tipo di destinazione).

> Le impostazioni di configurazione non sono disponibili fino a quando non si seleziona un tipo di destinazione.

5. Configurare l'account di cloud tiering (S3) attraverso il quale il nodo di archiviazione si connetterà al sistema di archiviazione esterno di destinazione in grado di supportare S3.

   La maggior parte dei campi di questa pagina sono esplicativi. Di seguito vengono descritti i campi per i quali potrebbe essere necessario fornire assistenza.

   - **Regione**: Disponibile solo se è selezionato **Usa AWS**. La regione selezionata deve corrispondere a quella del bucket.
   - **Endpoint** e **Use AWS**: Per Amazon Web Services (AWS), selezionare **Use AWS**. **Endpoint** viene quindi compilato automaticamente con un URL dell'endpoint in base agli attributi Bucket Name e Region. Ad esempio:

     ```
     https://bucket.region.amazonaws.com
     ```

     Per una destinazione non AWS, inserire l'URL del sistema che ospita il bucket, incluso il numero di porta. Ad esempio:

```
https://system.com:1080
```

   - **End Point Authentication**: Attivato per impostazione predefinita. Se la rete verso il sistema di storage di archiviazione esterno è attendibile, deselezionare la casella di controllo per disattivare la verifica del

certificato SSL dell'endpoint e del nome host per il sistema di storage di archiviazione esterno di destinazione. Se un'altra istanza di un sistema StorageGRID è il dispositivo di archiviazione di destinazione e il sistema è configurato con certificati firmati pubblicamente, è possibile mantenere la casella di controllo selezionata.

- **Storage Class** (Classe di storage): Selezionare **Standard (predefinito)** per lo storage normale. Selezionare **Redundancy ridotta** solo per gli oggetti che possono essere ricreati facilmente. **Redundancy ridotta** offre storage a costi inferiori con minore affidabilità. Se il sistema storage di archiviazione di destinazione è un'altra istanza del sistema StorageGRID, **Classe storage** controlla quante copie intermedie dell'oggetto vengono eseguite al momento dell'acquisizione nel sistema di destinazione, se viene utilizzato il doppio commit quando vengono acquisiti oggetti.

6. Selezionare **Applica modifiche**.

   Le impostazioni di configurazione specificate vengono validate e applicate al sistema StorageGRID. Una volta applicate le impostazioni, il target non può essere modificato.

Modificare le impostazioni di connessione per l'API S3

Una volta configurato il nodo di archiviazione per la connessione a un sistema di archiviazione esterno tramite l'API S3, è possibile modificare alcune impostazioni in caso di modifica della connessione.

Prima di iniziare

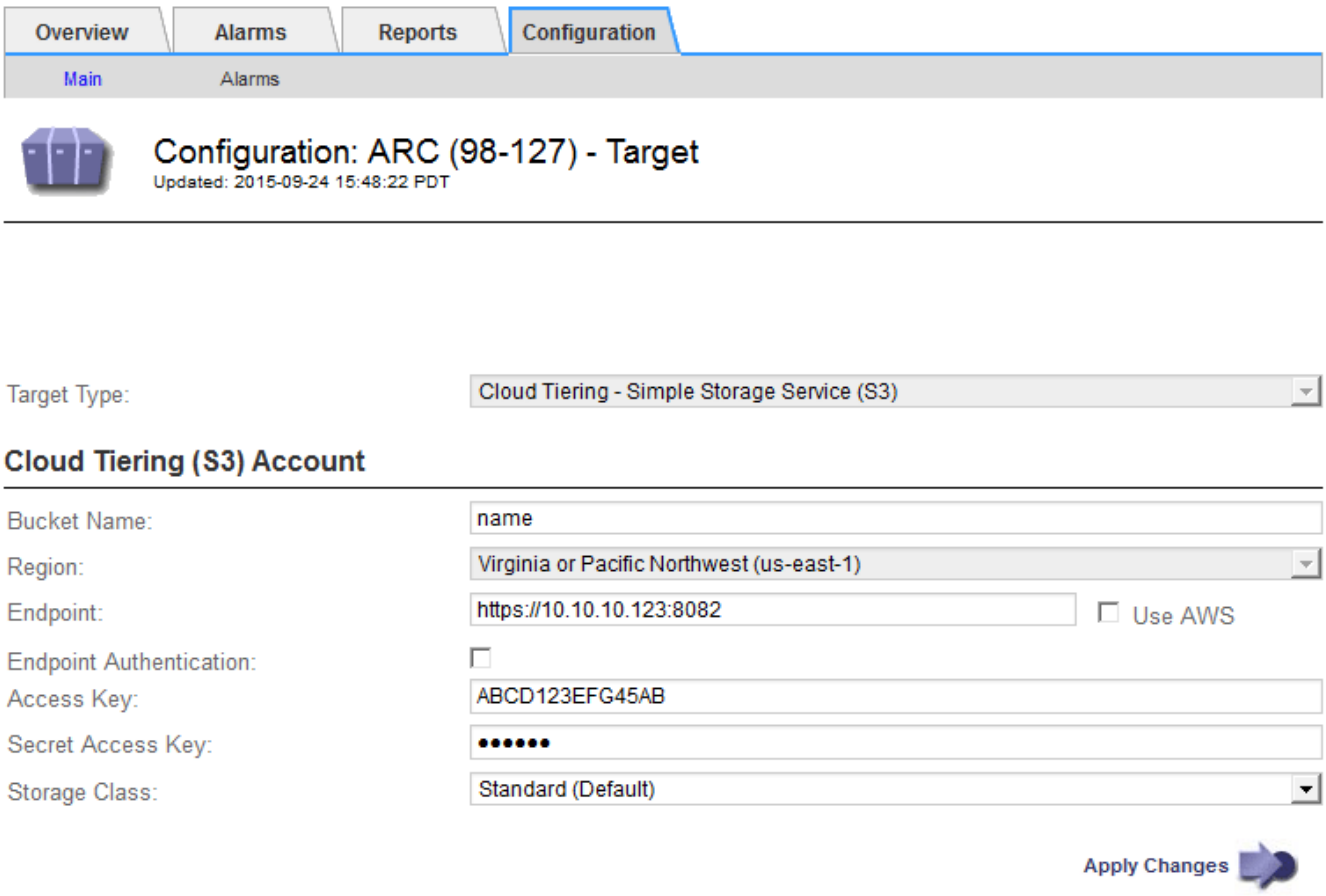
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Se si modifica l'account Cloud Tiering (S3), è necessario assicurarsi che le credenziali di accesso dell'utente abbiano accesso in lettura/scrittura al bucket, inclusi tutti gli oggetti precedentemente acquisiti dal nodo di archiviazione nel bucket.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare le informazioni dell'account, se necessario.

   Se si modifica la classe di storage, i nuovi dati dell'oggetto vengono memorizzati con la nuova classe di storage. L'oggetto esistente continua ad essere memorizzato nella classe di storage impostata al momento dell'acquisizione.

   Nome bucket, regione ed endpoint, utilizza i valori AWS e non può essere modificato.

5. Selezionare **Applica modifiche**.

Modificare lo stato del Cloud Tiering Service

È possibile controllare la capacità di lettura e scrittura del nodo di archiviazione nel sistema storage di archiviazione esterno di destinazione che si connette attraverso l'API S3 modificando lo stato del servizio di tiering cloud.

Prima di iniziare

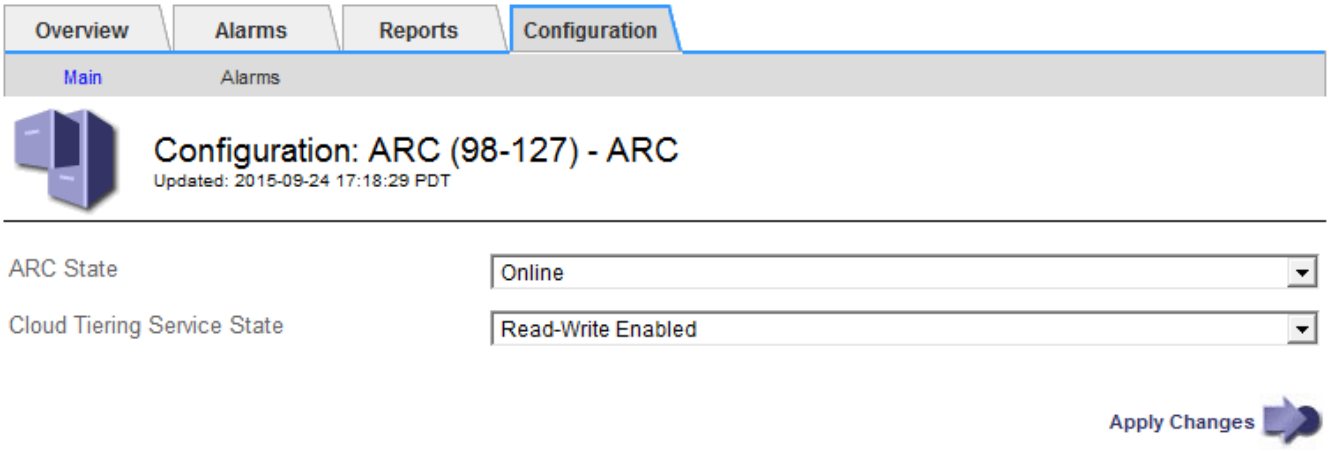
- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Il nodo di archiviazione deve essere configurato.

A proposito di questa attività

È possibile disattivare il nodo di archiviazione modificando lo stato del servizio di tiering cloud in **Read-Write Disabled**.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC**.
3. Selezionare **Configurazione** > **principale**.



4. Selezionare un **Cloud Tiering Service state**.
5. Selezionare **Applica modifiche**.

Ripristinare il numero di errori di archiviazione per la connessione API S3

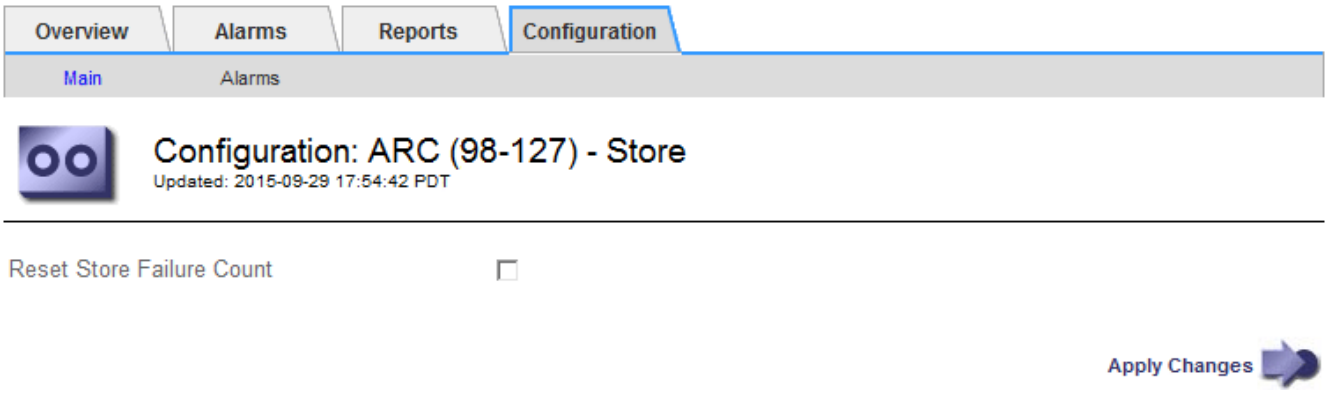
Se il nodo di archiviazione si connette a un sistema di storage di archiviazione tramite l'API S3, è possibile reimpostare il numero di errori di archiviazione, che può essere utilizzato per cancellare l'allarme ARVF (Store Failures).

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Store**.
3. Selezionare **Configurazione** > **principale**.



4. Selezionare **Reset Store Failure Count**.

5. Selezionare **Applica modifiche**.

   L'attributo Store Failures viene reimpostato su zero.

Migrazione di oggetti da Cloud Tiering - S3 a un Cloud Storage Pool

Se attualmente si utilizza la funzionalità **Cloud Tiering - Simple Storage Service (S3)** per tierare i dati degli oggetti in un bucket S3, è necessario migrare gli oggetti in un Cloud Storage Pool. I pool di cloud storage offrono un approccio scalabile che sfrutta tutti i nodi di storage nel sistema StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai già memorizzato oggetti nel bucket S3 configurato per il Cloud Tiering.

> Prima di migrare i dati degli oggetti, contatta il tuo rappresentante NetApp per conoscere e gestire i costi associati.

A proposito di questa attività

Dal punto di vista di ILM, un pool di storage cloud è simile a un pool di storage. Tuttavia, mentre i pool di storage sono costituiti da nodi di storage o nodi di archiviazione all'interno del sistema StorageGRID, un pool di storage cloud è costituito da un bucket S3 esterno.

Prima di migrare gli oggetti da Tier cloud - S3 a un pool di storage cloud, è necessario prima creare un bucket S3 e poi creare il pool di storage cloud in StorageGRID. Quindi, è possibile creare un nuovo criterio ILM e sostituire la regola ILM utilizzata per memorizzare gli oggetti nel bucket Cloud Tiering con una regola ILM clonata che memorizza gli stessi oggetti nel Cloud Storage Pool.

> Quando gli oggetti vengono memorizzati in un pool di storage cloud, le copie di tali oggetti non possono essere memorizzate anche in StorageGRID. Se la regola ILM attualmente in uso per il Cloud Tiering è configurata per memorizzare oggetti in più posizioni contemporaneamente, considerare se si desidera eseguire questa migrazione facoltativa perché si perde tale funzionalità. Se si continua con questa migrazione, è necessario creare nuove regole invece di clonare quelle esistenti.

Fasi

1. Creare un pool di storage cloud.

   Utilizza un nuovo bucket S3 per il Cloud Storage Pool per garantire che contenga solo i dati gestiti dal Cloud Storage Pool.

2. Individuare eventuali regole ILM nelle policy ILM attive che causano l'archiviazione degli oggetti nel bucket Cloud Tiering.
3. Clonare ciascuna di queste regole.
4. Nelle regole clonate, modificare la posizione di posizionamento nel nuovo Cloud Storage Pool.
5. Salvare le regole clonate.
6. Creare una nuova policy che utilizzi le nuove regole.

7. Simulare e attivare la nuova policy.

   Quando la nuova policy viene attivata e si verifica la valutazione ILM, gli oggetti vengono spostati dal bucket S3 configurato per il Cloud Tiering al bucket S3 configurato per il Cloud Storage Pool. Lo spazio utilizzabile sulla griglia non viene compromesso. Una volta spostati nel Cloud Storage Pool, gli oggetti vengono rimossi dal bucket Cloud Tiering.

Informazioni correlate

"Gestire gli oggetti con ILM"

Archiviazione su nastro tramite middleware TSM

È possibile configurare un nodo di archiviazione in modo che utilizzi un server Tivoli Storage Manager (TSM) che fornisce un'interfaccia logica per l'archiviazione e il recupero dei dati degli oggetti su dispositivi di storage ad accesso casuale o sequenziale, incluse le librerie su nastro.

Il servizio ARC del nodo di archiviazione agisce come client per il server TSM, utilizzando Tivoli Storage Manager come middleware per la comunicazione con il sistema di storage di archiviazione.

> Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura. Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità.
>
> Anche l'opzione Cloud Tiering - Simple Storage Service (S3) è obsoleta. Se si utilizza attualmente un nodo di archiviazione con questa opzione, "Migrare gli oggetti in un pool di storage cloud" invece.
>
> Inoltre, è necessario rimuovere i nodi di archiviazione dal criterio ILM attivo in StorageGRID 11,7 o versioni precedenti. La rimozione dei dati degli oggetti memorizzati nei nodi di archiviazione semplificherà gli aggiornamenti futuri. Vedere "Utilizzo delle regole ILM e delle policy ILM".

Classi di gestione TSM

Le classi di gestione definite dal middleware TSM delineano il funzionamento delle operazioni di backup e archiviazione di TSM's e possono essere utilizzate per specificare le regole per il contenuto che vengono applicate dal server TSM. Tali regole funzionano indipendentemente dalla policy ILM del sistema StorageGRID e devono essere coerenti con il requisito del sistema StorageGRID che gli oggetti siano memorizzati in modo permanente e siano sempre disponibili per il recupero da parte del nodo di archiviazione. Dopo che i dati dell'oggetto sono stati inviati a un server TSM dal nodo di archiviazione, il ciclo di vita del TSM e le regole di conservazione vengono applicati mentre i dati dell'oggetto vengono memorizzati sul nastro gestito dal server TSM.

La classe di gestione TSM viene utilizzata dal server TSM per applicare regole per la posizione o la conservazione dei dati dopo che gli oggetti sono stati inviati al server TSM dal nodo di archiviazione. Ad esempio, gli oggetti identificati come backup del database (contenuto temporaneo che può essere sovrascritto con dati più recenti) potrebbero essere trattati in modo diverso rispetto ai dati dell'applicazione (contenuto fisso che deve essere conservato a tempo indeterminato).

Prima che il nodo di archiviazione possa comunicare con il middleware Tivoli Storage Manager (TSM), è necessario configurare diverse impostazioni.

Prima di iniziare

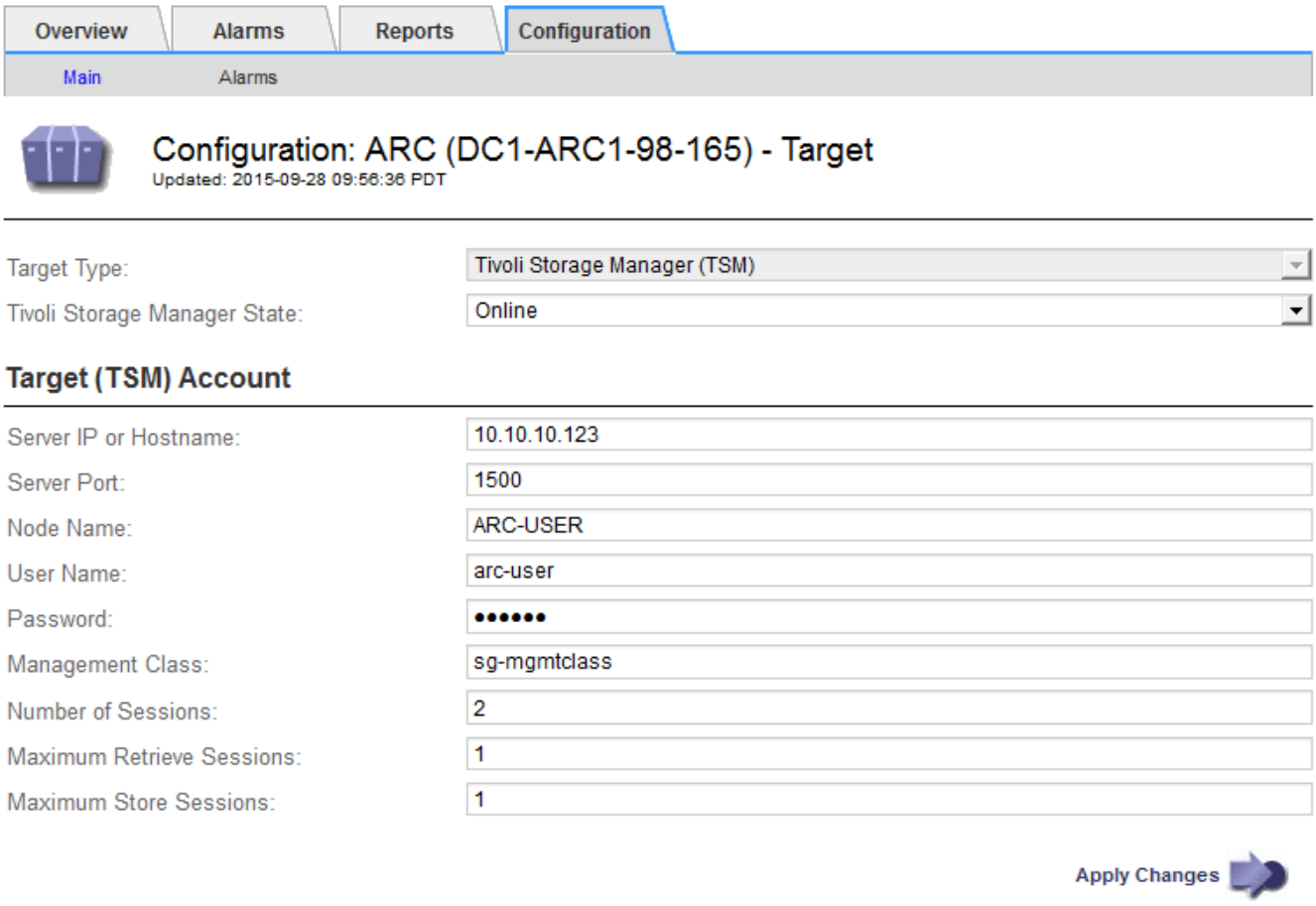
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Fino a quando queste impostazioni non vengono configurate, il servizio ARC rimane in uno stato di allarme principale in quanto non è in grado di comunicare con Tivoli Storage Manager.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.



4. Dall'elenco a discesa **Target Type** (tipo di destinazione), selezionare **Tivoli Storage Manager (TSM)**.
5. Per lo stato di **Tivoli Storage Manager**, selezionare **Offline** per impedire il recupero dal server middleware TSM.

   Per impostazione predefinita, lo stato di Tivoli Storage Manager è impostato su Online, il che significa che il nodo di archiviazione è in grado di recuperare i dati degli oggetti dal server middleware TSM.

6. Completare le seguenti informazioni:

   - **Server IP (IP server) o Hostname (Nome host)**: Specificare l'indirizzo IP o il nome di dominio completo del server middleware TSM utilizzato dal servizio ARC. L'indirizzo IP predefinito è 127.0.0.1.
   - **Server Port** (porta server): Specificare il numero di porta sul server middleware TSM a cui si connetterà il servizio ARC. Il valore predefinito è 1500.
   - **Node Name** (Nome nodo): Specificare il nome del nodo di archiviazione. Immettere il nome (arco -utente) registrato sul server middleware TSM.
   - **User Name** (Nome utente): Specificare il nome utente utilizzato dal servizio ARC per accedere al server TSM. Immettere il nome utente predefinito (Arc-user) o l'utente amministrativo specificato per il nodo di archiviazione.
   - **Password**: Specificare la password utilizzata dal servizio ARC per accedere al server TSM.
   - **Classe di gestione**: Specificare la classe di gestione predefinita da utilizzare se non viene specificata una classe di gestione quando l'oggetto viene salvato nel sistema StorageGRID o se la classe di gestione specificata non viene definita nel server middleware TSM.
   - **Numero di sessioni**: Specificare il numero di unità nastro sul server middleware TSM dedicate al nodo di archiviazione. Il nodo di archiviazione crea contemporaneamente un massimo di una sessione per punto di montaggio più un piccolo numero di sessioni aggiuntive (meno di cinque).

     È necessario modificare questo valore in modo che sia uguale al valore impostato per MAXNUMMP (numero massimo di punti di montaggio) quando il nodo di archiviazione è stato registrato o aggiornato. (Nel comando register, il valore predefinito di MAXNUMMP utilizzato è 1, se non viene impostato alcun valore).

   È inoltre necessario modificare il valore di MAXSESSIONS per il server TSM con un numero pari almeno al numero di sessioni impostato per il servizio ARC. Il valore predefinito di MAXSESSIONS sul server TSM è 25.

   - **Numero massimo di sessioni di recupero**: Specificare il numero massimo di sessioni che il servizio ARC può aprire al server middleware TSM per le operazioni di recupero. Nella maggior parte dei casi, il valore appropriato è numero di sessioni meno numero massimo di sessioni del negozio. Se è necessario condividere un'unità a nastro per lo storage e il recupero, specificare un valore uguale al numero di sessioni.
   - **Numero massimo di sessioni di archiviazione**: Specificare il numero massimo di sessioni simultanee che il servizio ARC può aprire al server middleware TSM per le operazioni di archiviazione.

     Questo valore deve essere impostato su uno, tranne quando il sistema storage di archiviazione di destinazione è pieno e possono essere eseguiti solo i recuperi. Impostare questo valore su zero per utilizzare tutte le sessioni per i recuperi.

7. Selezionare **Applica modifiche**.

Ottimizza un nodo di archiviazione per sessioni middleware TSM

È possibile ottimizzare le prestazioni di un nodo di archiviazione che si connette a Tivoli Server Manager (TSM) configurando le sessioni del nodo di archiviazione.

Prima di iniziare

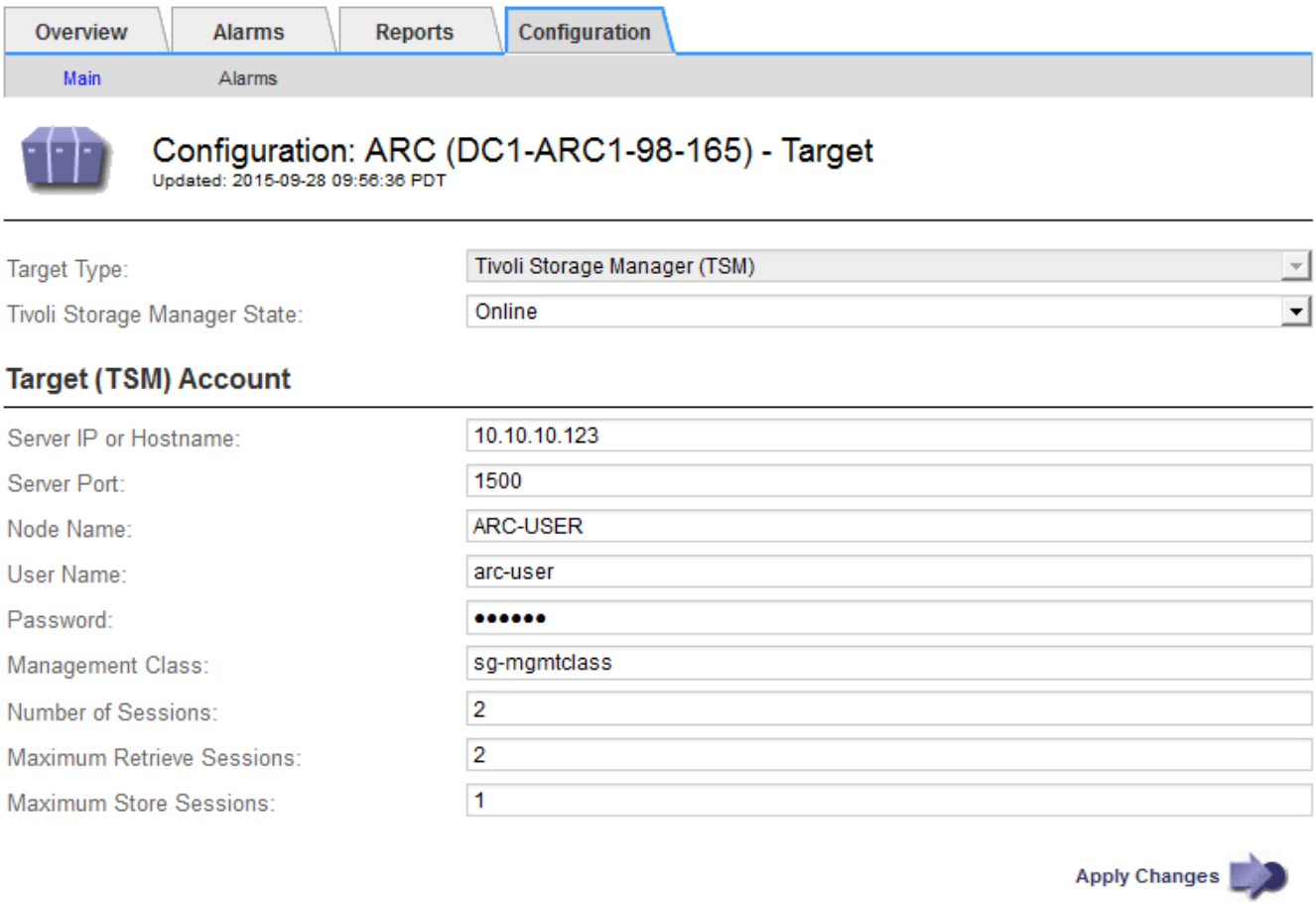
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

In genere, il numero di sessioni simultanee che il nodo di archiviazione ha aperto al server middleware TSM viene impostato sul numero di unità a nastro dedicate dal server TSM al nodo di archiviazione. Un'unità a nastro viene allocata per lo storage, mentre le altre vengono allocate per il recupero. Tuttavia, nelle situazioni in cui un nodo di storage viene ricostruito dalle copie del nodo di archivio o il nodo di archivio opera in modalità di sola lettura, è possibile ottimizzare le prestazioni del server TSM impostando il numero massimo di sessioni di recupero sullo stesso numero di sessioni simultanee. Il risultato è che tutti i dischi possono essere utilizzati contemporaneamente per il recupero e, al massimo, uno di questi dischi può essere utilizzato anche per lo storage, se applicabile.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.
4. Modificare **numero massimo di sessioni di recupero** in modo che sia uguale a **numero di sessioni**.



5. Selezionare **Applica modifiche**.

Configurare lo stato di archiviazione e i contatori per TSM

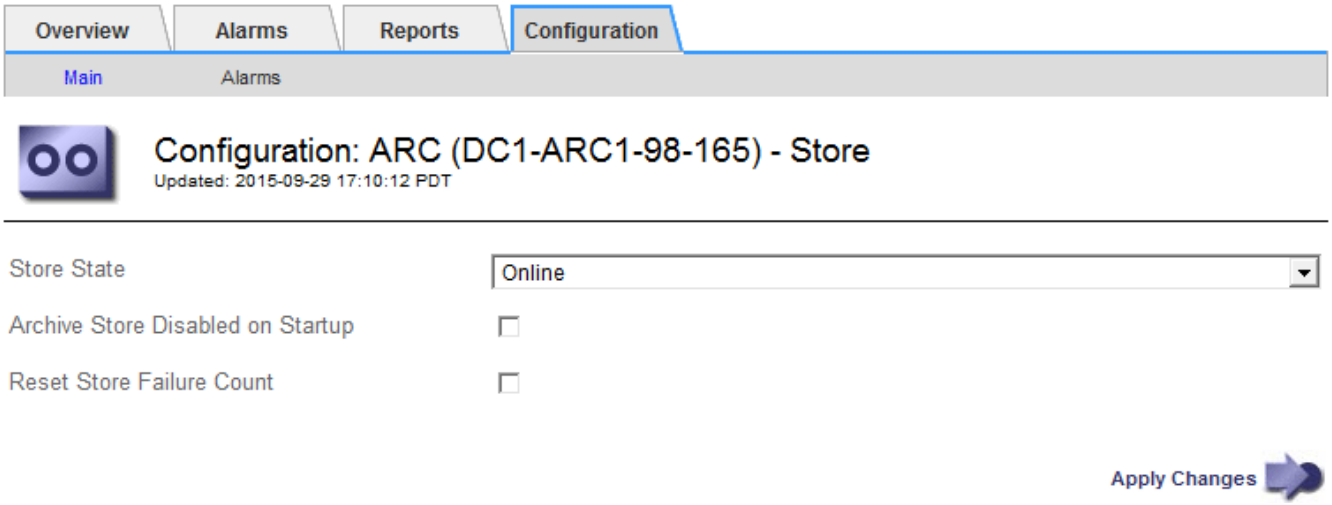
Se il nodo di archiviazione si connette a un server middleware TSM, è possibile configurare lo stato dell'archivio di un nodo di archiviazione su Online o Offline. È inoltre possibile disattivare l'archivio al primo avvio del nodo di archiviazione o ripristinare il conteggio degli errori rilevati per l'allarme associato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Store**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare le seguenti impostazioni, se necessario:
   - Store state (Stato di archiviazione): Impostare lo stato del componente su:
     - Online: Il nodo di archiviazione è disponibile per elaborare i dati a oggetti per lo storage nel sistema di storage di archiviazione.
     - Offline: Il nodo di archiviazione non è disponibile per elaborare i dati degli oggetti per lo storage nel sistema di storage di archiviazione.
   - Archivia archivio disattivata all'avvio: Se selezionato, il componente Archivia archivio rimane nello stato di sola lettura al riavvio. Utilizzato per disattivare in modo persistente lo storage nel sistema di storage di archiviazione di destinazione. Utile quando il sistema storage di archiviazione di destinazione non è in grado di accettare contenuti.
   - Reset Store Failure Count (Ripristina numero di guasti del punto vendita): Consente di reimpostare il contatore per gli errori Questa opzione può essere utilizzata per cancellare l'allarme ARVF (Memorizza guasto).
5. Selezionare **Applica modifiche**.

Informazioni correlate

"Gestire un nodo di archiviazione quando il server TSM raggiunge la capacità"

Gestire un nodo di archiviazione quando il server TSM raggiunge la capacità

Il server TSM non ha modo di notificare al nodo di archiviazione quando il database TSM o lo storage dei supporti di archiviazione gestito dal server TSM si avvicina alla capacità. Questa situazione può essere evitata attraverso il monitoraggio proattivo del server TSM.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

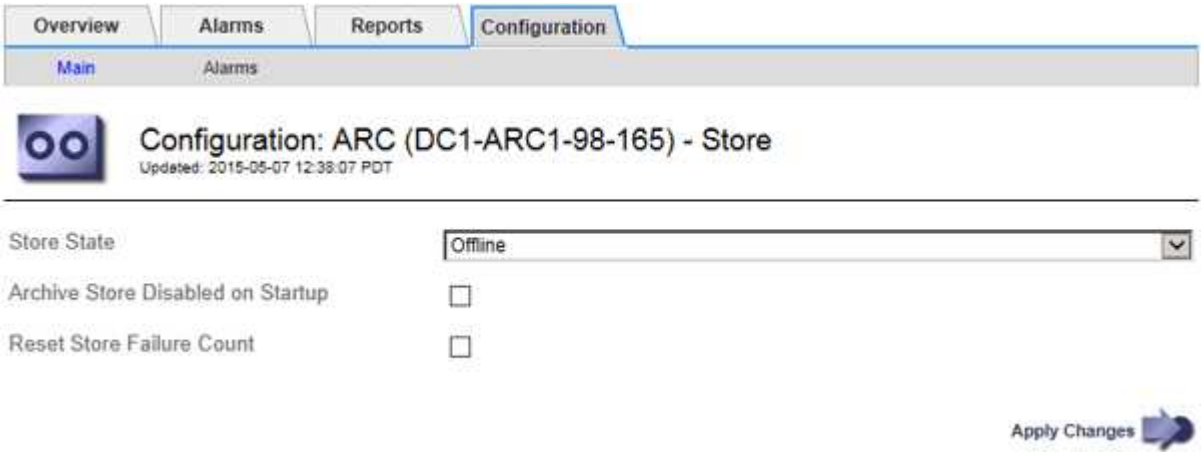
Il nodo di archiviazione continua ad accettare i dati dell'oggetto per il trasferimento al server TSM dopo che il server TSM ha interrotto l'accettazione del nuovo contenuto. Questo contenuto non può essere scritto su supporti gestiti dal server TSM. In questo caso, viene attivato un allarme.

Impedire al servizio ARC di inviare contenuto al server TSM

Per impedire al servizio ARC di inviare ulteriore contenuto al server TSM, è possibile disattivare il nodo di archiviazione portando il componente **ARC** > **Store** offline. Questa procedura può essere utile anche per prevenire gli allarmi quando il server TSM non è disponibile per la manutenzione.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Store**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare **Store state** in `Offline`.
5. Selezionare **Archivia archivio disabilitata all'avvio**.
6. Selezionare **Applica modifiche**.

Impostare Archive Node su Read-only se il middleware TSM raggiunge la capacità

Se il server middleware TSM di destinazione raggiunge la capacità, il nodo di archiviazione può essere ottimizzato per eseguire solo i recuperi.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.
4. Impostare il numero massimo di sessioni di recupero in modo che sia uguale al numero di sessioni simultanee elencate in numero di sessioni.
5. Impostare il numero massimo di sessioni di memorizzazione su 0.

Se il nodo di archiviazione è di sola lettura, non è necessario modificare il numero massimo di sessioni di archiviazione su 0. Le sessioni del negozio non verranno create.

6. Selezionare **Applica modifiche**.

Configurare le impostazioni di recupero del nodo di archiviazione

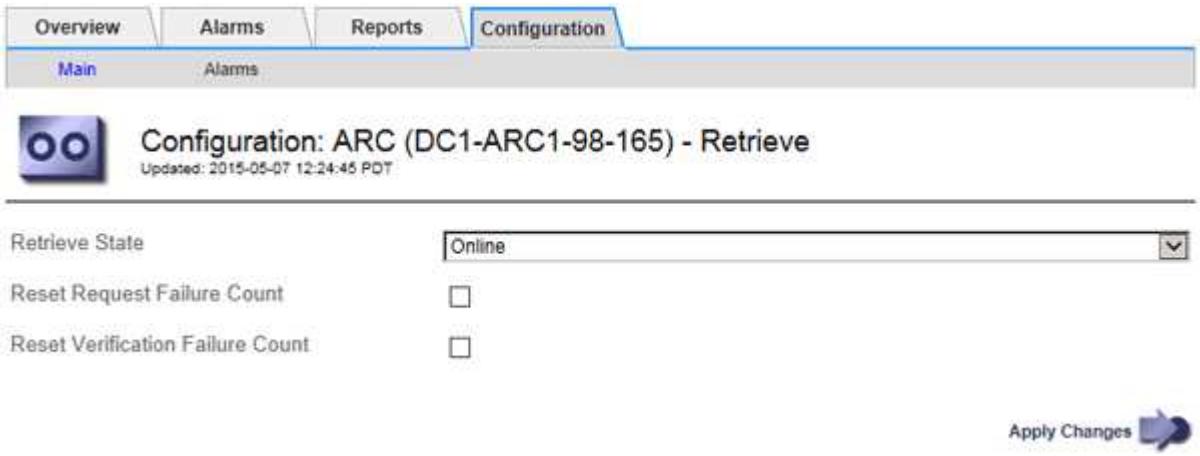
È possibile configurare le impostazioni di recupero per un nodo di archiviazione per impostare lo stato su Online o Offline, oppure reimpostare i conteggi degli errori rilevati per gli allarmi associati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare **nodo archivio** > **ARC** > **Recupera**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare le seguenti impostazioni, se necessario:
   - **Stato di recupero**: Impostare lo stato del componente su:
     - Online: Il nodo Grid è disponibile per recuperare i dati degli oggetti dal dispositivo di archiviazione.
     - Offline: Il nodo Grid non è disponibile per recuperare i dati dell'oggetto.
   - Reset Request Failures Count (Ripristina numero di errori richiesta): Selezionare la casella di controllo per azzerare il contatore dei guasti richiesta. Questa opzione può essere utilizzata per cancellare l'allarme ARRF (Request Failures).
   - Reset Verification Failure Count (Ripristina conteggio errori di verifica): Selezionare la casella di controllo per ripristinare il contatore per gli errori di verifica sui dati dell'oggetto recuperati. Questa opzione può essere utilizzata per cancellare l'allarme ARRV (Verification Failures) (errori di verifica).
5. Selezionare **Applica modifiche**.

Configurare la replica del nodo di archiviazione

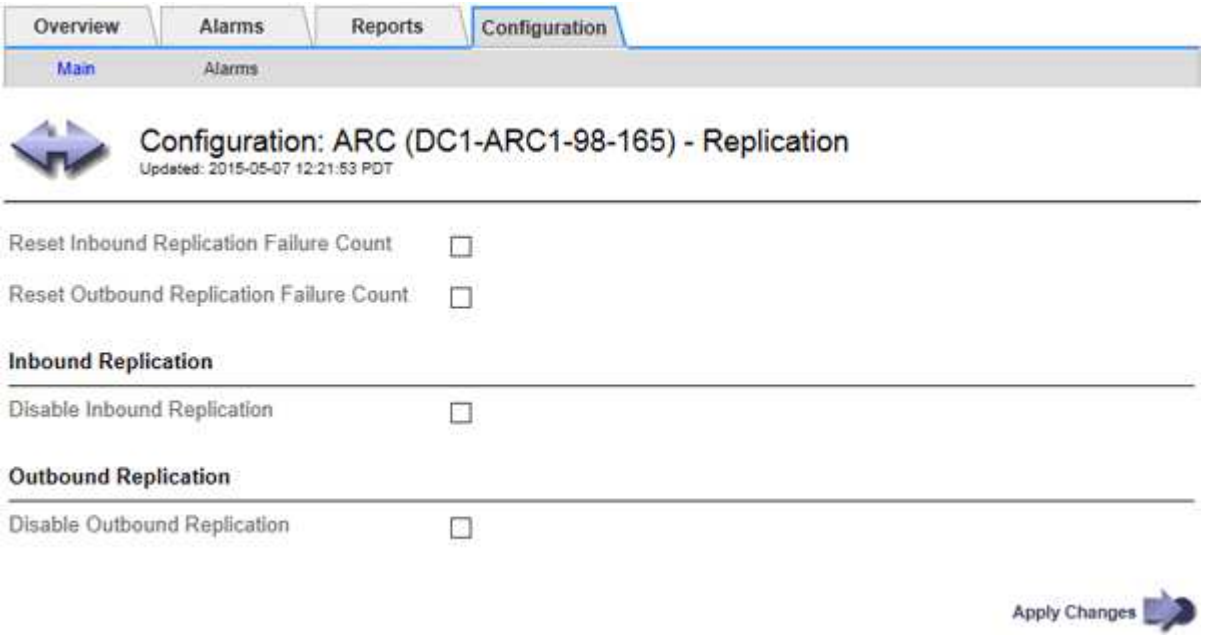
È possibile configurare le impostazioni di replica per un nodo di archiviazione e disattivare la replica in entrata e in uscita oppure reimpostare i conteggi degli errori rilevati per gli allarmi associati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Replication**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare le seguenti impostazioni, se necessario:
   - **Reset Inbound Replication Failure Count** (Ripristina conteggio errori replica in entrata): Selezionare per reimpostare il contatore per gli errori di replica in entrata. Questa opzione può essere utilizzata per cancellare l'allarme RIRF (Inbound Replications — Failed).
   - **Reset Outbound Replication Failure Count** (Ripristina conteggio errori replica in uscita): Selezionare per reimpostare il contatore per gli errori di replica in uscita. Questa opzione può essere utilizzata per cancellare l'allarme RORF (Outbound Replications — Failed).
   - **Disable Inbound Replication** (Disattiva replica in entrata): Selezionare questa opzione per disattivare la replica in entrata come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento.

     Quando la replica in entrata è disattivata, i dati degli oggetti possono essere recuperati dal servizio ARC per la replica in altre posizioni nel sistema StorageGRID, ma gli oggetti non possono essere replicati in questo servizio ARC da altre posizioni del sistema. Il servizio ARC è di sola lettura-.

   - **Disable Outbound Replication** (Disattiva replica in uscita): Selezionare la casella di controllo per disattivare la replica in uscita (incluse le richieste di contenuto per i recuperi HTTP) come parte di una

procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento.

Quando la replica in uscita è disattivata, i dati degli oggetti possono essere copiati in questo servizio ARC per soddisfare le regole ILM, ma i dati degli oggetti non possono essere recuperati dal servizio ARC per essere copiati in altre posizioni nel sistema StorageGRID. Il servizio ARC è di sola-scrittura.

5. Selezionare **Applica modifiche**.

Impostare gli allarmi personalizzati per il nodo di archiviazione

È necessario stabilire allarmi personalizzati per gli attributi ARQL e ARRL utilizzati per monitorare la velocità e l'efficienza del recupero dei dati a oggetti dal sistema di storage di archiviazione da parte del nodo di archiviazione.

- ARQL: Lunghezza media della coda. Il tempo medio, in microsecondi, in cui i dati dell'oggetto vengono messi in coda per il recupero dal sistema di storage di archiviazione.
- ARRL: Latenza media della richiesta. Il tempo medio, in microsecondi, necessario al nodo di archiviazione per recuperare i dati degli oggetti dal sistema di storage di archiviazione.

I valori accettabili per questi attributi dipendono dalla configurazione e dall'utilizzo del sistema di storage di archiviazione. (Andare a **ARC** > **Recupera** > **Panoramica** > **principale**.) I valori impostati per i timeout delle richieste e il numero di sessioni rese disponibili per le richieste di recupero sono particolarmente influenti.

Una volta completata l'integrazione, monitorare i recuperi dei dati dell'oggetto del nodo di archiviazione per stabilire i valori relativi ai tempi di recupero e alle lunghezze della coda normali. Quindi, creare allarmi personalizzati per ARQL e ARRL che si attiveranno in caso di condizioni operative anomale. Consultare le istruzioni per "gestione degli allarmi (sistema legacy)".

Integrare Tivoli Storage Manager

Configurazione e funzionamento del nodo di archiviazione

Il sistema StorageGRID gestisce il nodo di archiviazione come una posizione in cui gli oggetti vengono memorizzati a tempo indeterminato e sono sempre accessibili.

Quando viene acquisito un oggetto, vengono create copie in tutte le posizioni richieste, inclusi i nodi di archivio, sulla base delle regole ILM (Information Lifecycle Management) definite per il sistema StorageGRID. Il nodo di archiviazione funge da client per un server TSM e le librerie del client TSM vengono installate sul nodo di archiviazione mediante il processo di installazione del software StorageGRID. I dati dell'oggetto indirizzati al nodo di archiviazione per lo storage vengono salvati direttamente nel server TSM quando vengono ricevuti. Il nodo di archiviazione non esegue lo stage dei dati dell'oggetto prima di salvarli nel server TSM, né esegue l'aggregazione di oggetti. Tuttavia, il nodo di archiviazione può inviare più copie al server TSM in una singola transazione quando la velocità dei dati lo giustifica.

Dopo che il nodo di archiviazione ha salvato i dati dell'oggetto nel server TSM, i dati dell'oggetto vengono gestiti dal server TSM utilizzando i relativi criteri di conservazione/ciclo di vita. Questi criteri di conservazione devono essere definiti in modo da essere compatibili con il funzionamento del nodo di archiviazione. Ovvero, i dati degli oggetti salvati dal nodo di archiviazione devono essere memorizzati a tempo indeterminato e devono essere sempre accessibili dal nodo di archiviazione, a meno che non vengano cancellati dal nodo di archiviazione.

Non esiste alcuna connessione tra le regole ILM del sistema StorageGRID e le policy di conservazione/ciclo di vita del server TSM. Ciascuno di essi opera indipendentemente dall'altro; tuttavia, quando ciascun oggetto

viene acquisito nel sistema StorageGRID, è possibile assegnargli una classe di gestione TSM. Questa classe di gestione viene passata al server TSM insieme ai dati dell'oggetto. L'assegnazione di diverse classi di gestione a diversi tipi di oggetti consente di configurare il server TSM in modo che i dati degli oggetti siano memorizzati in diversi pool di storage o di applicare criteri di migrazione o conservazione diversi in base alle esigenze. Ad esempio, gli oggetti identificati come backup del database (contenuto temporaneo che può essere sovrascritto con dati più recenti) potrebbero essere trattati in modo diverso rispetto ai dati dell'applicazione (contenuto fisso che deve essere conservato a tempo indeterminato).

Il nodo di archiviazione può essere integrato con un server TSM nuovo o esistente; non richiede un server TSM dedicato. I server TSM possono essere condivisi con altri client, a condizione che il server TSM sia dimensionato in modo appropriato per il carico massimo previsto. TSM deve essere installato su un server o una macchina virtuale separato dal nodo di archiviazione.

È possibile configurare più di un nodo di archiviazione per la scrittura sullo stesso server TSM; tuttavia, questa configurazione è consigliata solo se i nodi di archiviazione scrivono set di dati diversi nel server TSM. La configurazione di più di un nodo di archivio per la scrittura sullo stesso server TSM non è consigliata quando ciascun nodo di archivio scrive copie degli stessi dati dell'oggetto nell'archivio. In quest'ultimo scenario, entrambe le copie sono soggette a un singolo punto di errore (il server TSM) per quelle che si suppone siano copie ridondanti indipendenti dei dati dell'oggetto.

I nodi di archiviazione non utilizzano il componente HSM (Hierarchical Storage Management) di TSM.

Best practice per la configurazione

Quando si esegue il dimensionamento e la configurazione del server TSM, è necessario applicare le Best practice per ottimizzarlo e utilizzarlo con il nodo di archiviazione.

Durante il dimensionamento e la configurazione del server TSM, è necessario considerare i seguenti fattori:

- Poiché il nodo di archiviazione non aggrega gli oggetti prima di salvarli nel server TSM, il database TSM deve essere dimensionato in modo da contenere riferimenti a tutti gli oggetti che verranno scritti nel nodo di archiviazione.
- Il software Archive Node non è in grado di tollerare la latenza necessaria per la scrittura di oggetti direttamente su nastro o su altri supporti rimovibili. Pertanto, il server TSM deve essere configurato con un pool di storage su disco per la memorizzazione iniziale dei dati salvati dal nodo di archiviazione ogni volta che si utilizzano supporti rimovibili.
- È necessario configurare i criteri di conservazione TSM per utilizzare la conservazione basata su eventi-. Il nodo di archiviazione non supporta i criteri di conservazione TSM basati sulla creazione. Utilizzare le seguenti impostazioni consigliate di retmin=0 e retver=0 nel criterio di conservazione (che indica che la conservazione inizia quando il nodo di archiviazione attiva un evento di conservazione e viene mantenuta per 0 giorni dopo). Tuttavia, questi valori per retmin e retver sono facoltativi.

Il pool di dischi deve essere configurato per migrare i dati nel pool di nastri (ovvero, il pool di nastri deve essere il NXTSTGPOOL del pool di dischi). Il pool di nastri non deve essere configurato come pool di copie del pool di dischi con scrittura simultanea su entrambi i pool (ovvero, il pool di nastri non può essere un COPYSTGPOOL per il pool di dischi). Per creare copie non in linea dei nastri contenenti dati del nodo di archiviazione, configurare il server TSM con un secondo pool di nastri che è un pool di copie del pool di nastri utilizzato per i dati del nodo di archiviazione.

Completare la configurazione del nodo di archiviazione

Il nodo di archiviazione non funziona dopo aver completato il processo di installazione. Prima che il sistema StorageGRID possa salvare gli oggetti nel nodo di archivio TSM, è

necessario completare l'installazione e la configurazione del server TSM e configurare il nodo di archivio per comunicare con il server TSM.

Fare riferimento alla seguente documentazione IBM, se necessario, durante la preparazione del server TSM per l'integrazione con il nodo di archiviazione in un sistema StorageGRID:

- "Guida per l'installazione e l'utente dei driver di dispositivo su nastro IBM"
- "IBM Tape Device Drivers Programming Reference"

Installare un nuovo server TSM

È possibile integrare il nodo di archiviazione con un server TSM nuovo o esistente. Se si sta installando un nuovo server TSM, seguire le istruzioni nella documentazione del TSM per completare l'installazione.

> Un nodo di archiviazione non può essere co-ospitato con un server TSM.

Configurare il server TSM

Questa sezione include istruzioni di esempio per preparare un server TSM seguendo le Best practice TSM.

Le seguenti istruzioni guidano l'utente nel processo di:

- Definizione di un pool di storage su disco e di un pool di storage su nastro (se necessario) sul server TSM
- Definizione di un criterio di dominio che utilizza la classe di gestione TSM per i dati salvati dal nodo di archiviazione e registrazione di un nodo per utilizzare questo criterio di dominio

Queste istruzioni sono fornite esclusivamente a scopo informativo; non sono intese a sostituire la documentazione del TSM o a fornire istruzioni complete e complete adatte a tutte le configurazioni. Le istruzioni specifiche per l'implementazione devono essere fornite da un amministratore TSM che abbia familiarità con i requisiti dettagliati e con la documentazione completa di TSM Server.

Definire i pool di storage su disco e nastro TSM

Il nodo di archiviazione scrive in un pool di dischi di storage. Per archiviare il contenuto su nastro, è necessario configurare il pool di storage su disco per spostare il contenuto in un pool di storage su nastro.

A proposito di questa attività

Per un server TSM, è necessario definire un pool di storage su nastro e un pool di storage su disco in Tivoli Storage Manager. Una volta definito il pool di dischi, creare un volume di dischi e assegnarlo al pool di dischi. Non è necessario un pool di nastri se il server TSM utilizza lo storage solo-disco.

Prima di creare un pool di storage su nastro, è necessario completare diversi passaggi sul server TSM. Creare una libreria di nastri e almeno un'unità nella libreria di nastri. Definire un percorso dal server alla libreria e dal server ai dischi, quindi definire una classe di dispositivi per i dischi. I dettagli di questi passaggi possono variare a seconda della configurazione hardware e dei requisiti di storage del sito. Per ulteriori informazioni, consultare la documentazione del TSM.

Il seguente set di istruzioni illustra il processo. Tenere presente che i requisiti del sito potrebbero essere diversi

a seconda dei requisiti dell'implementazione. Per informazioni dettagliate sulla configurazione e istruzioni, consultare la documentazione del TSM.

È necessario accedere al server con privilegi amministrativi e utilizzare lo strumento dsmadmc per eseguire i seguenti comandi.

Fasi

1. Creare una libreria di nastri.

   `define library tapelibrary libtype=scsi`

   Dove *tapelibrary* è un nome arbitrario scelto per la libreria di nastri e il valore di `libtype` può variare a seconda del tipo di libreria di nastri.

2. Definire un percorso dal server alla libreria di nastri.

   `define path servername tapelibrary srctype=server desttype=library device=lib-devicename`

   - *servername* È il nome del server TSM
   - *tapelibrary* è il nome della libreria di nastri definito
   - *lib-devicename* è il nome del dispositivo per la libreria di nastri

3. Definire un disco per la libreria.

   `define drive tapelibrary drivename`

   - *drivename* è il nome che si desidera specificare per l'unità
   - *tapelibrary* è il nome della libreria di nastri definito

     A seconda della configurazione dell'hardware, potrebbe essere necessario configurare uno o più dischi aggiuntivi. Ad esempio, se il server TSM è collegato a uno switch Fibre Channel con due ingressi da una libreria di nastri, è possibile definire un'unità per ciascun ingresso.

4. Definire un percorso dal server all'unità definita.

   `define path servername drivename srctype=server desttype=drive library=tapelibrary device=drive-dname`

   - *drive-dname* è il nome del dispositivo per il disco
   - *tapelibrary* è il nome della libreria di nastri definito

     Ripetere l'operazione per ogni disco definito per la libreria di nastri, utilizzando un disco separato *drivename* e. *drive-dname* per ciascun disco.

5. Definire una classe di dispositivi per i dischi.

   `define devclass DeviceClassName devtype=lto library=tapelibrary format=tapetype`

   - *DeviceClassName* è il nome della classe device

- *lto* è il tipo di disco collegato al server
- *tapelibrary* è il nome della libreria di nastri definito
- *tapetype* è il tipo di nastro, ad esempio ultrium3

6. Aggiungere volumi su nastro all'inventario per la libreria.

   ```
   checkin libvolume tapelibrary
   ```

   tapelibrary è il nome della libreria di nastri definito.

7. Creare il pool di storage su nastro primario.

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - *SGWSTapePool* È il nome del pool di storage su nastro del nodo di archiviazione. È possibile selezionare qualsiasi nome per il pool di storage su nastro (purché il nome utilizzi le convenzioni di sintassi previste dal server TSM).
   - *DeviceClassName* è il nome della classe di dispositivi per la libreria di nastri.
   - *description* È una descrizione del pool di storage che può essere visualizzato sul server TSM utilizzando `query stgpool` comando. Ad esempio: "Pool di archiviazione su nastro per il nodo di archiviazione".
   - *collocate=filespace* Specifica che il server TSM deve scrivere oggetti dallo stesso spazio di file in un singolo nastro.
   - XX è uno dei seguenti:
     - Il numero di nastri vuoti nella libreria di nastri (nel caso in cui il nodo di archiviazione sia l'unica applicazione che utilizza la libreria).
     - Il numero di nastri allocati per l'utilizzo da parte del sistema StorageGRID (nei casi in cui la libreria di nastri è condivisa).

8. Su un server TSM, creare un pool di storage su disco. Nella console di amministrazione del server TSM, immettere

   ```
   define stgpool SGWSDiskPool disk description=description
   maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
   lowmig=percent_low
   ```

   - *SGWSDiskPool* È il nome del pool di dischi del nodo di archiviazione. È possibile selezionare qualsiasi nome per il pool di storage su disco (purché il nome utilizzi le convenzioni di sintassi previste dal TSM).
   - *description* È una descrizione del pool di storage che può essere visualizzato sul server TSM utilizzando `query stgpool` comando. Ad esempio, "Pool di archiviazione su disco per il nodo di archiviazione".
   - *maximum_file_size* forza la scrittura diretta su nastro di oggetti di dimensioni superiori a tali, anziché la memorizzazione nella cache del pool di dischi. Si consiglia di impostare *maximum_file_size* A 10 GB.
   - *nextstgpool=SGWSTapePool* Fa riferimento al pool di storage su disco al pool di storage su nastro definito per il nodo di archiviazione.
   - *percent_high* imposta il valore in corrispondenza del quale il pool di dischi inizia la migrazione del

contenuto nel pool di nastri. Si consiglia di impostare *percent_high* a 0 in modo che la migrazione dei dati inizi immediatamente

- *percent_low* imposta il valore in corrispondenza del quale la migrazione al pool di nastri viene interrotta. Si consiglia di impostare *percent_low* a 0 per eliminare il pool di dischi.

9. Su un server TSM, creare uno o più volumi di dischi e assegnarli al pool di dischi.

```
define volume SGWSDiskPool volume_name formatsize=size
```

   - *SGWSDiskPool* è il nome del pool di dischi.
   - *volume_name* è il percorso completo verso la posizione del volume (ad esempio, `/var/local/arc/stage6.dsm`) Sul server TSM in cui scrive il contenuto del pool di dischi in preparazione del trasferimento su nastro.
   - *size* È la dimensione, in MB, del volume del disco.

     Ad esempio, per creare un singolo volume di disco in modo che il contenuto di un pool di dischi occupi un singolo nastro, impostare il valore di size su 200000 quando il volume del nastro ha una capacità di 200 GB.

     Tuttavia, potrebbe essere consigliabile creare più volumi di dischi di dimensioni inferiori, in quanto il server TSM può scrivere su ciascun volume del pool di dischi. Ad esempio, se la dimensione del nastro è di 250 GB, creare 25 volumi di dischi con una dimensione di 10 GB (10000) ciascuno.

Il server TSM preassegna lo spazio nella directory per il volume del disco. Il completamento di questa operazione può richiedere più di tre ore per un volume di disco da 200 GB.

Definire un criterio di dominio e registrare un nodo

È necessario definire un criterio di dominio che utilizzi la classe di gestione TSM per i dati salvati dal nodo di archiviazione, quindi registrare un nodo per utilizzare questo criterio di dominio.

> I processi del nodo di archiviazione possono perdere memoria se la password del client per il nodo di archiviazione in Tivoli Storage Manager (TSM) scade. Assicurarsi che il server TSM sia configurato in modo che il nome utente/la password del client per il nodo di archiviazione non scada mai.

Quando si registra un nodo sul server TSM per l'utilizzo del nodo di archiviazione (o per l'aggiornamento di un nodo esistente), è necessario specificare il numero di punti di montaggio che il nodo può utilizzare per le operazioni di scrittura specificando il parametro MAXNUMMP nel comando DEL NODO DI REGISTRO. Il numero di punti di montaggio equivale in genere al numero di testine del disco a nastro allocate al nodo di archiviazione. Il numero specificato per MAXNUMMP sul server TSM deve essere grande almeno quanto il valore impostato per **ARC** > **Target** > **Configurazione** > **principale** > **numero massimo di sessioni di archiviazione** per il nodo di archiviazione, Che è impostato su un valore pari a 0 o 1, in quanto le sessioni dello store simultanee non sono supportate dal nodo di archiviazione.

Il valore di MAXSESSIONS impostato per il server TSM controlla il numero massimo di sessioni che possono essere aperte al server TSM da tutte le applicazioni client. Il valore di MAXSESSIONS specificato nel TSM deve essere almeno grande quanto il valore specificato per **ARC** > **Target** > **Configurazione** > **principale** > **numero di sessioni** nel Grid Manager per il nodo di archiviazione. Il nodo di archiviazione crea contemporaneamente al massimo una sessione per punto di montaggio più un piccolo numero (< 5) di sessioni aggiuntive.

Il nodo TSM assegnato al nodo di archiviazione utilizza una policy di dominio personalizzata `tsm-domain`. Il `tsm-domain` Il criterio di dominio è una versione modificata del criterio di dominio "standard", configurata per la scrittura su nastro e con la destinazione di archivio impostata come pool di archiviazione del sistema StorageGRID (*`SGWSDiskPool`*).

> È necessario accedere al server TSM con privilegi amministrativi e utilizzare lo strumento dsmacmc per creare e attivare i criteri di dominio.

Creare e attivare i criteri di dominio

È necessario creare un criterio di dominio e attivarlo per configurare il server TSM in modo da salvare i dati inviati dal nodo di archiviazione.

Fasi

1. Creare un criterio di dominio.

   ```
   copy domain standard tsm-domain
   ```

2. Se non si utilizza una classe di gestione esistente, immettere una delle seguenti informazioni:

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   `default` è la classe di gestione predefinita per l'implementazione.

3. Creare un gruppo di copygroup nel pool di storage appropriato. Immettere (su una riga):

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   `default` È la classe di gestione predefinita per il nodo di archiviazione. I valori di `retinit`, `retmin`, e. `retver` Sono stati scelti per riflettere il comportamento di conservazione attualmente utilizzato dal nodo di archiviazione

   > Non impostare `retinit` a. `retinit=create`. Impostazione `retinit=create` Impedisce al nodo di archiviazione di eliminare il contenuto, poiché gli eventi di conservazione vengono utilizzati per rimuovere il contenuto dal server TSM.

4. Assegnare la classe di gestione come predefinita.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Impostare il nuovo set di criteri come attivo.

   ```
   activate policyset tsm-domain standard
   ```

   Ignorare l'avviso "nessun gruppo di copie di backup" visualizzato quando si immette il comando di attivazione.

6. Registrare un nodo per utilizzare il nuovo set di criteri sul server TSM. Sul server TSM, immettere (su una riga):

```
register node arc-user arc-password passexp=0 domain=tsm-domain
MAXNUMMP=number-of-sessions
```

Arc-user e Arc-password sono lo stesso nome e password del nodo client definiti nel nodo di archiviazione e il valore di MAXNUMMP è impostato sul numero di unità nastro riservate per le sessioni di archiviazione del nodo di archiviazione.

> Per impostazione predefinita, la registrazione di un nodo crea un ID utente amministrativo con l'autorità del proprietario del client, con la password definita per il nodo.

Migrare i dati in StorageGRID

È possibile migrare grandi quantità di dati nel sistema StorageGRID utilizzando contemporaneamente il sistema StorageGRID per le operazioni quotidiane.

Utilizza questa guida per pianificare una migrazione di grandi quantità di dati nel sistema StorageGRID. Non si tratta di una guida generale alla migrazione dei dati e non include procedure dettagliate per l'esecuzione di una migrazione. Seguire le linee guida e le istruzioni di questa sezione per garantire che i dati vengano migrati in modo efficiente nel sistema StorageGRID senza interferire con le operazioni quotidiane e che i dati migrati vengano gestiti in modo appropriato dal sistema StorageGRID.

Confermare la capacità del sistema StorageGRID

Prima di migrare grandi quantità di dati nel sistema StorageGRID, verificare che il sistema StorageGRID disponga della capacità del disco necessaria per gestire il volume previsto.

Se il sistema StorageGRID include un nodo di archiviazione e una copia degli oggetti migrati è stata salvata nello storage nearline (ad esempio su nastro), assicurarsi che lo storage del nodo di archiviazione abbia una capacità sufficiente per il volume previsto dei dati migrati.

Nell'ambito della valutazione della capacità, esaminare il profilo dei dati degli oggetti che si intende migrare e calcolare la quantità di capacità del disco richiesta. Per ulteriori informazioni sul monitoraggio della capacità del disco del sistema StorageGRID, vedere "Gestire i nodi di storage" e le istruzioni per "Monitoraggio di StorageGRID".

Determinare il criterio ILM per i dati migrati

Il criterio ILM del sistema StorageGRID determina il numero di copie eseguite, le posizioni in cui vengono memorizzate e il periodo di conservazione delle copie. Un criterio ILM è costituito da un insieme di regole ILM che descrivono come filtrare gli oggetti e gestire i dati degli oggetti nel tempo.

A seconda del modo in cui vengono utilizzati i dati migrati e dei requisiti per i dati migrati, è possibile definire regole ILM univoche per i dati migrati che sono diverse dalle regole ILM utilizzate per le operazioni quotidiane. Ad esempio, se esistono requisiti normativi diversi per la gestione quotidiana dei dati rispetto ai dati inclusi nella migrazione, è possibile che si desideri un numero diverso di copie dei dati migrati su un diverso livello di storage.

È possibile configurare regole che si applicano esclusivamente ai dati migrati se è possibile distinguere in modo univoco tra i dati migrati e i dati oggetto salvati dalle operazioni quotidiane.

Se è possibile distinguere in modo affidabile tra i tipi di dati utilizzando uno dei criteri dei metadati, è possibile utilizzare questi criteri per definire una regola ILM che si applica solo ai dati migrati.

Prima di iniziare la migrazione dei dati, assicurarsi di aver compreso il criterio ILM del sistema StorageGRID e il modo in cui verrà applicato ai dati migrati e di aver apportato e verificato eventuali modifiche al criterio ILM. Vedere "Gestire gli oggetti con ILM".

> Un criterio ILM specificato in modo non corretto può causare una perdita di dati irreversibile. Esaminare attentamente tutte le modifiche apportate a un criterio ILM prima di attivarlo per assicurarsi che il criterio funzioni come previsto.

Valutare l'impatto della migrazione sulle operazioni

Un sistema StorageGRID è progettato per fornire un funzionamento efficiente per lo storage e il recupero di oggetti e per fornire un'eccellente protezione contro la perdita di dati attraverso la creazione perfetta di copie ridondanti di dati a oggetti e metadati.

Tuttavia, la migrazione dei dati deve essere gestita con attenzione in base alle istruzioni contenute in questa guida per evitare di avere un impatto sulle operazioni quotidiane del sistema o, in casi estremi, mettere i dati a rischio di perdita in caso di guasto nel sistema StorageGRID.

La migrazione di grandi quantità di dati pone un carico aggiuntivo sul sistema. Quando il sistema StorageGRID viene caricato pesantemente, risponde più lentamente alle richieste di archiviazione e recupero degli oggetti. Ciò può interferire con le richieste di archiviazione e recupero che sono parte integrante delle operazioni quotidiane. La migrazione può anche causare altri problemi operativi. Ad esempio, quando un nodo di storage si sta avvicinando alla capacità, il carico intermittente elevato dovuto all'acquisizione batch può causare il ciclo del nodo di storage tra sola lettura e lettura/scrittura, generando notifiche.

Se il carico pesante persiste, è possibile sviluppare code per varie operazioni che il sistema StorageGRID deve eseguire per garantire la ridondanza completa dei dati degli oggetti e dei metadati.

La migrazione dei dati deve essere gestita con attenzione in base alle linee guida del presente documento per garantire un funzionamento sicuro ed efficiente del sistema StorageGRID durante la migrazione. Durante la migrazione dei dati, acquisire oggetti in batch o ridurre continuamente l'acquisizione. Quindi, monitorare continuamente il sistema StorageGRID per garantire che i diversi valori degli attributi non vengano superati.

Pianificare e monitorare la migrazione dei dati

La migrazione dei dati deve essere pianificata e monitorata, se necessario, per garantire che i dati vengano inseriti in base alla policy ILM entro i tempi richiesti.

Pianificazione della migrazione dei dati

Evita la migrazione dei dati durante le ore di funzionamento principali. Limitare la migrazione dei dati a serate, fine settimana e altri periodi in cui l'utilizzo del sistema è basso.

Se possibile, non pianificare la migrazione dei dati durante i periodi di attività elevata. Tuttavia, se non è pratico evitare completamente il periodo di attività elevato, è sicuro procedere finché si monitorano attentamente gli attributi pertinenti e si interviene se superano i valori accettabili.

Monitorare la migrazione dei dati

Questa tabella elenca gli attributi da monitorare durante la migrazione dei dati e i problemi che rappresentano.

Se si utilizzano criteri di classificazione del traffico con limiti di velocità per accelerare l'acquisizione, è possibile monitorare la velocità osservata insieme alle statistiche descritte nella tabella seguente e ridurre i limiti, se necessario.

Monitorare	Descrizione
Numero di oggetti in attesa di valutazione ILM	1. Selezionare **SUPPORT** > **Tools** > **Grid topology**. 2. Selezionare ***deployment*** > **Overview** > **Main**. 3. Nella sezione ILM Activity (attività ILM), monitorare il numero di oggetti visualizzati per i seguenti attributi: ◦ **In attesa - tutti (XQUZ)**: Il numero totale di oggetti in attesa di valutazione ILM. ◦ **In attesa - Client (XCQZ)**: Il numero totale di oggetti in attesa di valutazione ILM dalle operazioni del client (ad esempio, acquisizione). 4. Se il numero di oggetti visualizzato per uno di questi attributi supera 100,000, ridurre il tasso di acquisizione degli oggetti per ridurre il carico sul sistema StorageGRID.
Capacità di storage del sistema di archiviazione mirato	Se la policy ILM salva una copia dei dati migrati in un sistema storage di archiviazione di destinazione (nastro o cloud), monitorate la capacità del sistema storage di archiviazione di destinazione per garantire che vi sia una capacità sufficiente per i dati migrati.
Nodo archivio > **ARC** > **Memorizza**	Se viene attivato un allarme per l'attributo **Store Failures (ARVF)**, il sistema storage di archiviazione di destinazione potrebbe aver raggiunto la capacità. Controllare il sistema storage di archiviazione di destinazione e risolvere eventuali problemi che hanno generato un allarme.

Gestire gli oggetti con ILM

Gestire gli oggetti con ILM

Le regole di gestione del ciclo di vita delle informazioni (ILM, Information Lifecycle Management) contenute in un criterio ILM indicano a StorageGRID come creare e distribuire copie dei dati degli oggetti e come gestirle nel tempo.

A proposito di queste istruzioni

La progettazione e l'implementazione di regole e politiche ILM richiedono un'attenta pianificazione. È necessario comprendere i requisiti operativi, la topologia del sistema StorageGRID, le esigenze di protezione degli oggetti e i tipi di storage disponibili. Quindi, è necessario determinare come si desidera copiare, distribuire e memorizzare diversi tipi di oggetti.

Seguire queste istruzioni per:

- Scopri di più su StorageGRID ILM, tra cui "Come ILM opera per tutta la vita di un oggetto".
- Scopri come configurare "pool di storage", "Pool di cloud storage", e. "Regole ILM".
- Scopri come "Creare, simulare e attivare un criterio ILM" che proteggerà i dati degli oggetti in uno o più siti.
- Scopri come "Gestire gli oggetti con S3 Object Lock", Che aiuta a garantire che gli oggetti in specifici

bucket S3 non vengano cancellati o sovrascritti per un determinato periodo di tempo.

Scopri di più

Per ulteriori informazioni, consulta questi video:

- "Video: Regole di gestione del ciclo di vita delle informazioni in StorageGRID 11,8".
- "Video: Politiche di gestione del ciclo di vita delle informazioni in StorageGRID 11,8"

ILM e ciclo di vita degli oggetti

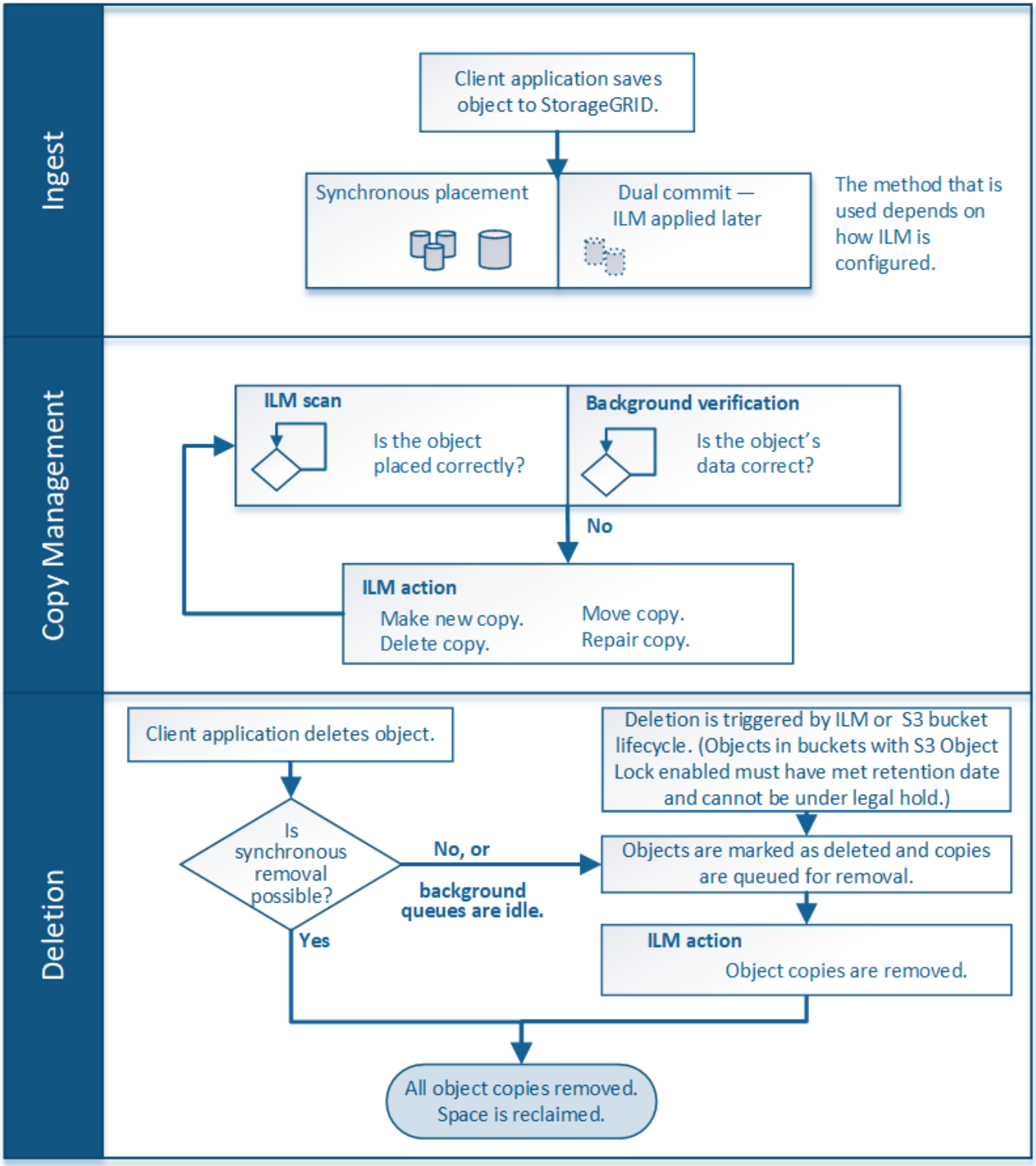
Come ILM opera per tutta la vita di un oggetto

Comprendere come StorageGRID utilizza ILM per gestire gli oggetti in ogni fase della loro vita può aiutarti a progettare una policy più efficace.

- **Acquisizione**: L'acquisizione inizia quando un'applicazione client S3 o Swift stabilisce una connessione per salvare un oggetto nel sistema StorageGRID ed è completa quando StorageGRID restituisce un messaggio di acquisizione riuscita al client. I dati degli oggetti vengono protetti durante l'acquisizione applicando immediatamente le istruzioni ILM (posizionamento sincrono) o creando copie interinali e applicando ILM successivamente (doppio commit), a seconda di come sono stati specificati i requisiti ILM.
- **Gestione delle copie**: Dopo aver creato il numero e il tipo di copie degli oggetti specificati nelle istruzioni di posizionamento di ILM, StorageGRID gestisce le posizioni degli oggetti e protegge gli oggetti dalla perdita.
  - **Scansione e valutazione ILM**: StorageGRID esegue la scansione continua dell'elenco degli oggetti memorizzati nella griglia e verifica se le copie correnti soddisfano i requisiti ILM. Quando sono richiesti tipi, numeri o posizioni diversi di copie di oggetti, StorageGRID crea, elimina o sposta le copie in base alle necessità.
  - **Verifica dello sfondo**: StorageGRID esegue continuamente la verifica dello sfondo per verificare l'integrità dei dati dell'oggetto. Se viene rilevato un problema, StorageGRID crea automaticamente una nuova copia dell'oggetto o un frammento di oggetto erasure-coded sostitutivo in una posizione che soddisfa i requisiti ILM correnti. Vedere "Verificare l'integrità dell'oggetto".
- **Eliminazione oggetto**: La gestione di un oggetto termina quando tutte le copie vengono rimosse dal sistema StorageGRID. Gli oggetti possono essere rimossi in seguito a una richiesta di eliminazione da parte di un client o in seguito all'eliminazione da parte di ILM o all'eliminazione causata dalla scadenza di un ciclo di vita del bucket S3.

> Gli oggetti in un bucket con S3 Object Lock abilitato non possono essere cancellati se sono in stato di conservazione legale o se è stato specificato un periodo di conservazione fino alla data, ma non ancora soddisfatto.

Il diagramma riassume il funzionamento di ILM durante l'intero ciclo di vita di un oggetto.



Modalità di acquisizione degli oggetti

Opzioni di acquisizione

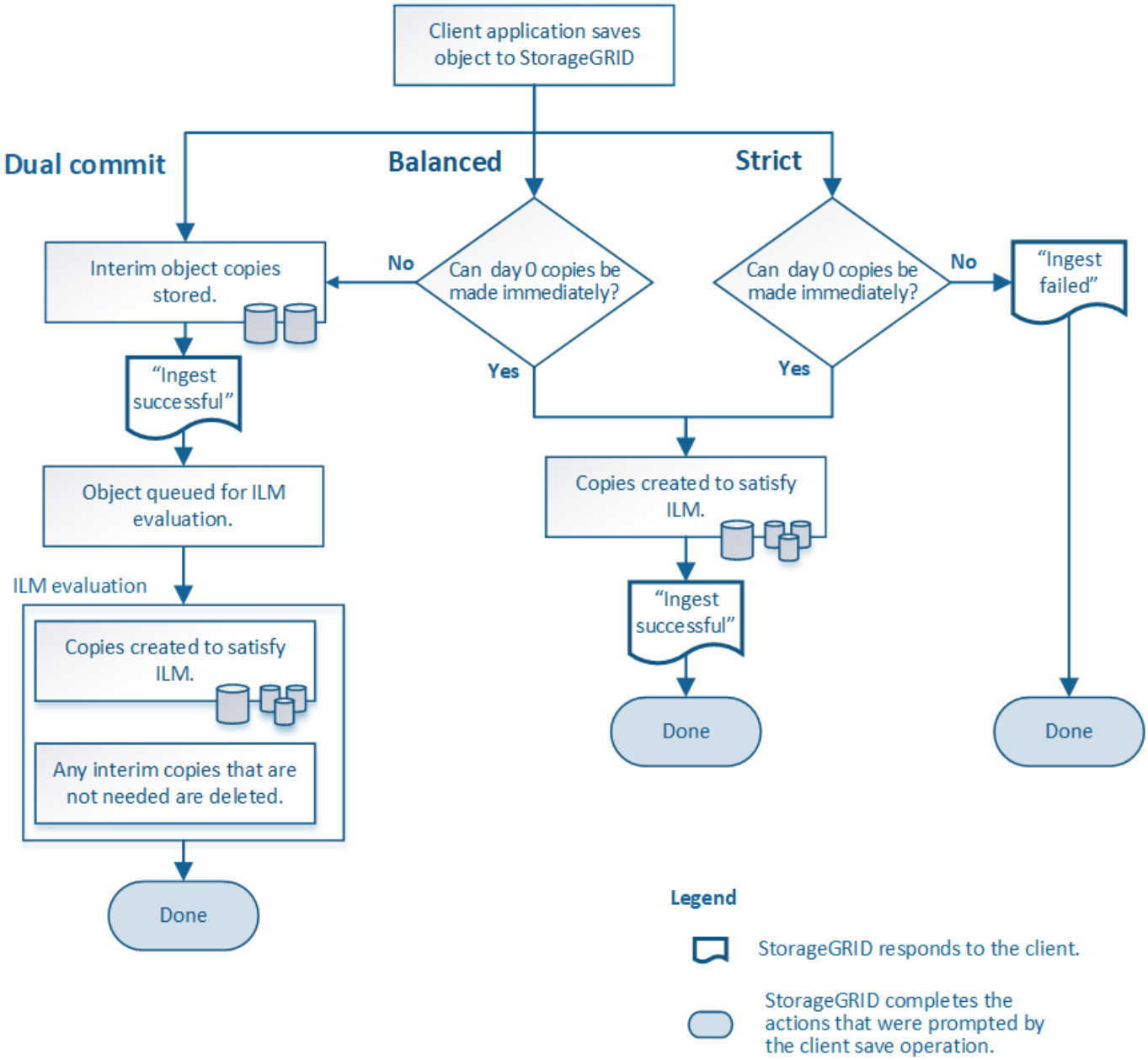
Quando si crea una regola ILM, si specifica una delle tre opzioni per la protezione degli oggetti in fase di acquisizione: Dual commit, strict o Balanced.

A seconda della scelta, StorageGRID esegue copie temporanee e mette in coda gli oggetti per la valutazione

ILM in un secondo momento, oppure utilizza il posizionamento sincrono e crea immediatamente copie per soddisfare i requisiti ILM.

Diagramma di flusso delle opzioni di acquisizione

Il diagramma di flusso mostra cosa accade quando gli oggetti vengono associati da una regola ILM che utilizza ciascuna delle tre opzioni di acquisizione.



Commit doppio

Quando si seleziona l'opzione Dual Commit, StorageGRID crea immediatamente copie temporanee degli oggetti su due diversi nodi storage e restituisce un messaggio "acquisizione riuscita" al client. L'oggetto viene messo in coda per la valutazione ILM e le copie che soddisfano le istruzioni di posizionamento della regola vengono eseguite in un secondo momento. Se il criterio ILM non può essere elaborato immediatamente dopo il dual commit, la protezione in caso di perdita del sito potrebbe richiedere del tempo.

Utilizzare l'opzione Dual Commit in uno dei seguenti casi:

- Stai utilizzando regole ILM multi-sito e la latenza di acquisizione client è la tua principale considerazione. Quando si utilizza il doppio commit, è necessario assicurarsi che la griglia possa eseguire il lavoro aggiuntivo di creazione e rimozione delle copie a doppio commit se non soddisfano ILM. In particolare:
  - Il carico sulla griglia deve essere sufficientemente basso da impedire un backlog ILM.
  - La griglia deve avere risorse hardware in eccesso (IOPS, CPU, memoria, larghezza di banda della rete e così via).
- Si stanno utilizzando regole ILM multi-sito e la connessione WAN tra i siti in genere ha una latenza elevata o una larghezza di banda limitata. In questo scenario, l'utilizzo dell'opzione di commit doppio può contribuire a prevenire i timeout del client. Prima di scegliere l'opzione Dual Commit, è necessario testare l'applicazione client con carichi di lavoro realistici.

Bilanciato (impostazione predefinita)

Quando si seleziona l'opzione Balanced (bilanciamento), StorageGRID utilizza anche il posizionamento sincrono all'acquisizione e crea immediatamente tutte le copie specificate nelle istruzioni di posizionamento della regola. In contrasto con l'opzione rigorosa, se StorageGRID non riesce immediatamente a fare tutte le copie, utilizza invece il doppio commit. Se la policy ILM utilizza posizionamenti su più siti e non è possibile ottenere una protezione immediata in caso di perdita del sito, viene attivato l'avviso **posizionamento ILM non raggiungibile**.

Utilizza l'opzione Balanced per ottenere la migliore combinazione di protezione dei dati, performance di grid e successo di acquisizione. Balanced (bilanciamento) è l'opzione predefinita nella creazione guidata regola ILM.

Rigoroso

Quando si seleziona l'opzione Strict, StorageGRID utilizza il posizionamento sincrono all'acquisizione e crea immediatamente tutte le copie degli oggetti specificate nelle istruzioni di posizionamento della regola. L'acquisizione non riesce se StorageGRID non riesce a creare tutte le copie, ad esempio perché una posizione di storage richiesta è temporaneamente non disponibile. Il client deve riprovare l'operazione.

Utilizzare l'opzione Strict se si dispone di un requisito operativo o normativo per memorizzare immediatamente gli oggetti solo nelle posizioni indicate nella regola ILM. Ad esempio, per soddisfare un requisito normativo, potrebbe essere necessario utilizzare l'opzione Strict e un filtro avanzato Location Constraint per garantire che gli oggetti non vengano mai memorizzati in determinati data center.

Vedere "Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione".

Vantaggi, svantaggi e limitazioni delle opzioni di acquisizione

Comprendere i vantaggi e gli svantaggi di ciascuna delle tre opzioni per la protezione dei dati in fase di acquisizione (Balanced, Strict o Dual Commit) può aiutare a decidere quale scegliere per una regola ILM.

Per una panoramica delle opzioni di acquisizione, vedere "Opzioni di acquisizione".

Vantaggi delle opzioni bilanciate e rigorose

Rispetto al doppio commit, che crea copie intermedie durante l'acquisizione, le due opzioni di posizionamento sincrono possono offrire i seguenti vantaggi:

- **Maggiore sicurezza dei dati**: I dati degli oggetti sono immediatamente protetti come specificato nelle istruzioni di posizionamento della regola ILM, che possono essere configurate per la protezione da un'ampia varietà di condizioni di guasto, incluso il guasto di più di una posizione di storage. Il doppio

commit può proteggere solo dalla perdita di una singola copia locale.

- **Operazione grid più efficiente**: Ogni oggetto viene elaborato una sola volta, man mano che viene acquisito. Poiché il sistema StorageGRID non deve tenere traccia o eliminare le copie temporanee, il carico di elaborazione è inferiore e lo spazio del database viene consumato meno.
- **(Balanced) Recommended** (consigliato): L'opzione Balanced (bilanciato) offre un'efficienza ILM ottimale. Si consiglia di utilizzare l'opzione Balanced (bilanciato), a meno che non sia richiesto un comportamento rigoroso di acquisizione o che la griglia soddisfi tutti i criteri per l'utilizzo di Dual Commit.
- **(Strict) certezze circa le posizioni degli oggetti**: L'opzione Strict garantisce che gli oggetti siano memorizzati immediatamente in base alle istruzioni di posizionamento nella regola ILM.

Svantaggi delle opzioni bilanciate e rigide

Rispetto al doppio commit, le opzioni bilanciate e rigide presentano alcuni svantaggi:

- **Ingest dei client più lunghi**: Le latenze di acquisizione dei client potrebbero essere più lunghe. Quando si utilizzano le opzioni bilanciate o rigorose, non viene restituito al client un messaggio di "acquisizione riuscita" finché non vengono creati e memorizzati tutti i frammenti con erasure coding o le copie replicate. Tuttavia, è molto probabile che i dati degli oggetti raggiungano il posizionamento finale molto più rapidamente.
- **(Strict) tassi più elevati di errore di acquisizione**: Con l'opzione Strict, l'acquisizione non riesce ogni volta che StorageGRID non è in grado di eseguire immediatamente tutte le copie specificate nella regola ILM. Se una posizione di storage richiesta è temporaneamente offline o se problemi di rete causano ritardi nella copia di oggetti tra siti, potrebbero verificarsi elevati tassi di errore di acquisizione.
- **(Strict) le posizioni di caricamento multiparte S3 potrebbero non essere quelle previste in alcune circostanze**: Con Strict, si prevede che gli oggetti vengano posizionati come descritto dalla regola ILM o che l'acquisizione non funzioni. Tuttavia, con un caricamento S3 multiparte, ILM viene valutato per ogni parte dell'oggetto così come viene acquisito e per l'oggetto nel suo complesso al termine del caricamento multiparte. Nei seguenti casi, ciò potrebbe comportare posizionamenti diversi da quelli previsti:
  - **Se ILM cambia mentre è in corso un caricamento di più parti S3**: Poiché ogni parte viene posizionata in base alla regola attiva quando la parte viene inserita, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento di più parti. In questi casi, l'acquisizione dell'oggetto non ha esito negativo. Al contrario, qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e spostata nella posizione corretta in un secondo momento.
  - **Quando le regole ILM filtrano sulla dimensione**: Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o superiori sono memorizzati in DC1 mentre tutti gli oggetti più piccoli sono memorizzati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene memorizzata in DC2. Quando ILM viene valutato per l'oggetto, tutte le parti dell'oggetto vengono spostate in DC1.
- **(Strict) Ingest non ha esito negativo quando i tag degli oggetti o i metadati vengono aggiornati e non è possibile eseguire le nuove posizioni richieste**: Con Strict, si prevede che gli oggetti vengano posizionati come descritto dalla regola ILM o che l'acquisizione non riesca. Tuttavia, quando si aggiornano metadati o tag per un oggetto già memorizzato nella griglia, l'oggetto non viene reinserito. Ciò significa che le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento non vengono apportate immediatamente. Le modifiche al posizionamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background. Se non è possibile apportare modifiche al posizionamento richieste (ad esempio, perché non è disponibile una nuova posizione richiesta), l'oggetto aggiornato mantiene la posizione corrente fino a quando non sono possibili modifiche al posizionamento.

Limitazioni al posizionamento degli oggetti con opzioni bilanciate e rigide

Le opzioni bilanciate o rigide non possono essere utilizzate per le regole ILM che hanno una delle seguenti istruzioni di posizionamento:

- Posizionamento in un pool di storage cloud al giorno 0.
- Posizionamento in un nodo di archivio al giorno 0.
- Posizionamenti in un pool di storage cloud o in un nodo di archivio quando la regola ha un tempo di creazione definito dall'utente come tempo di riferimento.

Queste restrizioni esistono perché StorageGRID non può eseguire copie in modo sincrono a un pool di storage cloud o a un nodo di archivio e un tempo di creazione definito dall'utente potrebbe risolversi fino al momento attuale.

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

Sia la regola ILM che la scelta della coerenza influiscono sulla protezione degli oggetti. Queste impostazioni possono interagire.

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

Di seguito viene riportato un breve riepilogo dei valori di coerenza disponibili in StorageGRID:

- **All**: Tutti i nodi ricevono immediatamente i metadati degli oggetti o la richiesta non riesce.
- **Strong-Global**: I metadati degli oggetti vengono immediatamente distribuiti a tutti i siti. Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
- **Strong-site**: I metadati degli oggetti vengono immediatamente distribuiti ad altri nodi del sito. Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write**: Fornisce coerenza lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available**: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

> Prima di selezionare un valore di coerenza, "leggi la descrizione completa della coerenza". Prima di modificare il valore predefinito, è necessario comprendere i vantaggi e le limitazioni.

Esempio di interazione tra le regole di coerenza e ILM

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

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

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

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

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

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

Informazioni correlate

- "Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"

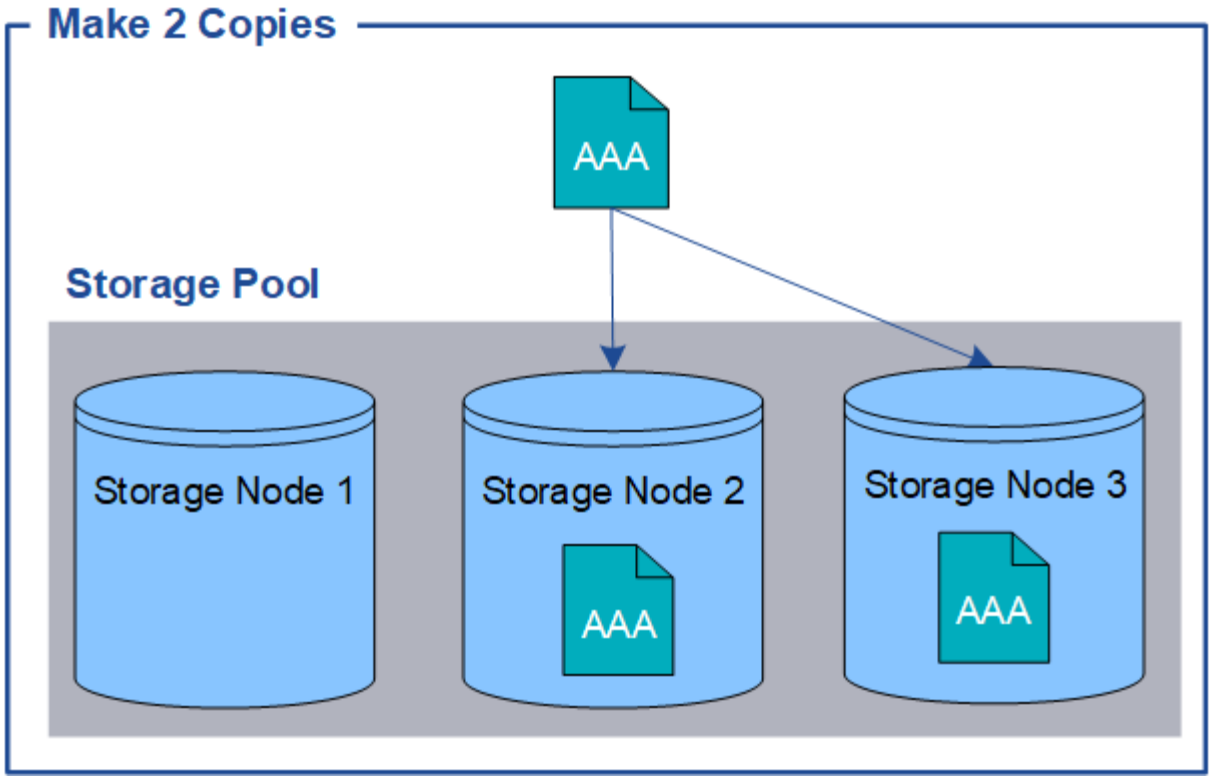
Modalità di archiviazione degli oggetti (replica o erasure coding)

Che cos'è la replica?

La replica è uno dei due metodi utilizzati da StorageGRID per memorizzare i dati degli oggetti. Quando gli oggetti corrispondono a una regola ILM che utilizza la replica, il sistema crea copie esatte dei dati dell'oggetto e le memorizza nei nodi di storage o nei nodi di archivio.

Quando si configura una regola ILM per la creazione di copie replicate, specificare il numero di copie da creare, la posizione delle copie e la durata della memorizzazione delle copie in ciascuna posizione.

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



Quando StorageGRID associa gli oggetti a questa regola, crea due copie dell'oggetto, collocando ciascuna copia su un nodo di storage diverso nel pool di storage. Le due copie possono essere collocate su due dei tre nodi di storage disponibili. In questo caso, la regola ha posizionato le copie degli oggetti sui nodi di storage 2 e 3. Poiché sono presenti due copie, l'oggetto può essere recuperato in caso di guasto di uno qualsiasi dei nodi del pool di storage.

> StorageGRID può memorizzare solo una copia replicata di un oggetto su un dato nodo di storage. Se la griglia include tre nodi di storage e si crea una regola ILM di 4 copie, verranno eseguite solo tre copie, una copia per ciascun nodo di storage. Viene attivato l'avviso **ILM placement unachievable** per indicare che la regola ILM non può essere applicata completamente.

Informazioni correlate

- "Che cos'è l'erasure coding"
- "Che cos'è un pool di storage"
- "Abilita la protezione contro la perdita di sito utilizzando la replica e l'erasure coding"

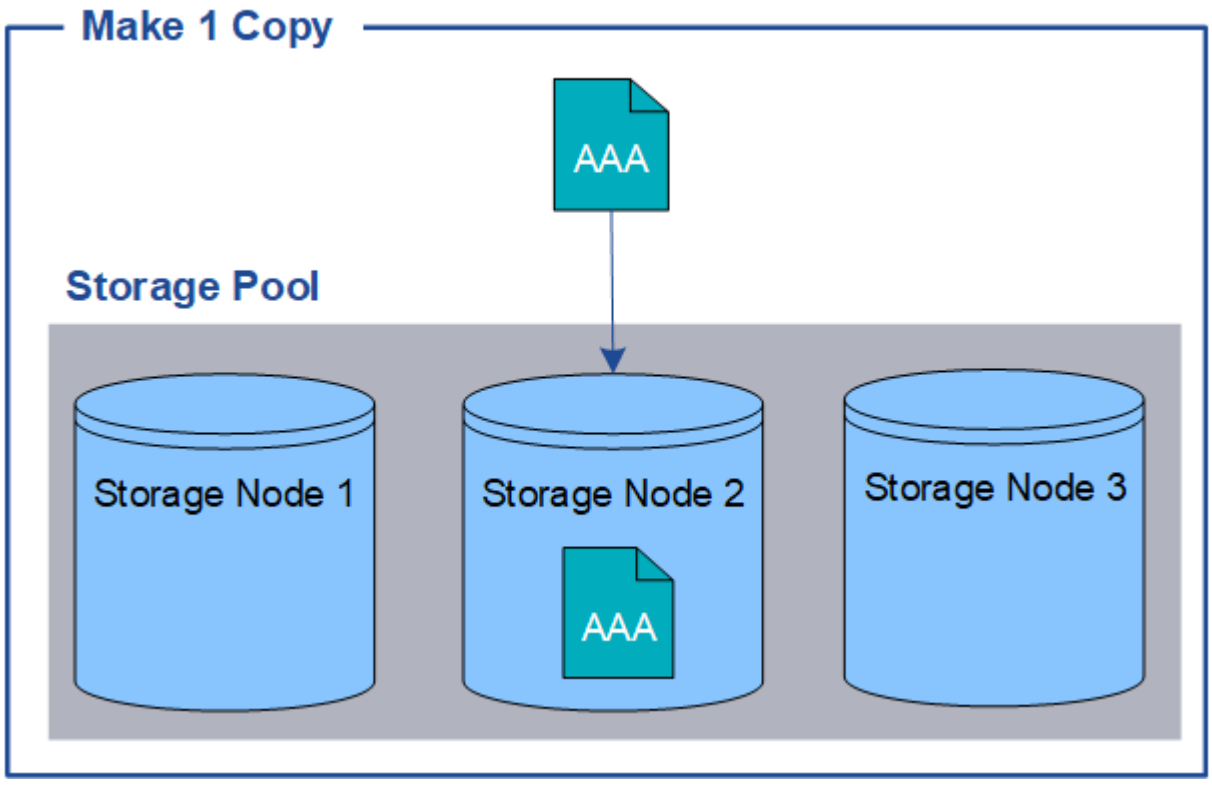
Perché non utilizzare la replica a copia singola

Quando si crea una regola ILM per creare copie replicate, è necessario specificare almeno due copie per un periodo di tempo qualsiasi nelle istruzioni di posizionamento.

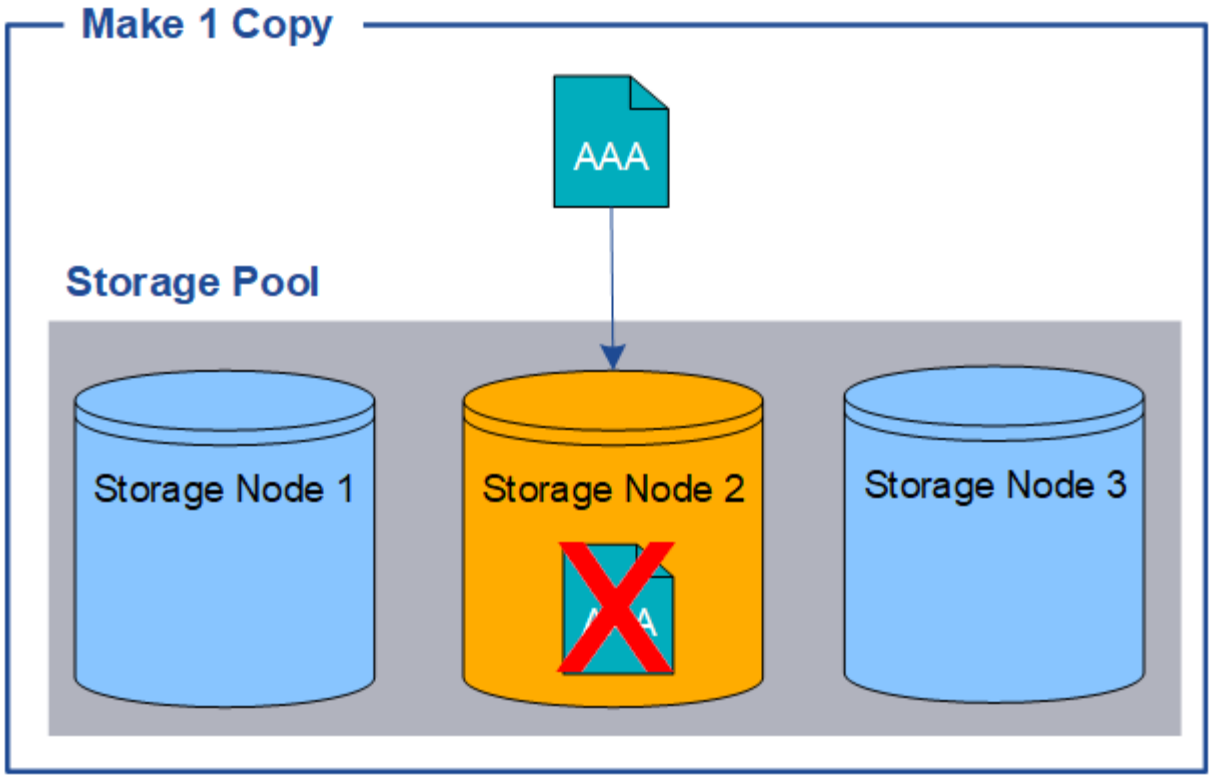
> Non utilizzare una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Nell'esempio seguente, la regola Make 1 Copy ILM specifica che una copia replicata di un oggetto deve

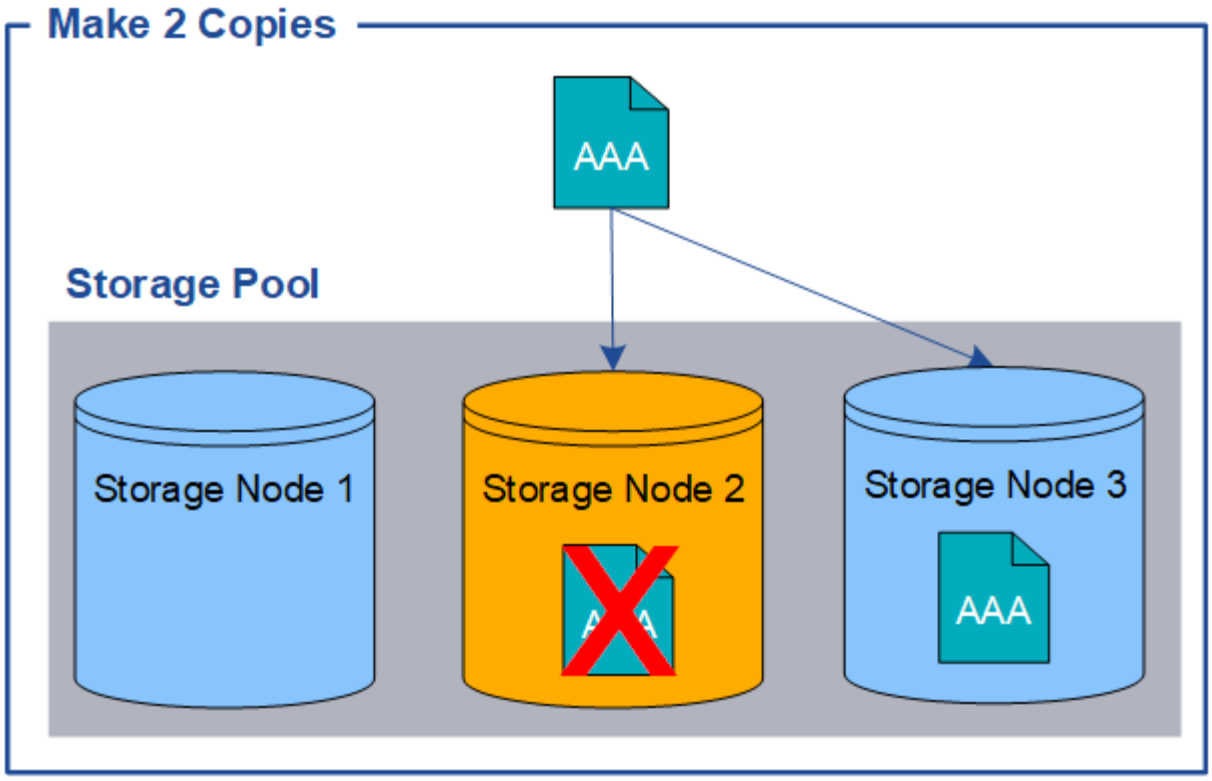
essere inserita in un pool di storage che contiene tre nodi di storage. Quando viene acquisito un oggetto che corrisponde a questa regola, StorageGRID inserisce una singola copia su un solo nodo di storage.



Quando una regola ILM crea una sola copia replicata di un oggetto, l'oggetto diventa inaccessibile quando il nodo di storage non è disponibile. In questo esempio, l'accesso all'oggetto AAA viene temporaneamente perso ogni volta che il nodo di storage 2 non è in linea, ad esempio durante un aggiornamento o un'altra procedura di manutenzione. In caso di guasto del nodo di storage 2, l'oggetto AAA andrà perso completamente.



Per evitare di perdere i dati degli oggetti, è necessario eseguire almeno due copie di tutti gli oggetti che si desidera proteggere con la replica. Se esistono due o più copie, è comunque possibile accedere all'oggetto se un nodo di storage si guasta o non è in linea.



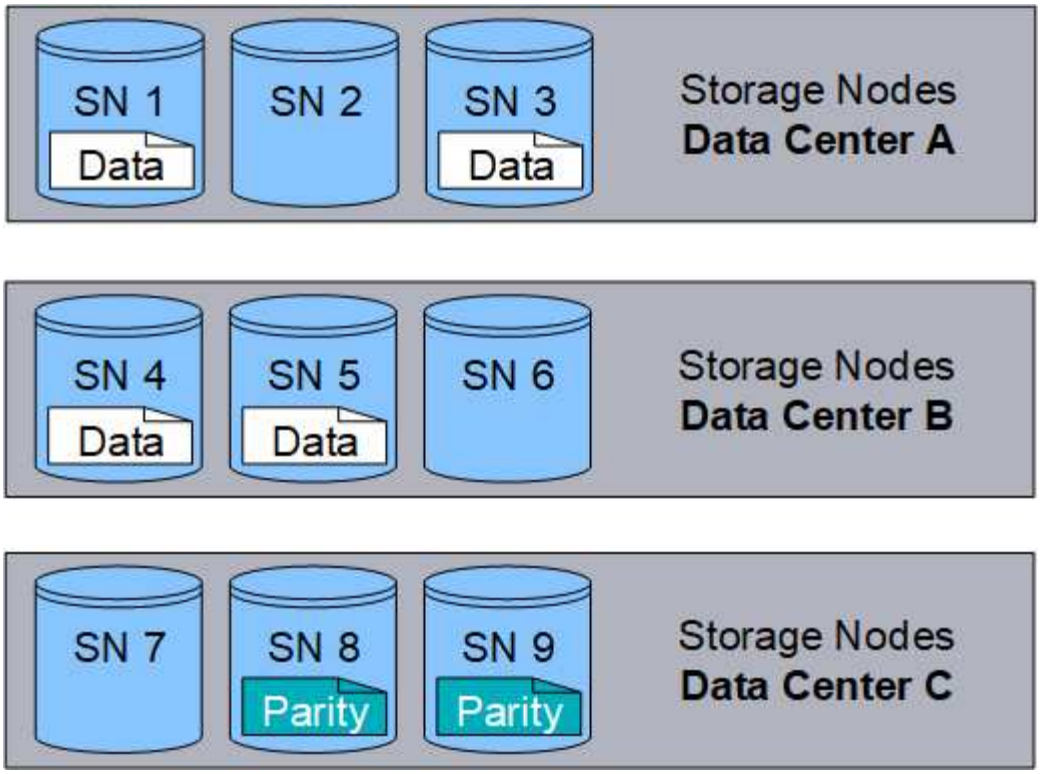
Cos'è la codifica erasure?

L'erasure coding è uno dei due metodi utilizzati da StorageGRID per memorizzare i dati degli oggetti. Quando gli oggetti corrispondono a una regola ILM che utilizza la codifica erasure, vengono suddivisi in frammenti di dati, vengono calcolati ulteriori frammenti di parità e ciascun frammento viene memorizzato in un nodo di storage diverso.

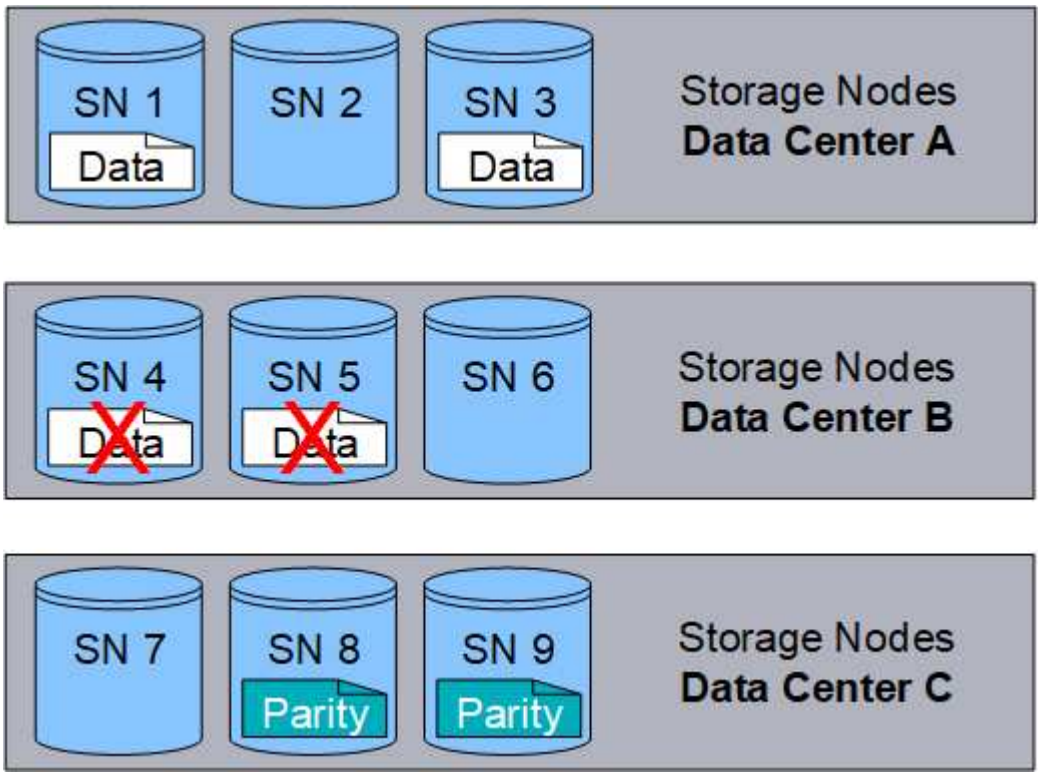
Quando si accede a un oggetto, questo viene riassemblato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità viene corrotto o perso, l'algoritmo di erasure coding può ricreare quel frammento utilizzando un sottoinsieme dei dati rimanenti e dei frammenti di parità.

Quando crei regole ILM, StorageGRID crea profili di erasure coding in grado di supportarle. Puoi visualizzare un elenco di profili di erasure coding, "rinominare un profilo con erasure coding", o. "Disattivare un profilo di erasure coding se non è attualmente utilizzato in nessuna regola ILM".

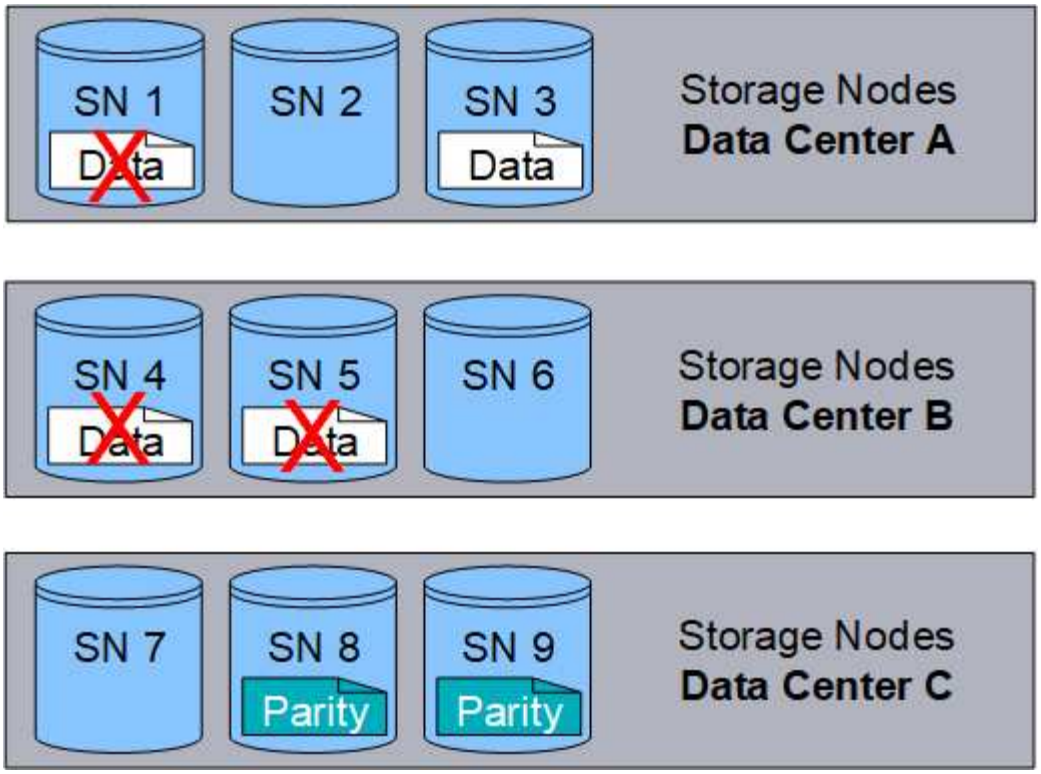
Nell'esempio seguente viene illustrato l'utilizzo di un algoritmo di erasure coding sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di erasure coding 4+2. Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati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



Lo schema di erasure coding 4+2 può essere configurato in vari modi. Ad esempio, è possibile configurare un pool di storage a sito singolo che contiene sei nodi di storage. Per "protezione contro la perdita di sito", È possibile utilizzare un pool di storage contenente tre siti con tre nodi di storage in ogni sito. Un oggetto può essere recuperato finché quattro dei sei frammenti (dati o parità) rimangono disponibili. È possibile perdere fino a due frammenti senza perdita dei dati dell'oggetto. In caso di perdita di un intero sito, l'oggetto può comunque essere recuperato o riparato, purché tutti gli altri frammenti rimangano accessibili.



In caso di perdita di più di due nodi di storage, l'oggetto non può essere recuperato.



Informazioni correlate

- "Cos'è la replica"
- "Che cos'è un pool di storage"
- "Cosa sono gli schemi di erasure coding"
- "Rinominare un profilo con erasure coding"
- "Disattivare un profilo di erasure coding"

Cosa sono gli schemi di erasure coding?

Gli schemi di erasure coding controllano il numero di frammenti di dati e il numero di frammenti di parità creati per ciascun oggetto.

Quando si configura il profilo di erasure coding per una regola ILM, si seleziona uno schema di erasure coding disponibile in base al numero di nodi e siti storage che compongono il pool di storage che si intende utilizzare.

Il sistema StorageGRID utilizza l'algoritmo di erasure coding Reed-Solomon. L'algoritmo suddivide un oggetto in `k` frammenti di dati e calcolo `m` frammenti di parità. Il `k + m = n` i frammenti sono sparsi `n` Nodi di storage per la protezione dei dati. Un oggetto può sostenere fino a. `m` frammenti persi o corrotti. Per recuperare o riparare un oggetto, `k` sono necessari frammenti.

Quando si seleziona il pool di storage da utilizzare per una regola che crea una copia con codice di cancellazione, utilizzare le seguenti linee guida per i pool di storage:

- Il pool di storage deve includere tre o più siti, o esattamente un sito.

  Non è possibile utilizzare la codifica di cancellazione se il pool di storage include due siti.

  - Schemi di erasure coding per pool di storage contenenti tre o più siti

    - Schemi di erasure coding per pool di storage a sito singolo
- Non utilizzare un pool di storage che includa il sito predefinito, tutti i siti.
- Il pool di storage deve includere almeno `k+m +1` Nodi di storage in grado di memorizzare i dati di oggetti.

> I nodi di storage possono essere configurati durante l'installazione in modo da contenere solo metadati di oggetti e non dati di oggetti. Per ulteriori informazioni, vedere "Tipi di nodi storage".

Il numero minimo di nodi di storage richiesto è `k+m`. Tuttavia, disporre di almeno un nodo di storage aggiuntivo può contribuire a prevenire gli errori di acquisizione o i backlog ILM se un nodo di storage richiesto non è temporaneamente disponibile.

L'overhead dello storage di uno schema di erasure coding viene calcolato dividendo il numero di frammenti di parità (`m`) in base al numero di frammenti di dati (`k`). È possibile utilizzare l'overhead dello storage per calcolare la quantità di spazio su disco richiesta da ciascun oggetto con codifica di cancellazione:

```
disk space = object size + (object size * storage overhead)
```

Ad esempio, se si memorizza un oggetto da 10 MB utilizzando lo schema 4+2 (con un overhead dello storage del 50%), l'oggetto consuma 15 MB di storage grid. Se si memorizza lo stesso oggetto da 10 MB utilizzando lo schema 6+2 (con un overhead dello storage del 33%), l'oggetto consuma circa 13.3 MB.

Selezionare lo schema di erasure coding con il valore totale più basso di `k+m` che soddisfa le tue esigenze. Gli schemi di erasure coding con un numero inferiore di frammenti sono in generale più efficienti dal punto di vista computazionale, in quanto vengono creati e distribuiti (o recuperati) meno frammenti per oggetto, possono mostrare performance migliori grazie alle maggiori dimensioni dei frammenti e possono richiedere l'aggiunta di un numero inferiore di nodi in un'espansione quando è necessario più storage. Per informazioni sulla pianificazione di un'espansione dello storage, consultare la "Istruzioni per espandere StorageGRID".)

Schemi di erasure coding per pool di storage contenenti tre o più siti

La seguente tabella descrive gli schemi di erasure coding attualmente supportati da StorageGRID per i pool di storage che includono tre o più siti. Tutti questi schemi offrono una protezione contro la perdita di sito. È possibile perdere un sito e l'oggetto sarà ancora accessibile.

Per gli schemi di erasure coding che forniscono la protezione dalla perdita di sito, il numero consigliato di nodi di storage nel pool di storage supera `k+m +1` Perché ogni sito richiede un minimo di tre nodi di storage.

Schema di erasure coding (*k+m*)	Numero minimo di siti implementati	Numero consigliato di nodi di storage in ogni sito	Numero totale consigliato di nodi di storage	Protezione contro le perdite di sito?	Overhead dello storage
4+2	3	3	9	Sì	50%
6+2	4	3	12	Sì	33%
8+2	5	3	15	Sì	25%
6+3	3	4	12	Sì	50%

Schema di erasure coding (*k+m*)	Numero minimo di siti implementati	Numero consigliato di nodi di storage in ogni sito	Numero totale consigliato di nodi di storage	Protezione contro le perdite di sito?	Overhead dello storage
9+3	4	4	16	Sì	33%
2+1	3	3	9	Sì	50%
4+1	5	3	15	Sì	25%
6+1	7	3	21	Sì	17%
7+5	3	5	15	Sì	71%

> StorageGRID richiede un minimo di tre nodi di storage per sito. Per utilizzare lo schema 7+5, ogni sito richiede almeno quattro nodi di storage. Si consiglia di utilizzare cinque nodi di storage per sito.

Quando si seleziona uno schema di erasure coding che fornisce la protezione del sito, bilanciare l'importanza relativa dei seguenti fattori:

- **Numero di frammenti**: Le prestazioni e la flessibilità di espansione sono generalmente migliori quando il numero totale di frammenti è inferiore.
- **Fault tolerance**: La tolleranza di errore viene aumentata con più segmenti di parità (cioè, quando `m` ha un valore più elevato).
- **Traffico di rete**: Durante il ripristino da errori, utilizzando uno schema con più frammenti (ovvero, un totale più elevato per `k+m`) crea più traffico di rete.
- **Overhead dello storage**: Gli schemi con overhead più elevato richiedono più spazio di storage per oggetto.

Ad esempio, quando si decide tra uno schema 4+2 e uno schema 6+3 (entrambi con un overhead dello storage del 50%), selezionare lo schema 6+3 se è richiesta una fault tolerance aggiuntiva. Selezionare lo schema 4+2 se le risorse di rete sono limitate. Se tutti gli altri fattori sono uguali, selezionare 4+2 perché il numero totale di frammenti è inferiore.

> In caso di dubbi sul programma da utilizzare, selezionare 4+2 o 6+3 oppure contattare il supporto tecnico.

Schemi di erasure coding per pool di storage a sito singolo

Un pool di storage a sito singolo supporta tutti gli schemi di erasure coding definiti per tre o più siti, a condizione che il sito disponga di un numero sufficiente di nodi di storage.

Il numero minimo di nodi di storage richiesto è `k+m`, ma un pool di storage con `k+m +1` Si consiglia di utilizzare i nodi di storage. Ad esempio, lo schema di erasure coding 2+1 richiede un pool di storage con almeno tre nodi di storage, ma si consiglia di utilizzare quattro nodi di storage.

Schema di erasure coding (*k*+*m*)	Numero minimo di nodi di storage	Numero consigliato di nodi di storage	Overhead dello storage
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Vantaggi, svantaggi e requisiti per l'erasure coding

Prima di decidere se utilizzare la replica o la cancellazione del codice per proteggere i dati degli oggetti dalla perdita, è necessario comprendere i vantaggi, gli svantaggi e i requisiti per la cancellazione del codice.

Vantaggi dell'erasure coding

Rispetto alla replica, l'erasure coding offre maggiore affidabilità, disponibilità ed efficienza dello storage.

- **Affidabilità**: L'affidabilità viene misurata in termini di tolleranza agli errori, ovvero il numero di guasti simultanei che possono essere sostenuti senza perdita di dati. Con la replica, più copie identiche vengono memorizzate su nodi diversi e tra siti diversi. Con la codifica erasure, un oggetto viene codificato in dati e frammenti di parità e distribuito su molti nodi e siti. Questa dispersione fornisce protezione da guasti sia a livello di sito che di nodo. Rispetto alla replica, l'erasure coding offre una maggiore affidabilità a costi di storage comparabili.
- **Disponibilità**: La disponibilità può essere definita come la capacità di recuperare oggetti se i nodi di storage si guastano o diventano inaccessibili. Rispetto alla replica, l'erasure coding offre una maggiore disponibilità a costi di storage comparabili.
- **Efficienza dello storage**: Per livelli simili di disponibilità e affidabilità, gli oggetti protetti tramite erasure coding consumano meno spazio su disco rispetto agli stessi oggetti se protetti tramite replica. Ad esempio, un oggetto da 10 MB replicato in due siti consuma 20 MB di spazio su disco (due copie), mentre un oggetto che è sottoposto a erasure coding in tre siti con uno schema di erasure coding 6+3 consuma solo 15 MB di spazio su disco.

Lo spazio su disco per gli oggetti con codifica in cancellazione viene calcolato come dimensione dell'oggetto più l'overhead dello storage. La percentuale di overhead dello storage è il numero di frammenti di parità diviso per il numero di frammenti di dati.

Svantaggi della codifica erasure

Rispetto alla replica, l'erasure coding presenta i seguenti svantaggi:

- È consigliato un maggior numero di siti e nodi di storage, a seconda dello schema di erasure coding. Al contrario, se si replicano i dati degli oggetti, è necessario un solo nodo di storage per ogni copia. Vedere "Schemi di erasure coding per pool di storage contenenti tre o più siti" e. "Schemi di erasure coding per pool di storage a sito singolo".
- Aumento dei costi e della complessità delle espansioni dello storage. Per espandere un'implementazione che utilizza la replica, è necessario aggiungere capacità di storage in ogni posizione in cui vengono eseguite le copie a oggetti. Per espandere un'implementazione che utilizza il erasure coding, è necessario prendere in considerazione sia lo schema di erasure coding in uso sia la capacità dei nodi di storage esistenti. Ad esempio, se si attende che i nodi esistenti siano pieni al 100%, è necessario aggiungere almeno `k+m` I nodi di storage, ma se si espandono quando i nodi esistenti sono pieni al 70%, è possibile aggiungere due nodi per sito e massimizzare la capacità di storage utilizzabile. Per ulteriori informazioni, vedere "Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione".
- L'utilizzo di erasure coding in siti distribuiti geograficamente aumenta le latenze di recupero. I frammenti di oggetto per un oggetto sottoposto a erasure coding e distribuito tra i siti remoti richiedono più tempo per il recupero su connessioni WAN rispetto a un oggetto replicato e disponibile in locale (lo stesso sito a cui si connette il client).
- Quando si utilizza il erasure coding in siti distribuiti geograficamente, il traffico di rete WAN è più elevato per recuperi e riparazioni, in particolare per oggetti recuperati di frequente o per riparazioni di oggetti su connessioni di rete WAN.
- Quando si utilizza l'erasure coding tra siti, il throughput massimo degli oggetti diminuisce drasticamente con l'aumentare della latenza di rete tra siti. Questa diminuzione è dovuta alla corrispondente diminuzione del throughput di rete TCP, che influisce sulla velocità con cui il sistema StorageGRID può memorizzare e recuperare frammenti di oggetti.
- Maggiore utilizzo delle risorse di calcolo.

Quando utilizzare la codifica di cancellazione

L'erasure coding è più adatto ai seguenti requisiti:

- Oggetti di dimensioni superiori a 1 MB.

L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

- Storage a lungo termine o a freddo per contenuti recuperati raramente.
- Elevata disponibilità e affidabilità dei dati.
- Protezione contro guasti completi del sito e dei nodi.
- Efficienza dello storage.
- Implementazioni a singolo sito che richiedono una protezione dei dati efficiente con una sola copia codificata in cancellazione anziché più copie replicate.

- Implementazioni multi-sito in cui la latenza tra siti è inferiore a 100 ms.

Come viene determinata la conservazione degli oggetti

StorageGRID offre agli amministratori di grid e ai singoli utenti tenant opzioni per specificare la durata della memorizzazione degli oggetti. In generale, tutte le istruzioni di conservazione fornite da un utente tenant hanno la precedenza sulle istruzioni di conservazione fornite dall'amministratore della griglia.

Come gli utenti tenant controllano la conservazione degli oggetti

Gli utenti del tenant possono controllare per quanto tempo i propri oggetti vengono memorizzati in StorageGRID in tre modi principali:

- Se l'impostazione globale S3 Object Lock è attivata per la griglia, gli utenti del tenant 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 ciascuna versione dell'oggetto aggiunta a quel bucket.
  - Una versione dell'oggetto soggetta a blocco legale non può essere eliminata da 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 blocco oggetti S3 abilitato vengono conservati da ILM "per sempre". Tuttavia, una volta raggiunta la data di conservazione, una versione dell'oggetto può essere eliminata da una richiesta client o dalla scadenza del ciclo di vita del bucket. Vedere "Gestire gli oggetti con S3 Object Lock".
- Gli utenti del tenant 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 memorizza un oggetto fino a quando non viene soddisfatta la data o il numero di giorni specificati nell'azione di scadenza, a meno che il client non elimini prima l'oggetto. Vedere "Creare la configurazione del ciclo di vita S3".
- Un client S3 o Swift può emettere una richiesta di eliminazione degli oggetti. StorageGRID assegna sempre la priorità alle richieste di eliminazione dei client sul ciclo di vita del bucket S3 o ILM quando si determina se eliminare o conservare un oggetto.

Come gli amministratori della griglia controllano la conservazione degli oggetti

Gli amministratori della griglia utilizzano le istruzioni di posizionamento ILM per controllare la durata della memorizzazione degli oggetti. Quando un oggetto viene associato da una regola ILM, StorageGRID memorizza tali oggetti fino allo scadere dell'ultimo periodo di tempo della regola ILM. Gli oggetti vengono conservati a tempo indeterminato se per le istruzioni di posizionamento viene specificato "per sempre".

Indipendentemente da chi controlla la durata della conservazione degli oggetti, le impostazioni ILM determinano i tipi di copie degli oggetti (replicate o sottoposte a erasure coding) archiviati e la posizione delle copie (nodi storage, pool di cloud storage o nodi di archivio).

Come interagiscono il ciclo di vita del bucket S3 e ILM

Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti che corrispondono al filtro del ciclo di vita. Di conseguenza, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni ILM per il posizionamento dell'oggetto.

Esempi di conservazione degli oggetti

Per comprendere meglio le interazioni tra blocco oggetti S3, impostazioni del ciclo di vita del bucket, richieste di eliminazione client e ILM, considerare gli esempi seguenti.

Esempio 1: Il ciclo di vita del bucket S3 mantiene gli oggetti più a lungo di ILM

ILM

Memorizzazione di due copie per 1 anno (365 giorni)

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Risultato

StorageGRID memorizza l'oggetto per 730 giorni. StorageGRID utilizza le impostazioni del ciclo di vita del bucket per determinare se eliminare o conservare un oggetto.

> Se il ciclo di vita del bucket specifica che gli oggetti devono essere mantenuti più a lungo di quanto specificato da ILM, StorageGRID continua a utilizzare le istruzioni di posizionamento ILM per determinare il numero e il tipo di copie da memorizzare. In questo esempio, due copie dell'oggetto continueranno ad essere memorizzate in StorageGRID dai giorni 366 al 730.

Esempio 2: Il ciclo di vita del bucket S3 scade gli oggetti prima di ILM

ILM

Memorizzazione di due copie per 2 anni (730 giorni)

Ciclo di vita del bucket

Scadenza oggetti in 1 anno (365 giorni)

Risultato

StorageGRID elimina entrambe le copie dell'oggetto dopo il giorno 365.

Esempio 3: L'eliminazione del client sovrascrive il ciclo di vita del bucket e ILM

ILM

Memorizzazione di due copie sui nodi storage "per sempre"

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Richiesta di eliminazione del client

Emesso il giorno 400

Risultato

StorageGRID elimina entrambe le copie dell'oggetto il giorno 400 in risposta alla richiesta di eliminazione del client.

Esempio 4: S3 Object Lock sovrascrive la richiesta di eliminazione del client

Blocco oggetti S3

Retain-until-date per una versione a oggetti è 2026-03-31. Non è in vigore una conservazione a fini giudiziari.

Regola ILM conforme

Memorizzazione di due copie sui nodi storage "per sempre"

Richiesta di eliminazione del client

Pubblicato il 2024-03-31

Risultato

StorageGRID non eliminerà la versione dell'oggetto perché la data di conservazione è ancora a 2 anni di distanza.

Modalità di eliminazione degli oggetti

StorageGRID può eliminare gli oggetti in risposta diretta a una richiesta del client o automaticamente in conseguenza della scadenza di un ciclo di vita del bucket S3 o dei requisiti della policy ILM. La comprensione dei diversi modi in cui è possibile eliminare gli oggetti e del modo in cui StorageGRID gestisce le richieste di eliminazione può aiutare a gestire gli oggetti in modo più efficace.

StorageGRID può utilizzare uno dei due metodi per eliminare gli oggetti:

- Eliminazione sincrona: Quando StorageGRID riceve una richiesta di eliminazione del client, tutte le copie degli oggetti vengono rimosse immediatamente. Il client viene informato che l'eliminazione è stata eseguita correttamente dopo la rimozione delle copie.
- Gli oggetti vengono messi in coda per l'eliminazione: Quando StorageGRID riceve una richiesta di eliminazione, l'oggetto viene messo in coda per l'eliminazione e il client viene immediatamente informato dell'avvenuta eliminazione. Le copie degli oggetti vengono rimosse in seguito dall'elaborazione ILM in background.

Quando si eliminano gli oggetti, StorageGRID utilizza il metodo che ottimizza le performance di eliminazione, riduce al minimo i potenziali backlog di eliminazione e libera lo spazio più rapidamente.

La tabella riassume quando StorageGRID utilizza ciascun metodo.

Metodo di eliminazione	Se utilizzato
Gli oggetti vengono messi in coda per l'eliminazione	Quando **una delle seguenti condizioni** è vera: • L'eliminazione automatica degli oggetti è stata attivata da uno dei seguenti eventi: ◦ Viene raggiunta la data di scadenza o il numero di giorni nella configurazione del ciclo di vita di un bucket S3. ◦ È trascorso l'ultimo periodo di tempo specificato in una regola ILM. **Nota:** gli oggetti in un bucket che ha attivato il blocco oggetti S3 non possono essere cancellati se sono in stato di conservazione legale o se è stato specificato un periodo di conservazione fino alla data, ma non ancora soddisfatto. • Un client S3 o Swift richiede l'eliminazione e una o più di queste condizioni sono vere: ◦ Impossibile eliminare le copie entro 30 secondi perché, ad esempio, una posizione dell'oggetto non è temporaneamente disponibile. ◦ Le code di eliminazione in background sono inattive.
Gli oggetti vengono rimossi immediatamente (eliminazione sincrona)	Quando un client S3 o Swift effettua una richiesta di eliminazione e **tutte** le seguenti condizioni sono soddisfatte: • Tutte le copie possono essere rimosse entro 30 secondi. • Le code di eliminazione in background contengono oggetti da elaborare.

Quando i client S3 o Swift effettuano richieste di eliminazione, StorageGRID inizia aggiungendo oggetti alla coda di eliminazione. Passa quindi all'eliminazione sincrona. Assicurarsi che la coda di eliminazione in background disponga di oggetti da elaborare consente a StorageGRID di elaborare le eliminazioni in modo più efficiente, in particolare per i client con bassa concorrenza, evitando al contempo i backlog di eliminazione dei client.

Tempo necessario per eliminare gli oggetti

Il modo in cui StorageGRID elimina gli oggetti può influire sulle prestazioni del sistema:

- Quando StorageGRID esegue l'eliminazione sincrona, StorageGRID può impiegare fino a 30 secondi per restituire un risultato al client. Ciò significa che l'eliminazione può sembrare più lenta, anche se le copie vengono effettivamente rimosse più rapidamente di quanto non lo siano quando StorageGRID mette in coda gli oggetti per l'eliminazione.
- Se si sta monitorando attentamente le prestazioni di eliminazione durante un'eliminazione in blocco, è possibile notare che la velocità di eliminazione sembra essere lenta dopo l'eliminazione di un certo numero di oggetti. Questa modifica si verifica quando StorageGRID passa dall'accodamento di oggetti per l'eliminazione all'eliminazione sincrona. La riduzione apparente del tasso di eliminazione non significa che le copie degli oggetti vengano rimosse più lentamente. Al contrario, indica che, in media, lo spazio viene liberato più rapidamente.

Se si eliminano grandi quantità di oggetti e la priorità è liberare spazio rapidamente, considerare l'utilizzo di una richiesta client per eliminare gli oggetti piuttosto che eliminarli utilizzando ILM o altri metodi. In generale, lo spazio viene liberato più rapidamente quando l'eliminazione viene eseguita dai client perché StorageGRID può

utilizzare l'eliminazione sincrona.

La quantità di tempo necessaria per liberare spazio dopo l'eliminazione di un oggetto dipende da diversi fattori:

- Se le copie degli oggetti vengono rimosse in modo sincrono o messe in coda per la rimozione in un secondo momento (per le richieste di eliminazione del client).
- Altri fattori, come il numero di oggetti nella griglia o la disponibilità di risorse della griglia quando le copie degli oggetti vengono messe in coda per la rimozione (sia per le eliminazioni dei client che per altri metodi).

Modalità di eliminazione degli oggetti con versione S3

Quando il controllo delle versioni è attivato per un bucket S3, StorageGRID segue il comportamento di Amazon S3 quando risponde alle richieste di eliminazione, sia che provengano da un client S3, dalla scadenza di un ciclo di vita del bucket S3 o dai requisiti della policy ILM.

Quando gli oggetti sono in versione, le richieste di eliminazione degli oggetti non eliminano la versione corrente dell'oggetto e non liberano spazio. Invece, una richiesta di eliminazione di un oggetto crea un marcatore di eliminazione di zero byte come versione corrente dell'oggetto, rendendo la versione precedente dell'oggetto "non corrente". Un marcatore di eliminazione di un oggetto diventa un marcatore di eliminazione di un oggetto scaduto quando è la versione corrente e non ci sono versioni non correnti.

Anche se l'oggetto non è stato rimosso, StorageGRID si comporta come se la versione corrente dell'oggetto non fosse più disponibile. Le richieste a quell'oggetto restituiscono 404 non trovato. Tuttavia, poiché i dati dell'oggetto non correnti non sono stati rimossi, le richieste che specificano una versione non corrente dell'oggetto possono avere successo.

Per liberare spazio quando si eliminano gli oggetti con versione o per rimuovere i marcatori di eliminazione, utilizzare una delle seguenti opzioni:

- **Richiesta del client S3**: Specificare l'ID della versione dell'oggetto nella richiesta di ELIMINAZIONE dell'oggetto S3 (`DELETE /object?versionId=ID`). Tenere presente che questa richiesta rimuove solo le copie degli oggetti per la versione specificata (le altre versioni occupano ancora spazio).
- **Ciclo di vita del bucket**: Utilizzare `NoncurrentVersionExpiration` azione nella configurazione del ciclo di vita del bucket. Quando viene raggiunto il numero di giorni non correnti specificato, StorageGRID rimuove in modo permanente tutte le copie delle versioni degli oggetti non correnti. Queste versioni degli oggetti non possono essere ripristinate.

  Il `NewerNoncurrentVersions` L'azione nella configurazione del ciclo di vita del bucket specifica il numero di versioni non correnti conservate in un bucket S3 con versione. Se sono presenti più versioni non aggiornate di `NewerNoncurrentVersions` Specifica, StorageGRID rimuove le versioni precedenti quando il valore NoncurrentDays è scaduto. Il `NewerNoncurrentVersions` Threshold sovrascrive le regole del ciclo di vita fornite da ILM, il che significa che un oggetto non corrente con una versione all'interno di `NewerNoncurrentVersions` La soglia viene mantenuta se ILM richiede la sua eliminazione.

  Per rimuovere gli oggetti scaduti, eliminare i contrassegni utilizzando `Expiration` azione con uno dei seguenti tag: `ExpiredObjectDeleteMarker`, `Days`, o. `Date`.

- **ILM**: "Clonazione di una policy attiva" E aggiungere due regole ILM alla nuova policy:
  - Prima regola: Utilizzare "ora non corrente" come ora di riferimento per far corrispondere le versioni non correnti dell'oggetto. Poll "Fase 1 (immettere i dettagli) della procedura guidata Crea una regola ILM", Selezionare **Sì** per la domanda "applicare questa regola solo alle versioni di oggetti precedenti (nei

bucket S3 con versione abilitata)?"

- Seconda regola: Utilizzare **Ingest Time** per corrispondere alla versione corrente. La regola "ora non corrente" deve essere visualizzata nel criterio sopra la regola **ora acquisizione**.

> ILM non può essere utilizzato per rimuovere gli indicatori di eliminazione dell'oggetto corrente. Utilizzare una richiesta client S3 o un ciclo di vita bucket S3 per rimuovere i marcatori di eliminazione degli oggetti correnti.

- **Elimina oggetti nel bucket**: Utilizza il gestore tenant per "elimina tutte le versioni degli oggetti", inclusi i marcatori di cancellazione, da un bucket.

  Quando un oggetto con versione viene eliminato, StorageGRID crea un marcatore di eliminazione a byte zero come versione corrente dell'oggetto. Tutti gli oggetti e i marcatori di eliminazione devono essere rimossi prima di poter eliminare un bucket in versione.

  - I marcatori di eliminazione creati in StorageGRID 11,7 o versioni precedenti possono essere rimossi solo tramite richieste client S3, ma non tramite ILM, regole del ciclo di vita bucket o Elimina oggetti nelle operazioni bucket.
  - I marcatori di eliminazione da un bucket creato in StorageGRID 11,8 o versioni successive possono essere rimossi da ILM, regole del ciclo di vita bucket, Elimina oggetti nelle operazioni bucket o un'eliminazione client S3 esplicita. I marcatori di eliminazione scaduti in StorageGRID 11,8 o versioni successive devono essere rimossi dalle regole del ciclo di vita del bucket o da una richiesta client S3 esplicita con un ID versione specificato.

Informazioni correlate

- "UTILIZZARE L'API REST S3"
- "Esempio 4: Regole ILM e policy per gli oggetti con versione S3"

Creare e assegnare i gradi di storage

I gradi di storage identificano il tipo di storage utilizzato da un nodo di storage. È possibile creare gradi di storage se si desidera che le regole ILM posizionino determinati oggetti su determinati nodi di storage.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Quando si installa StorageGRID per la prima volta, il livello di storage **predefinito** viene assegnato automaticamente a ogni nodo di storage del sistema. In base alle esigenze, è possibile definire gradazioni di storage personalizzate e assegnarle a diversi nodi di storage.

L'utilizzo di storage grades personalizzati consente di creare pool di storage ILM che contengono solo un tipo specifico di Storage Node. Ad esempio, è possibile che alcuni oggetti vengano memorizzati nei nodi di storage più veloci, ad esempio le appliance di storage all-flash StorageGRID.

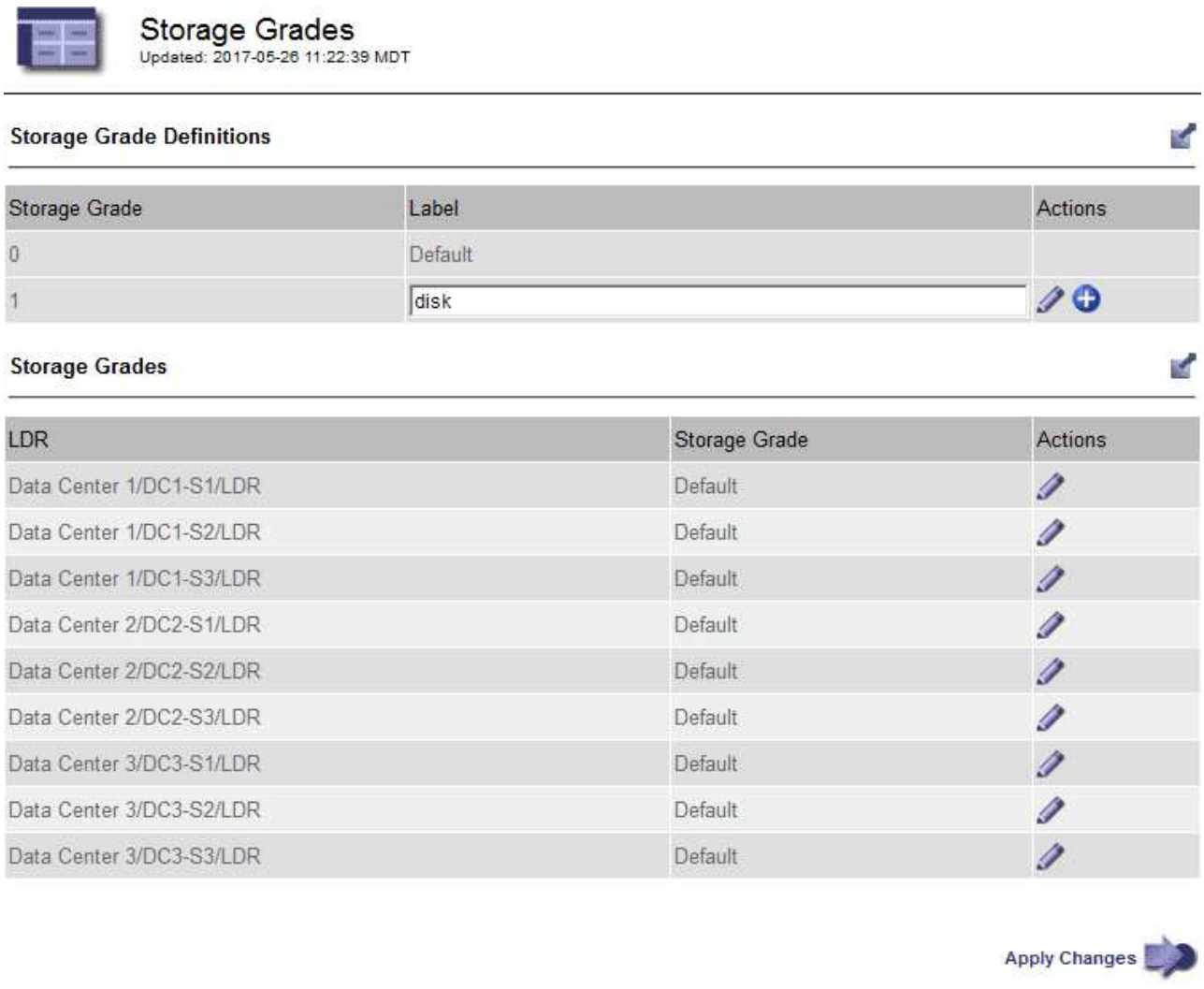
> I nodi di storage possono essere configurati durante l'installazione in modo da contenere solo metadati di oggetti e non dati di oggetti. Ai nodi di storage con soli metadati non può essere assegnato un livello di storage. Per ulteriori informazioni, vedere "Tipi di nodi storage".

Se il livello di storage non è un problema (ad esempio, tutti i nodi storage sono identici), è possibile saltare questa procedura e utilizzare la selezione **include all storage grades** (include tutti i livelli di storage) per il livello di storage "creare pool di storage". L'utilizzo di questa selezione garantisce che il pool di storage includa ogni nodo di storage del sito, indipendentemente dal suo livello di storage.

> Non creare più storage di quanto necessario. Ad esempio, non creare un livello di storage per ciascun nodo di storage. Assegnare invece ogni livello di storage a due o più nodi. I gradi di storage assegnati a un solo nodo possono causare backlog ILM se tale nodo non è più disponibile.

Fasi

1. Selezionare **ILM** > **Storage grades**.
2. Definire i livelli di storage personalizzati:
   a. Per ogni livello di storage personalizzato che si desidera aggiungere, selezionare **Inserisci** per aggiungere una riga.
   b. Inserire un'etichetta descrittiva.



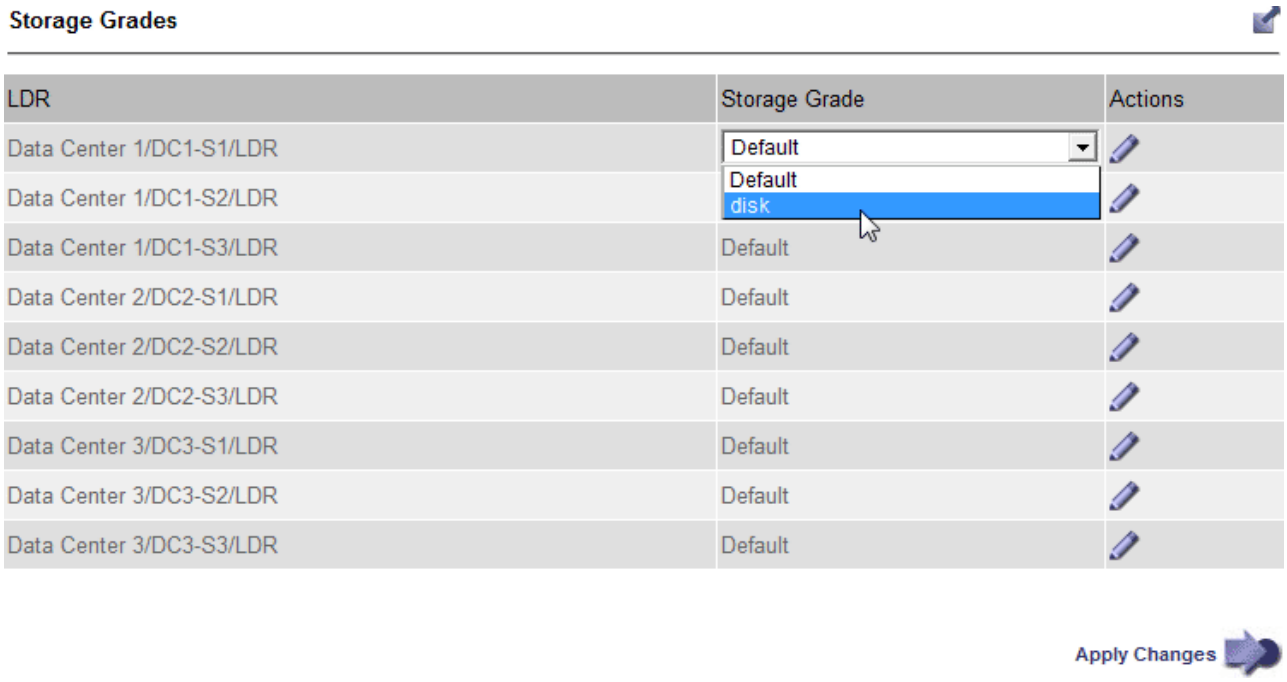
   c. Selezionare **Applica modifiche**.
   d. Se si desidera modificare un'etichetta salvata, selezionare **Modifica** E selezionare **Applica modifiche**.

Non puoi eliminare i gradi di storage.

3. Assegnare nuovi gradi di storage ai nodi di storage:

   a. Individuare il nodo di storage nell'elenco LDR e selezionare l'icona **Edit** .

   b. Selezionare il livello di storage appropriato dall'elenco.



Assegnare un grado di storage a un nodo di storage specifico una sola volta. Un nodo di storage recuperato dal guasto mantiene il livello di storage assegnato in precedenza. Non modificare questa assegnazione dopo l'attivazione della policy ILM. Se l'assegnazione viene modificata, i dati vengono memorizzati in base al nuovo livello di storage.

   a. Selezionare **Applica modifiche**.

Utilizzare i pool di storage

Che cos'è un pool di storage?

Un pool di storage è un raggruppamento logico di nodi di storage o nodi di archivio.

Quando si installa StorageGRID, viene creato automaticamente un pool di storage per sito. È possibile configurare ulteriori pool di storage in base alle esigenze di storage.

È possibile configurare i nodi di storage durante l'installazione in modo che contengano dati di oggetti e metadati di oggetti o solo metadati di oggetti. I nodi di storage solo metadati non possono essere utilizzati nei pool di storage. Per ulteriori informazioni, vedere "Tipi di nodi storage".

Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura. Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità.

I pool di storage hanno due attributi:

- **Storage grade**: Per i nodi di storage, le performance relative dello storage di backup.
- **Sito**: Il data center in cui verranno memorizzati gli oggetti.

I pool di storage vengono utilizzati nelle regole ILM per determinare dove sono memorizzati i dati degli oggetti e il tipo di storage utilizzato. Quando si configurano le regole ILM per la replica, si selezionano uno o più pool di storage che includono nodi di storage o nodi di archivio. Quando crei profili di erasure coding, seleziona un pool di storage che include nodi storage.

Linee guida per la creazione di pool di storage

Configurare e utilizzare i pool di storage per proteggersi dalla perdita di dati distribuendo i dati su più siti. Le copie replicate e le copie con codice di cancellazione richiedono diverse configurazioni del pool di storage.

Vedere "Esempi di attivazione della protezione dalle perdite di sito mediante la replica e la cancellazione del codice".

Linee guida per tutti i pool di storage

- Le configurazioni del pool di storage sono il più semplici possibile. Non creare più pool di storage del necessario.
- Creare pool di storage con il maggior numero possibile di nodi. Ogni pool di storage deve contenere due o più nodi. Un pool di storage con nodi insufficienti può causare backlog ILM se un nodo diventa non disponibile.
- Evitare di creare o utilizzare pool di storage che si sovrappongono (contenenti uno o più degli stessi nodi). Se i pool di storage si sovrappongono, è possibile che più di una copia dei dati dell'oggetto venga salvata sullo stesso nodo.
- In generale, non utilizzare il pool di storage All Storage Node (StorageGRID 11.6 e versioni precedenti) o il sito All Sites. Questi elementi vengono aggiornati automaticamente per includere i nuovi siti aggiunti in un'espansione, il che potrebbe non essere il comportamento desiderato.

Linee guida per i pool di storage utilizzati per le copie replicate

- Per la protezione contro la perdita di sito con "replica", specificare uno o più pool di storage specifici del sito in "Istruzioni di posizionamento per ogni regola ILM".

  Un pool di storage viene creato automaticamente per ogni sito durante l'installazione di StorageGRID.

  L'utilizzo di un pool di storage per ciascun sito garantisce che le copie degli oggetti replicate vengano posizionate esattamente dove ci si aspetta (ad esempio, una copia di ogni oggetto in ogni sito per la protezione dalla perdita di sito).

- Se si aggiunge un sito in un'espansione, creare un nuovo pool di storage che contenga solo il nuovo sito. Quindi, "Aggiornare le regole ILM" per controllare quali oggetti sono memorizzati nel nuovo sito.

- Se il numero di copie è inferiore al numero di pool di storage, il sistema distribuisce le copie per bilanciare l'utilizzo del disco tra i pool.
- Se i pool di storage si sovrappongono (contengono gli stessi nodi di storage), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. È necessario assicurarsi che i pool di storage selezionati non contengano gli stessi nodi di storage.

Linee guida per i pool di storage utilizzati per le copie erasure-coded

- Per la protezione contro la perdita di sito con "erasure coding", creare pool di storage composti da almeno tre siti. Se un pool di storage include solo due siti, non è possibile utilizzare tale pool di storage per la cancellazione del codice. Non sono disponibili schemi di erasure coding per un pool di storage con due siti.
- Il numero di nodi e siti di storage contenuti nel pool di storage determina quale "schemi di erasure coding" sono disponibili.
- Se possibile, un pool di storage deve includere un numero superiore al numero minimo di nodi di storage richiesto per lo schema di erasure coding selezionato. Ad esempio, se si utilizza uno schema di erasure coding 6+3, è necessario disporre di almeno nove nodi di storage. Tuttavia, si consiglia di disporre di almeno un nodo di storage aggiuntivo per sito.
- Distribuire i nodi di storage tra i siti nel modo più uniforme possibile. Ad esempio, per supportare uno schema di erasure coding 6+3, configurare un pool di storage che includa almeno tre nodi di storage in tre siti.
- Se si hanno requisiti di throughput elevati, si sconsiglia di utilizzare un pool di storage che include più siti se la latenza di rete tra siti è superiore a 100 ms. Con l'aumentare della latenza, la velocità con cui StorageGRID può creare, posizionare e recuperare frammenti di oggetti diminuisce drasticamente a causa della diminuzione del throughput di rete TCP.

  La diminuzione del throughput influisce sui tassi massimi raggiungibili di acquisizione e recupero degli oggetti (quando vengono selezionati come comportamento di acquisizione bilanciati o rigorosi) o può portare a backlog di coda ILM (quando viene selezionato il doppio commit come comportamento di acquisizione). Vedere "Comportamento di acquisizione delle regole ILM".

  > Se il grid include un solo sito, è impossibile utilizzare il pool di storage All Storage Nodes (StorageGRID 11,6 e versioni precedenti) o il sito predefinito All Sites in un profilo di erasure coding. Questo comportamento impedisce che il profilo diventi non valido se viene aggiunto un secondo sito.

- Non è possibile utilizzare i nodi di archiviazione per i dati con codifica erasure.

Linee guida per i pool di storage utilizzati per le copie archiviate

> Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura. Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità.
>
> Anche l'opzione Cloud Tiering - Simple Storage Service (S3) è obsoleta. Se si utilizza attualmente un nodo di archiviazione con questa opzione, "Migrare gli oggetti in un pool di storage cloud" invece.
>
> Inoltre, è necessario rimuovere i nodi di archiviazione dal criterio ILM attivo in StorageGRID 11,7 o versioni precedenti. La rimozione dei dati degli oggetti memorizzati nei nodi di archiviazione semplificherà gli aggiornamenti futuri. Vedere "Utilizzo delle regole ILM e delle policy ILM".

- Non è possibile creare un pool di storage che includa nodi di storage e nodi di archiviazione. Le copie archiviate richiedono un pool di storage che includa solo i nodi di archiviazione.
- Quando si utilizza un pool di storage che include nodi di archiviazione, è necessario mantenere almeno una copia replicata o codificata in cancellazione su un pool di storage che include nodi di storage.
- Se l'impostazione blocco oggetti S3 globale è attivata e si sta creando una regola ILM conforme, non è possibile utilizzare un pool di storage che include i nodi di archiviazione. Vedere le istruzioni per la gestione degli oggetti con S3 Object Lock.
- Se il tipo di destinazione di un nodo di archiviazione è Cloud Tiering - Simple Storage Service (S3), il nodo di archiviazione deve trovarsi nel proprio pool di storage.

Abilita la protezione contro la perdita di sito

Se l'implementazione di StorageGRID include più di un sito, è possibile utilizzare la replica e la cancellazione del codice con pool di storage configurati in modo appropriato per abilitare la protezione dalla perdita di sito.

La replica e l'erasure coding richiedono diverse configurazioni del pool di storage:

- Per utilizzare la replica per la protezione dalla perdita di sito, utilizzare i pool di storage specifici del sito creati automaticamente durante l'installazione di StorageGRID. Quindi, creare le regole ILM con "istruzioni per il posizionamento" che specificano più pool di storage in modo che una copia di ciascun oggetto venga posizionata in ciascun sito.
- Per utilizzare la codifica erasure per la protezione dalle perdite di sito, "creare pool di storage composti da più siti". Quindi, creare regole ILM che utilizzano un pool di storage costituito da più siti e qualsiasi schema di erasure coding disponibile.

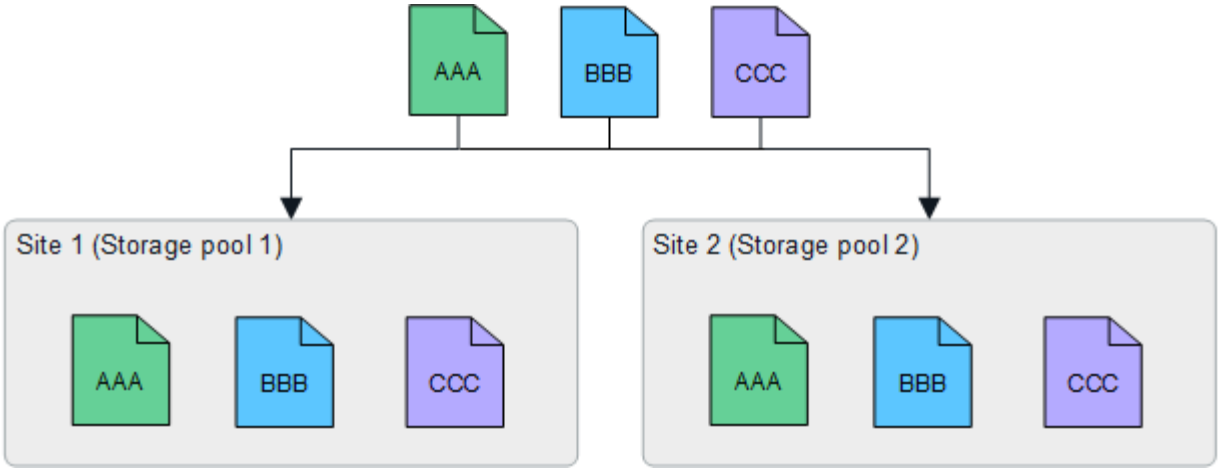
> Quando si configura la distribuzione di StorageGRID per la protezione contro la perdita di siti, è necessario tenere conto anche degli effetti di "opzioni di acquisizione" e. "coerenza".

Esempio di replica

Per impostazione predefinita, viene creato un pool di storage per ciascun sito durante l'installazione di StorageGRID. La disponibilità di pool di storage costituiti da un solo sito consente di configurare le regole ILM che utilizzano la replica per la protezione dalla perdita di sito. In questo esempio:

- Il pool di storage 1 contiene il sito 1
- Il pool di archiviazione 2 contiene il sito 2
- La regola ILM contiene due posizioni:
  - Memorizzare gli oggetti replicando 1 copia nel sito 1
  - Memorizzare gli oggetti replicando 1 copia nel sito 2

Posizionamento delle regole ILM:



In caso di perdita di un sito, le copie degli oggetti sono disponibili nell'altro sito.

Esempio di erasure coding

La disponibilità di pool di storage costituiti da più di un sito per pool di storage consente di configurare le regole ILM che utilizzano la codifica di cancellazione per la protezione dalla perdita di sito. In questo esempio:

- Il pool di storage 1 contiene i siti da 1 a 3
- La regola ILM contiene un unico posizionamento: Memorizzare gli oggetti tramite erasure coding utilizzando uno schema EC 4+2 nello Storage Pool 1, che contiene tre siti

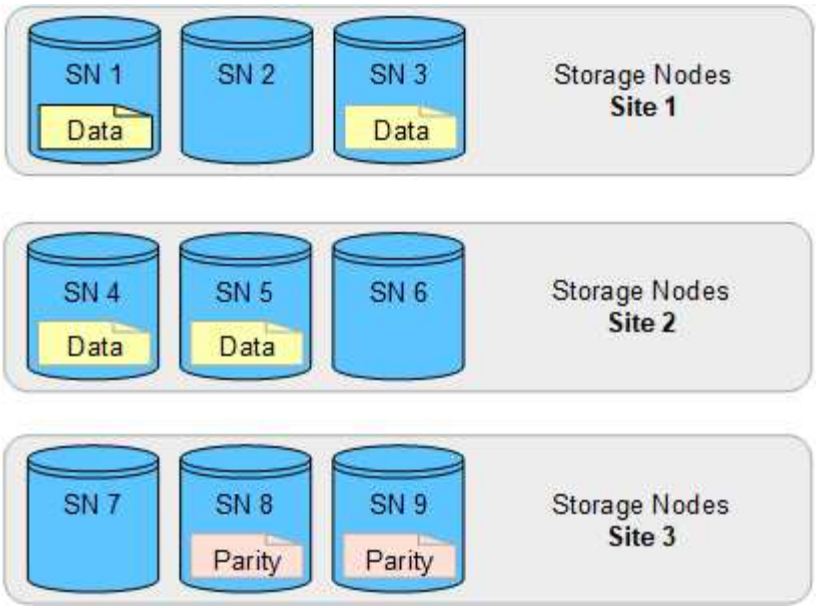
Posizionamento delle regole ILM:

In questo esempio:

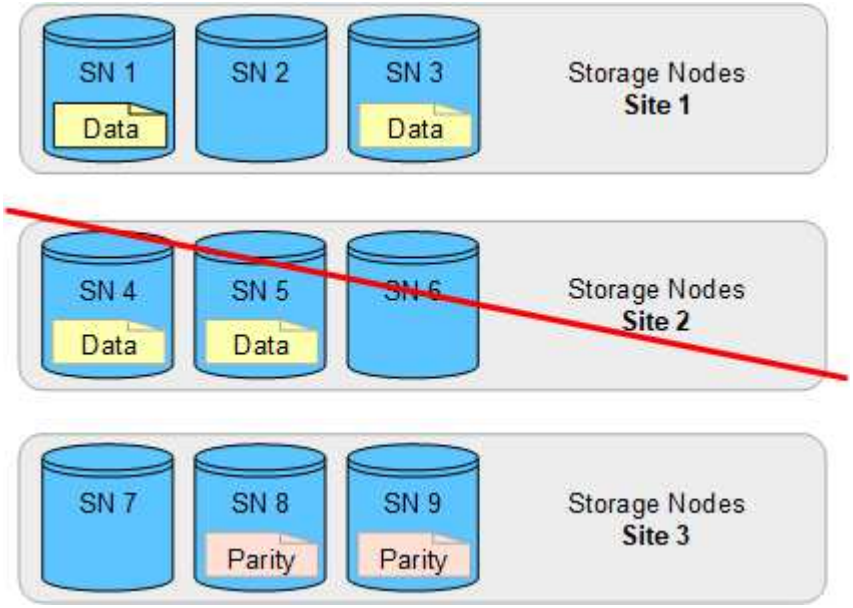
- La regola ILM utilizza uno schema di erasure coding 4+2.
- Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati dell'oggetto.
- Ciascuno dei sei frammenti viene memorizzato su un nodo diverso in tre siti del data center per fornire protezione dei dati in caso di guasti al nodo o perdita del sito.

> La codifica di cancellazione è consentita nei pool di storage contenenti un numero qualsiasi di siti, ad eccezione di due siti.

Regola ILM con schema di erasure coding 4+2:



In caso di perdita di un sito, è possibile recuperare i dati:



Creare un pool di storage

Si creano pool di storage per determinare dove il sistema StorageGRID memorizza i dati a oggetti e il tipo di storage utilizzato. Ogni pool di storage include uno o più siti e uno o più tipi di storage.

> Quando si installa StorageGRID 11,8 su un nuovo grid, vengono creati automaticamente dei pool di storage per ogni sito. Tuttavia, se inizialmente è stato installato StorageGRID 11,6 o versione precedente, i pool di storage non vengono creati automaticamente per ogni sito.

Se si desidera creare pool di storage cloud per memorizzare i dati degli oggetti al di fuori del sistema StorageGRID, consultare la "Informazioni sull'utilizzo dei Cloud Storage Pools".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai esaminato le linee guida per la creazione di pool di storage.

A proposito di questa attività

I pool di storage determinano la posizione in cui vengono memorizzati i dati degli oggetti. Il numero di pool di storage necessari dipende dal numero di siti nella griglia e dal tipo di copie desiderato: Replicate o con codifica di cancellazione.

- Per la replica e l'erasure coding a sito singolo, creare un pool di storage per ciascun sito. Ad esempio, se si desidera memorizzare copie di oggetti replicate in tre siti, creare tre pool di storage.
- Per la cancellazione del codice in tre o più siti, creare un pool di storage che includa una voce per ciascun sito. Ad esempio, se si desidera erasure gli oggetti del codice in tre siti, creare un pool di storage.

> Non includere il sito All Sites in un pool di storage che verrà utilizzato in un profilo di erasure coding. Invece, Aggiungi una voce separata al pool di storage per ogni sito che memorizzerà i dati sottoposti a erasure coding. Vedere questo passo ad esempio.

- Se si dispone di più storage di livello, non creare un pool di storage che includa diversi tipi di storage in un singolo sito. Vedere "Linee guida per la creazione di pool di storage".

Fasi

1. Selezionare **ILM** > **Storage Pools**.

   La scheda Storage Pools elenca tutti i pool di storage definiti.

   > Per le nuove installazioni di StorageGRID 11.6 o versioni precedenti, il pool di storage di tutti i nodi di storage viene aggiornato automaticamente ogni volta che si aggiungono nuovi siti del data center. Non utilizzare questo pool nelle regole ILM.

2. Per creare un nuovo pool di storage, selezionare **Crea**.
3. Immettere un nome univoco per il pool di storage. Utilizzare un nome che sia facile da identificare quando si configurano i profili di erasure coding e le regole ILM.
4. Dall'elenco a discesa **Sito**, selezionare un sito per questo pool di storage.

   Quando si seleziona un sito, il numero di nodi di storage e di nodi di archiviazione nella tabella viene aggiornato automaticamente.

   In generale, non utilizzare il sito All Sites in alcun pool di storage. Le regole ILM che utilizzano un pool di storage All Sites posizionano gli oggetti in qualsiasi sito disponibile, offrendo un minore controllo sul posizionamento degli oggetti. Inoltre, un pool di storage All Sites utilizza immediatamente i nodi di storage in un nuovo sito, il che potrebbe non essere il comportamento previsto.

5. Dall'elenco a discesa **Storage grade**, selezionare il tipo di storage da utilizzare se una regola ILM utilizza questo pool di storage.

   Il grado dello storage, *include tutti i gradi dello storage*, include tutti i nodi storage nel sito selezionato. Il livello di storage dei nodi di archiviazione predefinito include tutti i nodi di archiviazione nel sito selezionato. Se sono stati creati altri gradi di storage per i nodi di storage nel grid, questi vengono elencati nell'elenco a discesa.

6. se si desidera utilizzare il pool di archiviazione in un profilo di erasure coding multisito, selezionare **Aggiungi più nodi** per aggiungere una voce per ciascun sito al pool di archiviazione.

> Non è possibile creare voci duplicate o creare un pool di storage che includa sia il livello di storage dei nodi di archiviazione che qualsiasi livello di storage che contenga nodi di storage.
>
> Viene visualizzato un avviso se si aggiungono più voci con diversi gradi di storage per un sito.

Per rimuovere una voce, selezionare l'icona di eliminazione ✕.

7. Quando si è soddisfatti delle selezioni effettuate, selezionare **Save** (Salva).

Il nuovo pool di storage viene aggiunto all'elenco.

Visualizzare i dettagli del pool di storage

È possibile visualizzare i dettagli di un pool di storage per determinare dove viene utilizzato il pool di storage e per vedere quali nodi e gradi di storage sono inclusi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **ILM** > **Storage Pools**.

La tabella Storage Pools include le seguenti informazioni per ogni pool di storage che include i nodi di storage:

- **Name**: Il nome univoco del pool di storage.
- **Node count**: Numero di nodi nel pool di storage.
- **Utilizzo dello storage**: Percentuale dello spazio utilizzabile totale utilizzato per i dati dell'oggetto su questo nodo. Questo valore non include i metadati degli oggetti.
- **Capacità totale**: Dimensione del pool di storage, che equivale alla quantità totale di spazio utilizzabile per i dati oggetto per tutti i nodi del pool di storage.
- **Utilizzo ILM**: Modalità di utilizzo del pool di storage. Un pool di storage potrebbe essere inutilizzato o potrebbe essere utilizzato in una o più regole ILM, profili di erasure coding o entrambe.

> Non è possibile rimuovere un pool di storage se viene utilizzato.

2. Per visualizzare i dettagli su uno specifico pool di storage, selezionare il nome.

Viene visualizzata la pagina dei dettagli del pool di storage.

3. Visualizzare la scheda **nodi** per informazioni sui nodi di storage o di archivio inclusi nel pool di storage.

La tabella include le seguenti informazioni per ciascun nodo:

- Nome del nodo
- Nome del sito
- Storage grade
- Storage usage (utilizzo storage): La percentuale dello spazio utilizzabile totale per i dati degli oggetti utilizzati per il nodo di storage. Questo campo non è visibile per i pool di nodi di archiviazione.

> Lo stesso valore di utilizzo dello storage (%) viene visualizzato anche nel grafico Storage Used - Object Data per ciascun nodo di storage (selezionare **NODE** > ***Storage Node*** > **Storage**).

4. Selezionare la scheda **utilizzo ILM** per determinare se il pool di storage è attualmente utilizzato in qualsiasi regola ILM o profilo di erasure coding.
5. Se si desidera, accedere alla pagina **ILM rules** per informazioni e gestione delle regole che utilizzano il pool di storage.

   Vedere "Istruzioni per l'utilizzo delle regole ILM".

Modificare il pool di storage

È possibile modificare un pool di storage per modificarne il nome o per aggiornare siti e gradi di storage.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- È stata esaminata la "linee guida per la creazione di pool di storage".
- Se si intende modificare un pool di storage utilizzato da una regola nel criterio ILM attivo, si è preso in considerazione il modo in cui le modifiche influiranno sul posizionamento dei dati degli oggetti.

A proposito di questa attività

Se si aggiunge un nuovo livello di sito o storage a un pool di storage utilizzato nella policy ILM attiva, tenere presente che i nodi di storage nel nuovo livello di sito o storage non verranno utilizzati automaticamente. Per forzare StorageGRID a utilizzare un nuovo sito o storage grade, è necessario attivare un nuovo criterio ILM dopo aver salvato il pool di storage modificato.

Fasi

1. Selezionare **ILM** > **Storage Pools**.
2. Selezionare la casella di controllo del pool di storage che si desidera modificare.

   Non è possibile modificare il pool di storage di tutti i nodi di storage (StorageGRID 11.6 e versioni precedenti).

3. Selezionare **Modifica**.
4. Se necessario, modificare il nome del pool di storage.
5. Se necessario, selezionare altri siti e livelli di storage.

Al cliente viene impedito di modificare il livello del sito o dello storage se il pool di storage viene utilizzato in un profilo di erasure coding e la modifica porterebbe all'invalidità dello schema di erasure coding. Ad esempio, se un pool di storage utilizzato in un profilo di erasure coding include al momento un livello dello storage con un solo sito, è impossibile utilizzare un livello dello storage con due siti, perché la modifica renderebbe lo schema di erasure coding non valido.

6. Selezionare **Salva**.

Al termine

Se è stato aggiunto un nuovo livello di sito o storage a un pool di storage utilizzato nel criterio ILM attivo, attivare un nuovo criterio ILM per forzare StorageGRID a utilizzare il nuovo livello di storage o di sito. Ad esempio, clonare il criterio ILM esistente e attivare il clone. Vedere "Utilizzare le regole ILM e i criteri ILM".

Rimuovere un pool di storage

È possibile rimuovere un pool di storage che non viene utilizzato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "autorizzazioni di accesso richieste".

Fasi

1. Selezionare **ILM** > **Storage Pools**.
2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il pool di storage.

   Non puoi rimuovere un pool di storage se è utilizzato in una regola ILM o in un profilo di erasure coding. Se necessario, selezionare ***nome pool di storage*** > **utilizzo ILM** per determinare dove viene utilizzato il pool di storage.

3. Se il pool di storage che si desidera rimuovere non viene utilizzato, selezionare la casella di controllo.
4. Selezionare **Rimuovi**.
5. Selezionare **OK**.

Utilizza i Cloud Storage Pools

Che cos'è un pool di storage cloud?

Un pool di storage cloud consente di utilizzare ILM per spostare i dati degli oggetti all'esterno del sistema StorageGRID. Ad esempio, è possibile spostare gli oggetti con accesso non frequente in uno storage cloud a basso costo, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o il Tier di accesso all'archivio nello storage Microsoft Azure Blob. In alternativa, è possibile mantenere un backup cloud degli oggetti StorageGRID per migliorare il disaster recovery.

Dal punto di vista di ILM, un pool di storage cloud è simile a un pool di storage. Per memorizzare gli oggetti in entrambe le posizioni, selezionare il pool quando si creano le istruzioni di posizionamento per una regola ILM. Tuttavia, mentre i pool di storage sono costituiti da nodi di storage o nodi di archiviazione all'interno del sistema StorageGRID, un pool di storage cloud è costituito da un bucket esterno (S3) o da un container

(storage blob Azure).

> Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è obsoleto ed è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità. Se si sta utilizzando un nodo di archiviazione con l'opzione Cloud Tiering - Simple Storage Service (S3), "Migrare gli oggetti in un pool di storage cloud" invece.

La tabella confronta i pool di storage con i pool di storage cloud e mostra le analogie e le differenze di alto livello.

	Pool di storage	**Pool di cloud storage**
Come viene creato?	Utilizzando l'opzione **ILM** > **Storage Pools** in Grid Manager.	Utilizzando l'opzione **ILM** > **Storage Pools** > **Cloud Storage Pools** in Grid Manager. È necessario configurare il bucket o il container esterno prima di poter creare il Cloud Storage Pool.
Quanti pool è possibile creare?	Senza limiti.	Fino a 10.
Dove sono memorizzati gli oggetti?	Su uno o più nodi di storage o nodi di archiviazione all'interno di StorageGRID.	In un bucket Amazon S3, un container di storage BLOB di Azure o Google Cloud esterno al sistema StorageGRID. Se il Cloud Storage Pool è un bucket Amazon S3: • È possibile configurare un ciclo di vita del bucket per la transizione di oggetti a storage a lungo termine e a basso costo, come Amazon S3 Glacier o S3 Glacier Deep Archive. Il sistema di storage esterno deve supportare la classe di storage Glacier e l'API S3 RestoreObject. • È possibile creare pool di storage cloud da utilizzare con AWS Commercial Cloud Services (C2S), che supporta l'AWS Secret Region. Se il pool di storage cloud è un container di storage Azure Blob, StorageGRID passa l'oggetto al Tier di archiviazione. **Nota:** in generale, non configurare la gestione del ciclo di vita dello storage Azure Blob per il container utilizzato per un pool di storage cloud. Le operazioni RestoreObject sugli oggetti nel Cloud Storage Pool possono essere interessate dal ciclo di vita configurato.
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nei criteri ILM attivi.	Una regola ILM nei criteri ILM attivi.

	Pool di storage	Pool di cloud storage
Quale metodo di protezione dei dati viene utilizzato?	Replica o erasure coding.	Replica.
Quante copie di ciascun oggetto sono consentite?	Multiplo.	Una copia nel pool di storage cloud e, facoltativamente, una o più copie in StorageGRID. **Nota:** non è possibile memorizzare un oggetto in più di un Cloud Storage Pool alla volta.
Quali sono i vantaggi?	Gli oggetti sono rapidamente accessibili in qualsiasi momento.	Storage a basso costo.
		Nota: Non è possibile eseguire il tiering dei dati FabricPool nei pool di storage cloud. Gli oggetti con blocco oggetti S3 abilitato non possono essere posizionati nei pool di storage cloud.

Ciclo di vita di un oggetto Cloud Storage Pool

Prima di implementare i Cloud Storage Pool, esaminare il ciclo di vita degli oggetti memorizzati in ciascun tipo di Cloud Storage Pool.

S3: Ciclo di vita di un oggetto Cloud Storage Pool

Questa procedura descrive le fasi del ciclo di vita di un oggetto memorizzato in un Cloud Storage Pool S3.

> "Glacier" si riferisce sia alla classe di storage Glacier che a quella Glacier Deep Archive, con una sola eccezione: La classe di storage Glacier Deep Archive non supporta il Tier di ripristino Expedited. È supportato solo il recupero in blocco o standard.

> Google Cloud Platform (GCP) supporta il recupero di oggetti dallo storage a lungo termine senza richiedere un'operazione POST-ripristino.

1. **Oggetto memorizzato in StorageGRID**

   Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. **Oggetto spostato in S3 Cloud Storage Pool**
   - Quando l'oggetto viene associato a una regola ILM che utilizza un pool di storage cloud S3 come posizione di posizionamento, StorageGRID sposta l'oggetto nel bucket S3 esterno specificato dal pool di storage cloud.
   - Quando l'oggetto è stato spostato nel Cloud Storage Pool S3, l'applicazione client può recuperarlo utilizzando una richiesta GetObject S3 da StorageGRID, a meno che l'oggetto non sia stato spostato

nello storage Glacier.

3. **Oggetto in transizione a Glacier (stato non recuperabile)**
   - Facoltativamente, l'oggetto può essere passato allo storage Glacier. Ad esempio, il bucket S3 esterno potrebbe utilizzare la configurazione del ciclo di vita per trasferire un oggetto allo storage Glacier immediatamente o dopo un certo numero di giorni.

> Per trasferire oggetti, è necessario creare una configurazione del ciclo di vita per il bucket S3 esterno e utilizzare una soluzione storage che implementi la classe di storage Glacier e supporti l'API S3 RestoreObject.

> Non utilizzare i Cloud Storage Pools per gli oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste RestoreObject, pertanto StorageGRID non sarà in grado di recuperare gli oggetti Swift passati allo storage S3 Glacier. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).

   - Durante la transizione, l'applicazione client può utilizzare una richiesta S3 HeadObject per monitorare lo stato dell'oggetto.

4. **Oggetto ripristinato dallo storage Glacier**

   Se un oggetto è stato spostato nello storage Glacier, l'applicazione client può emettere una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel Cloud Storage Pool S3. La richiesta specifica il numero di giorni in cui la copia deve essere disponibile nel Cloud Storage Pool e il Tier di accesso ai dati da utilizzare per l'operazione di ripristino (accelerato, Standard o in blocco). Una volta raggiunta la data di scadenza della copia recuperabile, la copia viene automaticamente riportata in uno stato non recuperabile.

> Se una o più copie dell'oggetto esistono anche sui nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier mediante una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

5. **Oggetto recuperato**

   Una volta ripristinato un oggetto, l'applicazione client può emettere una richiesta GetObject per recuperare l'oggetto ripristinato.

Azure: Ciclo di vita di un oggetto Cloud Storage Pool

Questa procedura descrive le fasi del ciclo di vita di un oggetto memorizzato in un Cloud Storage Pool di Azure.

1. **Oggetto memorizzato in StorageGRID**

   Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. **Oggetto spostato in Azure Cloud Storage Pool**

   Quando l'oggetto viene associato a una regola ILM che utilizza un Azure Cloud Storage Pool come posizione di posizionamento, StorageGRID sposta l'oggetto nel contenitore di storage BLOB di Azure esterno specificato dal Cloud Storage Pool.

Non utilizzare i Cloud Storage Pools per gli oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste RestoreObject, pertanto StorageGRID non sarà in grado di recuperare gli oggetti Swift che sono stati passati al Tier di archiviazione BLOB di Azure. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).

3. **Oggetto sottoposto a transizione al Tier di archiviazione (stato non recuperabile)**

   Subito dopo aver spostato l'oggetto nel pool di storage cloud di Azure, StorageGRID passa automaticamente l'oggetto al livello di archiviazione dello storage Blob di Azure.

4. **Oggetto ripristinato dal Tier di archiviazione**

   Se un oggetto è stato spostato nel Tier Archive, l'applicazione client può emettere una richiesta S3 RestoreObject per ripristinare una copia recuperabile nell'Azure Cloud Storage Pool.

   Quando StorageGRID riceve il RestoreObject, trasferisce temporaneamente l'oggetto al livello di raffreddamento dell'archiviazione BLOB di Azure. Non appena viene raggiunta la data di scadenza nella richiesta RestoreObject, StorageGRID trasferisce nuovamente l'oggetto al livello Archive.

   Se una o più copie dell'oggetto sono presenti anche nei nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso di archiviazione mediante una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

5. **Oggetto recuperato**

   Una volta ripristinato un oggetto in Azure Cloud Storage Pool, l'applicazione client può emettere una richiesta GetObject per recuperare l'oggetto ripristinato.

Informazioni correlate

"UTILIZZARE L'API REST S3"

Quando utilizzare i Cloud Storage Pools

Utilizzando i Cloud Storage Pools, è possibile eseguire il backup o il tiering dei dati in una posizione esterna. Inoltre, puoi eseguire il backup o il Tier dei dati in più cloud.

Eseguire il backup dei dati StorageGRID in una posizione esterna

È possibile utilizzare un pool di storage cloud per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, i dati dell'oggetto nel pool di storage cloud possono essere utilizzati per soddisfare le richieste dei client. Tuttavia, potrebbe essere necessario emettere la richiesta S3 RestoreObject per accedere alla copia dell'oggetto di backup nel Cloud Storage Pool.

I dati dell'oggetto in un pool di storage cloud possono essere utilizzati anche per recuperare i dati persi da StorageGRID a causa di un guasto di un volume di storage o di un nodo di storage. Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.

Per implementare una soluzione di backup:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che memorizzi simultaneamente le copie degli oggetti sui nodi di storage (come copie replicate o codificate in cancellazione) e una singola copia degli oggetti nel Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Dati di Tier da StorageGRID a posizione esterna

È possibile utilizzare un pool di storage cloud per memorizzare oggetti all'esterno del sistema StorageGRID. Si supponga, ad esempio, di disporre di un elevato numero di oggetti da conservare, ma si prevede di accedervi raramente, se mai. È possibile utilizzare un pool di storage cloud per tierare gli oggetti in modo da ridurre il costo dello storage e liberare spazio in StorageGRID.

Per implementare una soluzione di tiering:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che sposti gli oggetti utilizzati raramente dai nodi di storage al Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Mantenere più endpoint cloud

È possibile configurare più endpoint del Cloud Storage Pool se si desidera eseguire il Tier o il backup dei dati degli oggetti in più cloud. I filtri nelle regole ILM consentono di specificare quali oggetti sono memorizzati in ciascun Cloud Storage Pool. Ad esempio, è possibile memorizzare oggetti di alcuni tenant o bucket in Amazon S3 Glacier e oggetti di altri tenant o bucket nello storage Azure Blob. In alternativa, puoi spostare i dati tra lo storage Amazon S3 Glacier e Azure Blob.

> Quando si utilizzano endpoint multipli del Cloud Storage Pool, tenere presente che un oggetto può essere memorizzato in un solo Cloud Storage Pool alla volta.

Per implementare più endpoint cloud:

1. Crea fino a 10 pool di cloud storage.
2. Configurare le regole ILM in modo che memorizzino i dati dell'oggetto appropriati all'ora appropriata in ciascun Cloud Storage Pool. Ad esempio, memorizzare oggetti dal bucket A nel Cloud Storage Pool A e memorizzare oggetti dal bucket B nel Cloud Storage Pool B. Oppure, memorizzare gli oggetti nel Cloud Storage Pool A per un certo periodo di tempo e spostarli nel Cloud Storage Pool B.
3. Aggiungere le regole alla policy ILM. Quindi, simulare e attivare la policy.

Considerazioni per i Cloud Storage Pools

Se si prevede di utilizzare un pool di storage cloud per spostare oggetti fuori dal sistema StorageGRID, è necessario esaminare le considerazioni relative alla configurazione e all'utilizzo dei pool di storage cloud.

Considerazioni generali

- In generale, lo storage di archiviazione cloud, come Amazon S3 Glacier o Azure Blob, è un luogo conveniente per memorizzare i dati degli oggetti. Tuttavia, i costi per recuperare i dati dallo storage di archiviazione cloud sono relativamente elevati. Per ottenere il costo complessivo più basso, è necessario

considerare quando e con quale frequenza accedere agli oggetti nel Cloud Storage Pool. L'utilizzo di un Cloud Storage Pool è consigliato solo per i contenuti ai quali si prevede di accedere con frequenza limitata.

- Non utilizzare i Cloud Storage Pools per gli oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste RestoreObject, pertanto StorageGRID non sarà in grado di recuperare gli oggetti Swift passati all'archiviazione S3 Glacier o al Tier di archiviazione BLOB di Azure. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).
- 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.
- Gli oggetti con blocco oggetti S3 abilitato non possono essere posizionati nei pool di storage cloud.
- Se nel bucket S3 di destinazione per un Cloud Storage Pool è attivato il blocco degli oggetti S3, il tentativo di configurare la replica del bucket (PutBucketReplication) non riesce e viene visualizzato un errore AccessDenied.

Considerazioni sulle porte utilizzate per i pool di cloud storage

Per garantire che le regole ILM possano spostare oggetti da e verso il Cloud Storage Pool specificato, è necessario configurare la rete o le reti che contengono i nodi di storage del sistema. È necessario assicurarsi che le seguenti porte possano comunicare con il Cloud Storage Pool.

Per impostazione predefinita, i 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 un Cloud Storage Pool.

Se si utilizza un server proxy non trasparente, è necessario anche "configurare un proxy di archiviazione" per consentire l'invio dei messaggi a endpoint esterni, ad esempio un endpoint su internet.

Considerazioni sui costi

L'accesso allo storage nel cloud utilizzando un Cloud Storage Pool richiede la connettività di rete al cloud. Devi considerare il costo dell'infrastruttura di rete che utilizzerai per accedere al cloud e fornirlo in modo appropriato, in base alla quantità di dati che prevederai di spostare tra StorageGRID e il cloud utilizzando il pool di storage cloud.

Quando StorageGRID si connette all'endpoint esterno del pool di storage nel cloud, invia varie richieste per monitorare la connettività e garantire che possa eseguire le operazioni richieste. Anche se a queste richieste saranno associati costi aggiuntivi, il costo del monitoraggio di un pool di storage cloud dovrebbe essere solo una piccola frazione del costo complessivo di storage degli oggetti in S3 o Azure.

Se si devono spostare gli oggetti da un endpoint esterno del pool di cloud storage a StorageGRID, potrebbero verificarsi costi più significativi. Gli oggetti possono essere spostati di nuovo in StorageGRID in uno dei seguenti casi:

- L'unica copia dell'oggetto si trova in un pool di storage cloud e si decide di memorizzare l'oggetto in StorageGRID. In questo caso, le regole e i criteri ILM vengono riconfigurati. Quando si verifica la valutazione ILM, StorageGRID invia più richieste per recuperare l'oggetto dal pool di storage cloud. StorageGRID crea quindi localmente il numero specificato di copie replicate o codificate per la cancellazione. Una volta spostato di nuovo l'oggetto in StorageGRID, la copia nel pool di storage cloud viene eliminata.
- Gli oggetti vengono persi a causa di un guasto al nodo di storage. Se l'unica copia rimanente di un oggetto

si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.

> Quando gli oggetti vengono spostati di nuovo in StorageGRID da un pool di storage cloud, StorageGRID invia più richieste all'endpoint del pool di storage cloud per ciascun oggetto. Prima di spostare un gran numero di oggetti, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket Cloud Storage Pool

La policy del bucket per il bucket S3 esterno utilizzato per un pool di storage cloud deve concedere l'autorizzazione StorageGRID per spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto dallo storage Glacier quando richiesto e molto altro ancora. Idealmente, StorageGRID dovrebbe avere un accesso completo al bucket (`s3:*`); tuttavia, se ciò non è possibile, il criterio bucket deve concedere le seguenti autorizzazioni S3 a StorageGRID:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Considerazioni sul ciclo di vita del bucket esterno

Lo spostamento degli oggetti tra StorageGRID e il bucket S3 esterno specificato nel pool di storage cloud è controllato dalle regole ILM e dalle policy ILM attive in StorageGRID. Al contrario, la transizione degli oggetti dal bucket S3 esterno specificato nel Cloud Storage Pool ad Amazon S3 Glacier o S3 Glacier Deep Archive (o a una soluzione di storage che implementa la classe di storage Glacier) è controllata dalla configurazione del ciclo di vita di tale bucket.

Per trasferire oggetti da Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata nel bucket S3 esterno e utilizzare una soluzione storage che implementi la classe di storage Glacier e supporti l'API S3 RestoreObject.

Ad esempio, supponiamo che tutti gli oggetti spostati da StorageGRID al pool di storage cloud debbano essere trasferiti immediatamente allo storage Amazon S3 Glacier. Creare una configurazione del ciclo di vita sul bucket S3 esterno che specifica una singola azione (**transizione**) come segue:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Questa regola trasferirebbe tutti gli oggetti bucket al Glacier Amazon S3 il giorno in cui sono stati creati (ovvero il giorno in cui sono stati spostati da StorageGRID al pool di storage cloud).

> Quando si configura il ciclo di vita del bucket esterno, non utilizzare mai le azioni **Expiration** per definire quando gli oggetti scadono. Le azioni di scadenza fanno sì che il sistema di storage esterno elimini gli oggetti scaduti. Se in seguito si tenta di accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non viene trovato.

Se si desidera trasferire oggetti nel Cloud Storage Pool in S3 Glacier Deep Archive (invece di Amazon S3 Glacier), specificare `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tuttavia, tenere presente che non è possibile utilizzare `Expedited` tier per ripristinare gli oggetti da S3 Glacier Deep Archive.

Azure: Considerazioni per il Tier di accesso

Quando si configura un account di storage Azure, è possibile impostare il Tier di accesso predefinito su Hot o Cool. Quando si crea un account storage da utilizzare con un Cloud Storage Pool, è necessario utilizzare l'hot Tier come Tier predefinito. Anche se StorageGRID imposta immediatamente il Tier per l'archiviazione quando sposta gli oggetti nel pool di storage cloud, l'utilizzo dell'impostazione predefinita di Hot garantisce che non venga addebitata una tariffa per l'eliminazione anticipata degli oggetti rimossi dal Tier Cool prima del minimo di 30 giorni.

Azure: Gestione del ciclo di vita non supportata

Non utilizzare la gestione del ciclo di vita dello storage Azure Blob per il container utilizzato con un Cloud Storage Pool. Le operazioni del ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

- "Creare un pool di storage cloud"

Confronto tra Cloud Storage Pools e la replica di CloudMirror

Quando si inizia a utilizzare i pool di storage cloud, potrebbe essere utile comprendere le analogie e le differenze tra i pool di storage cloud e il servizio di replica di StorageGRID CloudMirror.

	Pool di cloud storage	Servizio di replica di CloudMirror
Qual è lo scopo principale?	Agisce come destinazione di archiviazione. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure può essere una copia aggiuntiva. Ovvero, invece di conservare due copie in loco, puoi conservarne una all'interno di StorageGRID e inviarne una copia al pool di storage cloud.	Consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). Crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente.
Come viene configurato?	Definito allo stesso modo dei pool di storage, utilizzando Grid Manager o l'API Grid Management. Può essere selezionata come posizione di posizionamento in una regola ILM. Mentre un pool di storage è costituito da un gruppo di nodi di storage, un pool di storage cloud viene definito utilizzando un endpoint remoto S3 o Azure (indirizzo IP, credenziali e così via).	Un utente tenant "Configura la replica di CloudMirror" Definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) utilizzando Tenant Manager o l'API S3. Una volta configurato l'endpoint CloudMirror, qualsiasi bucket di proprietà dell'account tenant può essere configurato per puntare all'endpoint CloudMirror.
Chi è responsabile della sua configurazione?	In genere, un amministratore di rete	In genere, un utente tenant
Qual è la destinazione?	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Tier Azure Blob Archive • Piattaforma Google Cloud (GCP)	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Piattaforma Google Cloud (GCP)
Qual è la causa dello spostamento degli oggetti nella destinazione?	Una o più regole ILM nei criteri ILM attivi. Le regole ILM definiscono gli oggetti che StorageGRID sposta nel pool di storage cloud e quando gli oggetti vengono spostati.	L'atto di inserire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror. Gli oggetti che esistevano nel bucket di origine prima della configurazione del bucket con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come vengono recuperati gli oggetti?	Le applicazioni devono effettuare richieste a StorageGRID per recuperare gli oggetti spostati in un pool di storage cloud. Se l'unica copia di un oggetto è stata trasferita allo storage di archiviazione, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia mirrorata nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto inviando richieste a StorageGRID o alla destinazione S3. Si supponga, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti in un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è necessario utilizzare StorageGRID.

	Pool di cloud storage	Servizio di replica di CloudMirror
Puoi leggere direttamente dalla destinazione?	No Gli oggetti spostati in un pool di storage cloud vengono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero dal pool di storage cloud).	Sì, perché la copia mirrorata è una copia indipendente.
Cosa succede se un oggetto viene cancellato dall'origine?	L'oggetto viene anche eliminato dal Cloud Storage Pool.	L'azione di eliminazione non viene replicata. Un oggetto cancellato non esiste più nel bucket StorageGRID, ma continua ad esistere nel bucket di destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.
Come si accede agli oggetti dopo un disastro (sistema StorageGRID non operativo)?	I nodi StorageGRID guasti devono essere ripristinati. Durante questo processo, le copie degli oggetti replicati potrebbero essere ripristinate utilizzando le copie nel Cloud Storage Pool.	Le copie degli oggetti nella destinazione CloudMirror sono indipendenti da StorageGRID, pertanto è possibile accedervi direttamente prima del ripristino dei nodi StorageGRID.

Creare un pool di storage cloud

Un Cloud Storage Pool specifica un singolo bucket Amazon S3 esterno o un altro provider compatibile con S3 o un container di storage Azure Blob.

Quando crei un pool di storage cloud, specifica il nome e la posizione del bucket o del container esterno che StorageGRID utilizzerà per memorizzare gli oggetti, il tipo di provider cloud (storage Amazon S3/GCP o Azure Blob) e le informazioni StorageGRID necessarie per accedere al bucket o al container esterno.

StorageGRID convalida il pool di storage cloud non appena viene salvato, quindi devi assicurarti che il bucket o il container specificato nel pool di storage cloud esista e sia raggiungibile.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "autorizzazioni di accesso richieste".
- Hai esaminato il "Considerazioni per i Cloud Storage Pools".
- Il bucket o il container esterno a cui fa riferimento il Cloud Storage Pool esiste già e ne conosci il nome e la posizione.
- Per accedere al bucket o al container, sono disponibili le seguenti informazioni relative al tipo di autenticazione scelto:

Chiave di accesso S3

Per il bucket S3 esterno

- L'ID della chiave di accesso per l'account proprietario del bucket esterno.
- La chiave di accesso segreta associata.

In alternativa, è possibile specificare Anonymous per il tipo di autenticazione.

Portale di accesso C2S

Per il servizio Commercial Cloud Services (C2S) S3

Hai a disposizione quanto segue:

- URL completo che StorageGRID utilizzerà per ottenere credenziali temporanee dal server CAP (Access Portal) di C2S, inclusi tutti i parametri API richiesti e opzionali assegnati all'account C2S.
- Certificato CA del server emesso da un'autorità di certificazione governativa (CA) appropriata. StorageGRID utilizza questo certificato per verificare l'identità del server CAP. Il certificato CA del server deve utilizzare la codifica PEM.
- Certificato del client emesso da un'autorità di certificazione governativa (CA) appropriata. StorageGRID utilizza questo certificato per identificare se stesso nel server CAP. Il certificato client deve utilizzare la codifica PEM e deve avere ottenuto l'accesso all'account C2S.
- Chiave privata con codifica PEM per il certificato client.
- Passphrase per la decrittografia della chiave privata per il certificato client, se crittografato.

> Se il certificato client viene crittografato, utilizzare il formato tradizionale per la crittografia. Il formato crittografato PKCS n. 8 non è supportato.

Storage Azure Blob

Per il container esterno

- Uniform Resource Identifier (URI) utilizzato per accedere al contenitore di storage Blob.
- Nome dell'account di storage e della chiave account. È possibile utilizzare il portale Azure per trovare questi valori.

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Selezionare **Crea**, quindi immettere le seguenti informazioni:

Campo	Descrizione
Nome del pool di cloud storage	Un nome che descrive brevemente il Cloud Storage Pool e il suo scopo. Utilizzare un nome che sia facile da identificare quando si configurano le regole ILM.

Campo	Descrizione
Tipo di provider	Quale cloud provider utilizzerai per questo Cloud Storage Pool: • **Amazon S3/GCP**: Selezionare questa opzione per Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) o altri provider compatibili con S3. • **Azure Blob Storage**
Bucket o container	Il nome del bucket S3 esterno o del container Azure. Non puoi modificare questo valore dopo il salvataggio del Cloud Storage Pool.

3. In base alla selezione del tipo di provider, inserire le informazioni sull'endpoint del servizio.

Amazon S3/GCP

a. Per il protocollo, selezionare HTTPS o HTTP.

> Non utilizzare connessioni HTTP per dati sensibili.

b. Inserire il nome host. Esempio:

`s3-aws-region.amazonaws.com`

c. Selezionare lo stile URL:

Opzione	Descrizione
Rilevamento automatico	Tentare di rilevare automaticamente lo stile URL da utilizzare, in base alle informazioni fornite. Ad esempio, se si specifica un indirizzo IP, StorageGRID utilizzerà un URL di tipo path. Selezionare questa opzione solo se non si conosce lo stile specifico da utilizzare.
Stile virtual-hosted	Utilizza un URL di tipo virtual-hosted per accedere al bucket. Gli URL in stile virtual-hosted includono il nome del bucket come parte del nome di dominio. Esempio: `https://bucket-name.s3.company.com/key-name`
Stile di percorso	Utilizzare un URL stile percorso per accedere al bucket. Gli URL stile percorso includono il nome del bucket alla fine Esempio: `https://s3.company.com/bucket-name/key-name` **Nota:** l'opzione URL stile percorso non è consigliata e sarà obsoleta in una release futura di StorageGRID.

d. Se si desidera, inserire il numero della porta o utilizzare la porta predefinita: 443 per HTTPS o 80 per HTTP.

Azure Blob Storage

a. Utilizzando uno dei seguenti formati, immettere l'URI per l'endpoint del servizio.

- `https://host:port`
- `http://host:port`

Esempio: `https://myaccount.blob.core.windows.net:443`

Se non si specifica una porta, per impostazione predefinita viene utilizzata la porta 443 per HTTPS e la porta 80 per HTTP.

4. Selezionare **continua**. Quindi, selezionare il tipo di autenticazione e immettere le informazioni richieste per l'endpoint del Cloud Storage Pool:

Tasto di accesso

Solo per provider Amazon S3/GCP

a. Per **Access key ID**, inserire l'ID della chiave di accesso per l'account proprietario del bucket esterno.
b. Per **Secret access key**, inserire la chiave di accesso segreta.

CAP (portale di accesso C2S)

Per il servizio Commercial Cloud Services (C2S) S3

a. Per **URL credenziali temporanee**, immettere l'URL completo che StorageGRID utilizzerà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API richiesti e facoltativi assegnati all'account C2S.
b. Per **certificato CA server**, selezionare **Sfoglia** e caricare il certificato CA con codifica PEM che StorageGRID utilizzerà per verificare il server CAP.
c. Per **certificato client**, selezionare **Sfoglia** e caricare il certificato con codifica PEM che StorageGRID utilizzerà per identificarsi nel server CAP.
d. Per **Client private key**, selezionare **Browse** e caricare la chiave privata codificata PEM per il certificato del client.
e. Se la chiave privata del client è crittografata, immettere la passphrase per la decrittografia della chiave privata del client. In caso contrario, lasciare vuoto il campo **Password chiave privata client**.

Azure Blob Storage

a. Per **Nome account**, immettere il nome dell'account di storage Blob proprietario del container di servizi esterno.
b. Per **account key**, inserire la chiave segreta per l'account di storage Blob.

Anonimo

Non sono richieste informazioni aggiuntive.

5. Selezionare **continua**. Quindi scegliere il tipo di verifica del server che si desidera utilizzare:

Opzione	Descrizione
Utilizzare i certificati della CA principale nel sistema operativo del nodo di storage	Utilizzare i certificati Grid CA installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Selezionare **Sfoglia** e caricare il certificato con codifica PEM.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato.

6. Selezionare **Salva**.

Quando si salva un pool di storage cloud, StorageGRID esegue le seguenti operazioni:

- Convalida l'esistenza del bucket o del container e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
- Scrive un file marker nel bucket o nel container per identificarlo come pool di storage cloud. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

  Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il bucket o il container specificato non esiste già, potrebbe essere visualizzato un errore.

7. Se si verifica un errore, consultare "Istruzioni per la risoluzione dei problemi dei Cloud Storage Pools", Risolvere eventuali problemi, quindi provare a salvare nuovamente il Cloud Storage Pool.

Modifica di un pool di storage cloud

È possibile modificare un Cloud Storage Pool per modificarne il nome, l'endpoint del servizio o altri dettagli; tuttavia, non è possibile modificare il bucket S3 o il container Azure per un Cloud Storage Pool.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai esaminato il "Considerazioni per i Cloud Storage Pools".

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.

   La tabella Cloud Storage Pools elenca i Cloud Storage Pools esistenti.

2. Selezionare la casella di controllo per il Cloud Storage Pool che si desidera modificare.
3. Selezionare **azioni** > **Modifica**.
4. Se necessario, modificare il nome visualizzato, l'endpoint del servizio, le credenziali di autenticazione o il metodo di convalida del certificato.

   > Non puoi modificare il tipo di provider, il bucket S3 o il container Azure per un Cloud Storage Pool.

   Se in precedenza è stato caricato un certificato server o client, è possibile selezionare **Dettagli certificato** per rivedere il certificato attualmente in uso.

5. Selezionare **Salva**.

   Quando si salva un pool di storage cloud, StorageGRID convalida l'esistenza del bucket o del container e dell'endpoint del servizio e che è possibile raggiungerli utilizzando le credenziali specificate.

   Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore. Ad esempio, se si verifica un errore del certificato, potrebbe essere visualizzato un errore.

   Consultare le istruzioni per "Risoluzione dei problemi relativi ai pool di storage cloud", Risolvere il problema, quindi provare a salvare nuovamente il Cloud Storage Pool.

Rimuovere un pool di storage cloud

È possibile rimuovere un Cloud Storage Pool se non utilizzato in una regola ILM e non contiene dati oggetto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "autorizzazioni di accesso richieste".

Se necessario, utilizzare ILM per spostare i dati dell'oggetto

Se il Cloud Storage Pool che si desidera rimuovere contiene dati a oggetti, è necessario utilizzare ILM per spostare i dati in una posizione diversa. Ad esempio, è possibile spostare i dati su nodi di storage nel proprio grid o su un pool di storage cloud diverso.

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il Cloud Storage Pool.

   Non puoi rimuovere un Cloud Storage Pool se viene utilizzato in una regola ILM o in un profilo di erasure coding.

3. Se si utilizza il Cloud Storage Pool, selezionare ***cloud storage pool name*** > **ILM usage**.
4. "Clonare ogni regola ILM" Che attualmente colloca gli oggetti nel Cloud Storage Pool che si desidera rimuovere.
5. Determinare dove si desidera spostare gli oggetti esistenti gestiti da ciascuna regola clonata.

   È possibile utilizzare uno o più pool di storage o un pool di storage cloud diverso.

6. Modificare ciascuna regola clonata.

   Per la fase 2 della creazione guidata regola ILM, selezionare la nuova posizione dal campo **copie at**.

7. "Creare un nuovo criterio ILM" e sostituire ciascuna delle vecchie regole con una regola clonata.
8. Attivare la nuova policy.
9. Attendere che ILM rimuova gli oggetti dal Cloud Storage Pool e li inseri nella nuova posizione.

Eliminare il pool di storage cloud

Quando il Cloud Storage Pool è vuoto e non viene utilizzato in alcuna regola ILM, è possibile eliminarlo.

Prima di iniziare

- Sono state rimosse tutte le regole ILM che potrebbero aver utilizzato il pool.
- Hai confermato che il bucket S3 o il container Azure non contiene oggetti.

  Si verifica un errore se si tenta di rimuovere un Cloud Storage Pool se contiene oggetti. Vedere "Risolvere i problemi dei pool di storage cloud".

Quando crei un pool di storage cloud, StorageGRID scrive un file di marker nel bucket o nel container per identificarlo come pool di storage cloud. Non rimuovere questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Se la colonna ILM Usage (utilizzo ILM) indica che il Cloud Storage Pool non è in uso, selezionare la casella di controllo.
3. Selezionare **azioni** > **Rimuovi**.
4. Selezionare **OK**.

Risolvere i problemi dei pool di storage cloud

Utilizzare questi passaggi per la risoluzione dei problemi per risolvere gli errori che potrebbero verificarsi durante la creazione, la modifica o l'eliminazione di un pool di storage cloud.

Determinare se si è verificato un errore

StorageGRID esegue una semplice verifica dello stato di salute di ogni pool di storage cloud una volta al minuto per garantire che sia possibile accedere al pool di storage cloud e che funzioni correttamente. Se il controllo dello stato di salute rileva un problema, viene visualizzato un messaggio nella colonna Last error (ultimo errore) della tabella Cloud Storage Pools (pool di storage cloud) della pagina Storage Pools (pool di storage).

La tabella mostra l'errore più recente rilevato per ciascun Cloud Storage Pool e indica quanto tempo fa si è verificato l'errore.

Inoltre, un avviso di **errore di connettività del Cloud Storage Pool** viene attivato se il controllo dello stato di salute rileva che uno o più nuovi errori del Cloud Storage Pool si sono verificati negli ultimi 5 minuti. Se si riceve una notifica via email per questo avviso, accedere alla pagina Storage Pools (selezionare **ILM** > **Storage Pools**), esaminare i messaggi di errore nella colonna Last error (ultimo errore) e consultare le linee guida per la risoluzione dei problemi riportate di seguito.

Controllare se un errore è stato risolto

Dopo aver risolto eventuali problemi sottostanti, è possibile determinare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, selezionare l'endpoint e selezionare **Clear error**. Un messaggio di conferma indica che StorageGRID ha eliminato l'errore per il pool di storage cloud.

Se il problema sottostante è stato risolto, il messaggio di errore non viene più visualizzato. Tuttavia, se il problema sottostante non è stato risolto (o se si verifica un errore diverso), il messaggio di errore viene visualizzato nella colonna Last error (ultimo errore) entro pochi minuti.

Errore: Questo Cloud Storage Pool contiene contenuti imprevisti

Questo errore potrebbe verificarsi quando si tenta di creare, modificare o eliminare un pool di storage cloud. Questo errore si verifica se il bucket o il container include `x-ntap-sgws-cloud-pool-uuid` Il file marker, ma non ha l'UUID previsto.

In genere, questo errore viene visualizzato solo se si crea un nuovo pool di storage cloud e un'altra istanza di

StorageGRID sta già utilizzando lo stesso pool di storage cloud.

Per risolvere il problema, attenersi alla seguente procedura:

- Assicurati che nessuno nella tua organizzazione stia utilizzando questo Cloud Storage Pool.
- Eliminare `x-ntap-sgws-cloud-pool-uuid` E provare a configurare nuovamente il Cloud Storage Pool.

Errore: Impossibile creare o aggiornare il Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si tenta di creare o modificare un pool di storage cloud. Questo errore indica che alcuni problemi di connettività o configurazione impediscono a StorageGRID di scrivere nel pool di storage cloud.

Per risolvere il problema, esaminare il messaggio di errore dall'endpoint.

- Se il messaggio di errore contiene `Get *url*: EOF`, Verificare che l'endpoint del servizio utilizzato per il Cloud Storage Pool non utilizzi HTTP per un container o bucket che richiede HTTPS.
- Se il messaggio di errore contiene `Get *url*: net/http: request canceled while waiting for connection`, Verificare che la configurazione di rete consenta ai nodi di storage di accedere all'endpoint del servizio utilizzato per il Cloud Storage Pool.
- Per tutti gli altri messaggi di errore degli endpoint, provare una o più delle seguenti soluzioni:
  - Creare un container o bucket esterno con lo stesso nome immesso per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.
  - Correggere il nome del container o bucket specificato per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.

Errore: Impossibile analizzare il certificato CA

Questo errore potrebbe verificarsi quando si tenta di creare o modificare un pool di storage cloud. L'errore si verifica se StorageGRID non ha potuto analizzare il certificato inserito durante la configurazione del pool di storage cloud.

Per correggere il problema, controllare il certificato CA fornito per eventuali problemi.

Errore: Impossibile trovare un pool di storage cloud con questo ID

Questo errore potrebbe verificarsi quando si tenta di modificare o eliminare un pool di storage cloud. Questo errore si verifica se l'endpoint restituisce una risposta 404, il che può significare una delle seguenti:

- Le credenziali utilizzate per il Cloud Storage Pool non dispongono dell'autorizzazione di lettura per il bucket.
- Il bucket utilizzato per il Cloud Storage Pool non include `x-ntap-sgws-cloud-pool-uuid` file marker.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare che l'utente associato alla chiave di accesso configurata disponga delle autorizzazioni necessarie.
- Modificare il Cloud Storage Pool con le credenziali che dispongono delle autorizzazioni necessarie.
- Se le autorizzazioni sono corrette, contattare l'assistenza.

Errore: Impossibile controllare il contenuto del Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Questo errore indica che un problema di connettività o configurazione impedisce a StorageGRID di leggere il contenuto del bucket del pool di storage cloud.

Per risolvere il problema, esaminare il messaggio di errore dall'endpoint.

Errore: Gli oggetti sono già stati posizionati in questo bucket

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Non è possibile eliminare un Cloud Storage Pool se contiene dati spostati da ILM, dati presenti nel bucket prima della configurazione del Cloud Storage Pool o dati inseriti nel bucket da un'altra origine dopo la creazione del Cloud Storage Pool.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Segui le istruzioni per riportare gli oggetti in StorageGRID in "ciclo di vita di un oggetto Cloud Storage Pool".
- Se si è certi che ILM non abbia inserito gli oggetti rimanenti nel Cloud Storage Pool, eliminarli manualmente dal bucket.

> Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbe essere stato collocato in tale posizione da ILM. Se in un secondo momento si tenta di accedere a un oggetto eliminato manualmente da StorageGRID, l'oggetto eliminato non viene trovato.

Errore: Il proxy ha rilevato un errore esterno durante il tentativo di raggiungere il Cloud Storage Pool

È possibile che si verifichi questo errore se è stato configurato un proxy di storage non trasparente tra i nodi di storage e l'endpoint S3 esterno utilizzato per il Cloud Storage Pool. Questo errore si verifica se il server proxy esterno non riesce a raggiungere l'endpoint del Cloud Storage Pool. Ad esempio, il server DNS potrebbe non essere in grado di risolvere il nome host o potrebbe esserci un problema di rete esterno.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare le impostazioni del Cloud Storage Pool (**ILM** > **Storage Pools**).
- Controllare la configurazione di rete del server proxy di archiviazione.

Informazioni correlate

"Ciclo di vita di un oggetto Cloud Storage Pool"

Gestire i profili di erasure coding

È possibile visualizzare i dettagli di un profilo di erasure coding e rinominare un profilo, se necessario. È possibile disattivare un profilo di erasure coding se non è attualmente utilizzato in nessuna regola ILM.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "autorizzazioni di accesso richieste".

Visualizza i dettagli del profilo di erasure coding

È possibile visualizzare i dettagli di un profilo di erasure coding per determinarne lo stato, lo schema di erasure coding utilizzato e altre informazioni.

Fasi

1. Selezionare **ILM** > **Erasure coding**.
2. Selezionare il profilo. Viene visualizzata la pagina dei dettagli del profilo.
3. In alternativa, è possibile visualizzare la scheda regole ILM per un elenco di regole ILM che utilizzano il profilo e i criteri ILM che utilizzano tali regole.
4. Facoltativamente, visualizzare la scheda nodi di archiviazione per i dettagli su ciascun nodo di archiviazione nel pool di archiviazione del profilo, ad esempio il sito in cui si trova e l'utilizzo dello storage.

Rinominare un profilo con erasure coding

Si consiglia di rinominare un profilo di erasure coding in modo da renderlo più ovvio.

Fasi

1. Selezionare **ILM** > **Erasure coding**.
2. Selezionare il profilo che si desidera rinominare.
3. Selezionare **Rinomina**.
4. Immettere un nome univoco per il profilo di erasure coding.

   Il nome del profilo di erasure coding viene aggiunto al nome del pool di storage nelle istruzioni di posizionamento di una regola ILM.

   > I nomi dei profili di erasure coding devono essere univoci. Si verifica un errore di convalida se si utilizza il nome di un profilo esistente, anche se tale profilo è stato disattivato.

5. Selezionare **Salva**.

Disattivare un profilo di erasure coding

È possibile disattivare un profilo di erasure coding se non si prevede più di utilizzarlo e se il profilo non è attualmente utilizzato in nessuna regola ILM.

> Verificare che non siano in corso operazioni di riparazione dei dati sottoposte a erasure coding o procedure di decommissionamento. Viene visualizzato un messaggio di errore se si tenta di disattivare un profilo di erasure coding mentre è in corso una di queste operazioni.

A proposito di questa attività

StorageGRID ti impedisce di disattivare un profilo di erasure coding se si verifica una delle seguenti condizioni:

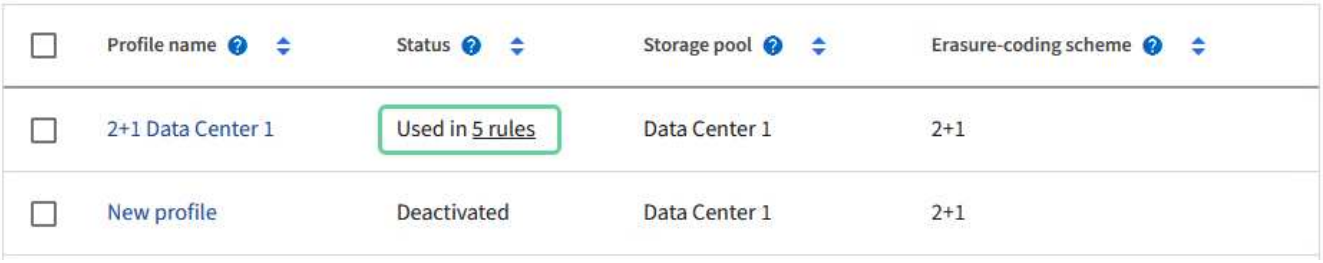
- Il profilo di erasure coding è attualmente utilizzato in una regola ILM.
- Il profilo di erasure coding non viene più utilizzato in nessuna regola ILM, ma i dati degli oggetti e i frammenti di parità per il profilo esistono ancora.

Fasi

1. Selezionare **ILM** > **Erasure coding**.

2. Nella scheda attivo, esaminare la colonna **Stato** per confermare che il profilo di erasure coding che si desidera disattivare non è utilizzato in nessuna regola ILM.

   Non è possibile disattivare un profilo di erasure coding se è utilizzato in qualsiasi regola ILM. Nell'esempio, il profilo 2+1 Data Center 1 viene utilizzato in almeno una regola ILM.



3. Se il profilo viene utilizzato in una regola ILM, attenersi alla seguente procedura:
   a. Selezionare **ILM** > **regole**.
   b. Selezionare ciascuna regola ed esaminare il diagramma di conservazione per determinare se la regola utilizza il profilo di erasure coding che si desidera disattivare.
   c. Se la regola ILM utilizza il profilo di erasure coding che si desidera disattivare, determinare se la regola è utilizzata in qualsiasi criterio ILM.
   d. Completare i passaggi aggiuntivi nella tabella, in base alla posizione in cui viene utilizzato il profilo di erasure coding.

Dove è stato utilizzato il profilo?	**Ulteriori passaggi da eseguire prima di disattivare il profilo**	**Fare riferimento a queste istruzioni aggiuntive**
Mai utilizzato in nessuna regola ILM	Non sono necessari passaggi aggiuntivi. Continuare con questa procedura.	*Nessuno*
In una regola ILM che non è mai stata utilizzata in alcun criterio ILM	i. Modificare o eliminare tutte le regole ILM interessate. Se si modifica la regola, rimuovere tutti i posizionamenti che utilizzano il profilo di erasure coding. ii. Continuare con questa procedura.	"Utilizzare le regole ILM e i criteri ILM"

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Fare riferimento a queste istruzioni aggiuntive
In una regola ILM che è attualmente in un criterio ILM attivo	i. Clonazione della policy. ii. Rimuovere la regola ILM che utilizza il profilo di erasure coding. iii. Aggiungere una o più nuove regole ILM per garantire la protezione degli oggetti. iv. Salvare, simulare e attivare la nuova policy. v. Attendere che il nuovo criterio venga applicato e che gli oggetti esistenti vengano spostati in nuove posizioni in base alle nuove regole aggiunte. **Nota:** a seconda del numero di oggetti e delle dimensioni del sistema StorageGRID, potrebbero essere necessarie settimane o addirittura mesi per le operazioni ILM per spostare gli oggetti in nuove posizioni, in base alle nuove regole ILM. Mentre è possibile tentare di disattivare un profilo di erasure coding mentre è ancora associato ai dati, l'operazione di disattivazione non riesce. Se il profilo non è ancora pronto per la disattivazione, viene visualizzato un messaggio di errore. vi. Modificare o eliminare la regola rimossa dal criterio. Se si modifica la regola, rimuovere tutti i posizionamenti che utilizzano il profilo di erasure coding. vii. Continuare con questa procedura.	"Creare un criterio ILM" "Utilizzare le regole ILM e i criteri ILM"
In una regola ILM che è attualmente in un criterio ILM	i. Modificare il criterio. ii. Rimuovere la regola ILM che utilizza il profilo di erasure coding. iii. Aggiungere una o più nuove regole ILM per garantire la protezione di tutti gli oggetti. iv. Salvare il criterio. v. Modificare o eliminare la regola rimossa dal criterio. Se si modifica la regola, rimuovere tutti i posizionamenti che utilizzano il profilo di erasure coding. vi. Continuare con questa procedura.	"Creare un criterio ILM" "Utilizzare le regole ILM e i criteri ILM"

e. Aggiornare la pagina Erasure-Coding Profiles per assicurarsi che il profilo non venga utilizzato in una regola ILM.

4. Se il profilo non viene utilizzato in una regola ILM, selezionare il pulsante di opzione e selezionare **Disattiva**. Viene visualizzata la finestra di dialogo Disattiva profilo di erasure coding.

> È possibile selezionare più profili da disattivare contemporaneamente, a condizione che ciascun profilo non venga utilizzato in alcuna regola.

5. Se sei sicuro di voler disattivare il profilo, seleziona **Disattiva**.

Risultati

- Se StorageGRID è in grado di disattivare il profilo di erasure coding, il suo stato è disattivato. Non è più possibile selezionare questo profilo per nessuna regola ILM. Non puoi riattivare un profilo disattivato.
- Se StorageGRID non è in grado di disattivare il profilo, viene visualizzato un messaggio di errore. Ad esempio, se i dati dell'oggetto sono ancora associati a questo profilo, viene visualizzato un messaggio di errore. Potrebbe essere necessario attendere alcune settimane prima di provare di nuovo il processo di disattivazione.

Configurazione delle regioni (opzionale e solo S3)

Le regole ILM possono filtrare gli oggetti in base alle aree in cui vengono creati i bucket S3, consentendo di memorizzare oggetti da diverse aree in diverse posizioni di storage.

Se si desidera utilizzare un'area del bucket S3 come filtro in una regola, è necessario innanzitutto creare le regioni che possono essere utilizzate dai bucket nel sistema.

> Una volta creato il bucket, non è possibile modificare l'area di un bucket.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Quando si crea un bucket S3, è possibile specificare che il bucket venga creato in un'area specifica. La specifica di una regione consente al bucket di essere geograficamente vicino ai propri utenti, in modo da ottimizzare la latenza, ridurre al minimo i costi e soddisfare i requisiti normativi.

Quando si crea una regola ILM, è possibile utilizzare la regione associata a un bucket S3 come filtro avanzato. Ad esempio, è possibile progettare una regola che si applica solo agli oggetti nei bucket S3 creati in `us-west-2` regione. È quindi possibile specificare che le copie di tali oggetti vengano collocate sui nodi di storage in un sito del data center all'interno di tale regione per ottimizzare la latenza.

Durante la configurazione delle regioni, attenersi alle seguenti linee guida:

- Per impostazione predefinita, tutti i bucket sono considerati come appartenenti a. `us-east-1` regione.
- È necessario creare le regioni utilizzando Grid Manager prima di poter specificare un'area non predefinita quando si creano i bucket utilizzando l'API Tenant Manager o Tenant Management o con l'elemento di richiesta LocationConstraint per le richieste API S3 PUT bucket. Si verifica un errore se una richiesta PUT bucket utilizza un'area non definita in StorageGRID.
- Quando si crea il bucket S3, è necessario utilizzare il nome esatto della regione. I nomi delle regioni rilevano la distinzione tra maiuscole e minuscole. I caratteri validi sono numeri, lettere e trattini.

EU non è considerato un alias per eu-West-1. Se si desidera utilizzare la regione EU o eu-West-1, è necessario utilizzare il nome esatto.

- Non è possibile eliminare o modificare una regione se utilizzata in una regola assegnata a qualsiasi criterio (attivo o inattivo).
- Se si utilizza un'area non valida come filtro avanzato in una regola ILM, non è possibile aggiungere tale regola a un criterio.

  Se si utilizza una regione come filtro avanzato in una regola ILM ma si elimina tale regione in un secondo momento o se si utilizza l'API Grid Management per creare una regola e specificare una regione non definita.

- Se si elimina una regione dopo averla utilizzata per creare un bucket S3, sarà necessario aggiungerla nuovamente se si desidera utilizzare il filtro avanzato Location Constraint per trovare gli oggetti in tale bucket.

Fasi

1. Selezionare **ILM** > **regioni**.

   Viene visualizzata la pagina regioni, con le regioni attualmente definite. **Regione 1** mostra la regione predefinita, `us-east-1`, che non possono essere modificati o rimossi.

2. Per aggiungere una regione:
   a. Selezionare **Aggiungi un'altra regione**.
   b. Immettere il nome di una regione che si desidera utilizzare durante la creazione dei bucket S3.

      Quando si crea il bucket S3 corrispondente, è necessario utilizzare il nome esatto della regione come elemento di richiesta LocationConstraint.

3. Per rimuovere una regione non utilizzata, selezionare l'icona di eliminazione ✕.

   Se si tenta di rimuovere una regione attualmente utilizzata in qualsiasi criterio (attivo o inattivo), viene visualizzato un messaggio di errore.

4. Una volta apportate le modifiche, selezionare **Salva**.

   È ora possibile selezionare queste regioni dalla sezione Advanced filters (filtri avanzati) nel passaggio 1 della creazione guidata regola ILM. Vedere "Utilizzare filtri avanzati nelle regole ILM".

Creare una regola ILM

Creare una regola ILM: Panoramica

Per gestire gli oggetti, creare un set di regole ILM (Information Lifecycle Management) e organizzarle in un criterio ILM.

Ogni oggetto acquisito nel sistema viene valutato in base al criterio attivo. Quando una regola del criterio corrisponde ai metadati di un oggetto, le istruzioni della regola determinano le azioni eseguite da StorageGRID per copiare e memorizzare tale oggetto.

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.

Elementi di una regola ILM

Una regola ILM ha tre elementi:

- **Filtering Criteria**: I filtri di base e avanzati di una regola definiscono a quali oggetti si applica la regola. Se un oggetto corrisponde a tutti i filtri, StorageGRID applica la regola e crea le copie dell'oggetto specificate nelle istruzioni di posizionamento della regola.
- **Istruzioni di posizionamento**: Le istruzioni di posizionamento di una regola definiscono il numero, il tipo e la posizione delle copie degli oggetti. Ciascuna regola può includere una sequenza di istruzioni di posizionamento per modificare il numero, il tipo e la posizione delle copie degli oggetti nel tempo. Quando scade il periodo di tempo per un posizionamento, le istruzioni nel posizionamento successivo vengono applicate automaticamente dalla valutazione ILM successiva.
- **Ingest Behavior**: Il comportamento di acquisizione di una regola consente di scegliere in che modo gli oggetti filtrati dalla regola vengono protetti durante l'acquisizione (quando un client S3 o Swift salva un oggetto nella griglia).

Filtraggio delle regole ILM

Quando si crea una regola ILM, si specificano i filtri per identificare gli oggetti a cui si applica la regola.

Nel caso più semplice, una regola potrebbe non utilizzare alcun filtro. Qualsiasi regola che non utilizza filtri si applica a tutti gli oggetti, quindi deve essere l'ultima regola (predefinita) in un criterio ILM. La regola predefinita fornisce istruzioni di archiviazione per gli oggetti che non corrispondono ai filtri di un'altra regola.

- I filtri di base consentono di applicare regole diverse a gruppi di oggetti distinti e di grandi dimensioni. Questi filtri consentono di applicare una regola a account tenant specifici, bucket S3 specifici o container Swift o entrambi.

  I filtri di base offrono un metodo semplice per applicare regole diverse a un numero elevato di oggetti. Ad esempio, potrebbe essere necessario memorizzare i record finanziari della tua azienda per soddisfare i requisiti normativi, mentre potrebbe essere necessario memorizzare i dati del reparto di marketing per facilitare le operazioni quotidiane. Dopo aver creato account tenant separati per ciascun reparto o aver separato i dati dai diversi reparti in bucket S3 separati, è possibile creare facilmente una regola che si applica a tutti i record finanziari e una seconda regola che si applica a tutti i dati di marketing.

- I filtri avanzati offrono un controllo granulare. È possibile creare filtri per selezionare gli oggetti in base alle seguenti proprietà dell'oggetto:
  - Tempo di acquisizione
  - Ora dell'ultimo accesso
  - Nome completo o parziale dell'oggetto (Key)
  - Vincolo di posizione (solo S3)
  - Dimensione dell'oggetto
  - Metadati dell'utente
  - Tag Object (solo S3)

È possibile filtrare gli oggetti in base a criteri molto specifici. Ad esempio, gli oggetti memorizzati dal reparto di

imaging di un ospedale potrebbero essere utilizzati frequentemente quando hanno meno di 30 giorni e poco tempo dopo, mentre gli oggetti che contengono informazioni sulle visite dei pazienti potrebbero dover essere copiati nel reparto di fatturazione della sede centrale della rete sanitaria. È possibile creare filtri che identifichino ciascun tipo di oggetto in base al nome dell'oggetto, alle dimensioni, ai tag di oggetto S3 o a qualsiasi altro criterio pertinente, quindi creare regole separate per memorizzare ciascun set di oggetti in modo appropriato.

È possibile combinare i filtri in base alle esigenze in una singola regola. Ad esempio, il reparto marketing potrebbe voler memorizzare file di immagini di grandi dimensioni in modo diverso dai record dei vendor, mentre il reparto risorse umane potrebbe dover memorizzare i record del personale in un'area geografica specifica e le informazioni sulle policy a livello centrale. In questo caso, è possibile creare regole che filtrino in base all'account tenant per separare i record da ciascun reparto, utilizzando i filtri in ciascuna regola per identificare il tipo specifico di oggetti a cui si applica la regola.

Istruzioni per il posizionamento delle regole ILM

Le istruzioni di posizionamento determinano dove, quando e come vengono memorizzati i dati degli oggetti. Una regola ILM può includere una o più istruzioni di posizionamento. Ogni istruzione di posizionamento si applica a un singolo periodo di tempo.

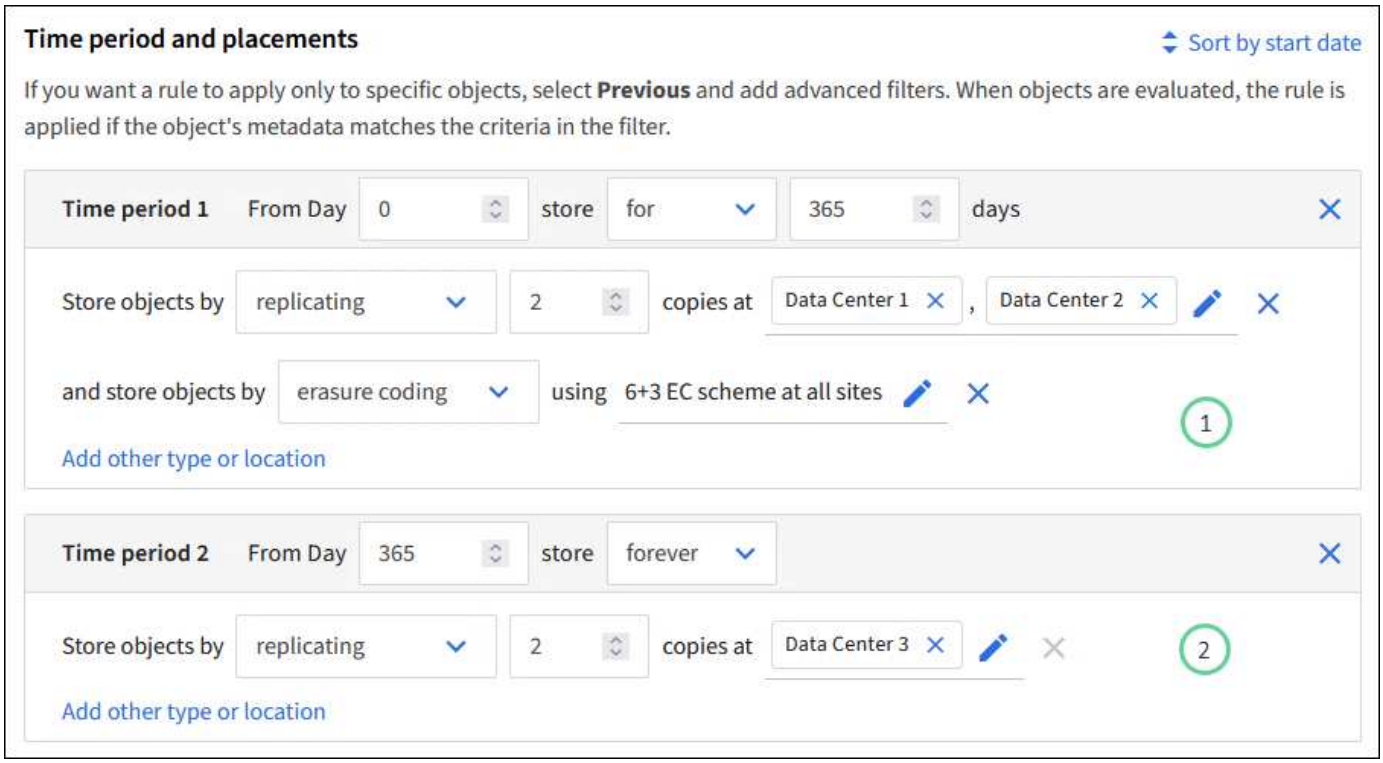
Quando si creano le istruzioni per il posizionamento:

- Si inizia specificando l'ora di riferimento, che determina quando iniziano le istruzioni di posizionamento. Il tempo di riferimento potrebbe essere quando un oggetto viene acquisito, quando si accede a un oggetto, quando un oggetto con versione diventa non corrente o un tempo definito dall'utente.
- Quindi, specificare quando applicare il posizionamento rispetto al tempo di riferimento. Ad esempio, un posizionamento potrebbe iniziare il giorno 0 e continuare per 365 giorni, rispetto a quando l'oggetto è stato acquisito.
- Infine, specificare il tipo di copie (replica o erasure coding) e la posizione in cui sono memorizzate le copie. Ad esempio, è possibile memorizzare due copie replicate in due siti diversi.

Ciascuna regola può definire più posizioni per un singolo periodo di tempo e posizioni diverse per periodi di tempo diversi.

- Per posizionare oggetti in più posizioni durante un singolo periodo di tempo, selezionare **Aggiungi altro tipo o posizione** per aggiungere più di una riga per quel periodo di tempo.
- Per posizionare oggetti in posizioni diverse in periodi di tempo diversi, selezionare **Aggiungi un altro periodo di tempo** per aggiungere il periodo di tempo successivo. Quindi, specificare una o più righe entro il periodo di tempo.

L'esempio mostra due istruzioni di posizionamento nella pagina Definisci posizioni della creazione guidata regola ILM.



La prima istruzione di posizionamento (1) ha due linee per il primo anno:

- La prima riga crea due copie di oggetti replicate in due siti del data center.
- La seconda riga crea una copia con erasure coding pari a 6+3 usando tutti i siti del data center.

La seconda istruzione di posizionamento (2) crea due copie dopo un anno e le conserva per sempre.

Quando si definisce il set di istruzioni di posizionamento per una regola, è necessario assicurarsi che almeno un'istruzione di posizionamento inizi al giorno 0, che non vi siano intervalli tra i periodi di tempo definiti, e che l'istruzione finale di posizionamento continui per sempre o fino a quando non si richiede più alcuna copia oggetto.

Alla scadenza di ogni periodo di tempo previsto dalla regola, vengono applicate le istruzioni per il posizionamento dei contenuti per il periodo di tempo successivo. Vengono create nuove copie di oggetti e tutte le copie non necessarie vengono eliminate.

Comportamento di acquisizione delle regole ILM

Il comportamento di acquisizione controlla se le copie degli oggetti vengono posizionate immediatamente in base alle istruzioni della regola o se vengono eseguite copie temporanee e le istruzioni di posizionamento vengono applicate in un secondo momento. Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

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

Informazioni correlate

- "Opzioni di acquisizione"
- "Vantaggi, svantaggi e limitazioni delle opzioni di acquisizione"
- "L'interazione tra coerenza e regole ILM per influire sulla protezione dei dati"

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applicano solo agli oggetti appartenenti al tenant A.
- Eseguire due copie replicate di tali oggetti e memorizzare ciascuna copia in un sito diverso.
- Conserva le due copie "per sempre", 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.
- Utilizzare l'opzione bilanciato 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.

Informazioni correlate

- "Che cos'è un pool di storage"
- "Che cos'è un Cloud Storage Pool"

Accedere alla procedura guidata Crea una regola ILM

Le regole ILM consentono di gestire il posizionamento dei dati degli oggetti nel tempo. Per creare una regola ILM, utilizzare la procedura guidata Crea una regola ILM.

> Se si desidera creare la regola ILM predefinita per un criterio, seguire "Istruzioni per la creazione di una regola ILM predefinita" invece.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Se si desidera specificare a quali account tenant si applica questa regola, si dispone di "Autorizzazione account tenant" Oppure si conosce l'ID account per ciascun account.
- Se si desidera che la regola filtri gli oggetti sui metadati dell'ultimo accesso, gli ultimi aggiornamenti dell'ora di accesso devono essere attivati dal bucket per S3 o dal container per Swift.
- Hai configurato qualsiasi pool di storage cloud che intendi utilizzare. Vedere "Creare un pool di storage cloud".
- Conosci già "opzioni di acquisizione".
- Se è necessario creare una regola conforme per l'utilizzo con il blocco oggetti S3, si ha familiarità con "Requisiti per il blocco oggetti S3".

- Facoltativamente, hai guardato il video: "Video: Regole di gestione del ciclo di vita delle informazioni in StorageGRID 11,8".

A proposito di questa attività

Quando si creano regole ILM:

- Prendere in considerazione la topologia e le configurazioni dello storage del sistema StorageGRID.
- Considerare i tipi di copie degli oggetti da creare (replicate o sottoposte a erasure coding) e il numero di copie di ciascun oggetto necessario.
- Determinare i tipi di metadati degli oggetti utilizzati nelle applicazioni che si connettono al sistema StorageGRID. Le regole ILM filtrano gli oggetti in base ai metadati.
- Considerare dove si desidera che le copie a oggetti vengano collocate nel tempo.
- Decidere quale opzione di acquisizione utilizzare (Balanced, Strict o Dual Commit).

Fasi

1. Selezionare **ILM** > **regole**.
2. Selezionare **Crea**. "Fase 1 (inserire i dettagli)" Viene visualizzata la procedura guidata Crea una regola ILM.

Fase 1 di 3: Inserire i dettagli

La fase **Enter details** della creazione guidata di una regola ILM consente di immettere un nome e una descrizione per la regola e di definire i filtri per la regola.

L'immissione di una descrizione e la definizione dei filtri per la regola sono facoltativi.

A proposito di questa attività

Quando si valuta un oggetto rispetto a un "Regola ILM", StorageGRID confronta i metadati dell'oggetto con i filtri della regola. Se i metadati dell'oggetto corrispondono a tutti i filtri, StorageGRID utilizza la regola per posizionare l'oggetto. È possibile progettare una regola da applicare a tutti gli oggetti, oppure specificare filtri di base, come uno o più account tenant o nomi bucket, o filtri avanzati, come la dimensione dell'oggetto o i metadati dell'utente.

Fasi

1. Immettere un nome univoco per la regola nel campo **Nome**.
2. Se si desidera, inserire una breve descrizione per la regola nel campo **Descrizione**.

   È necessario descrivere lo scopo o la funzione della regola in modo da poterne riconoscere in un secondo momento.

3. Facoltativamente, selezionare uno o più account tenant S3 o Swift a cui si applica questa regola. Se questa regola è applicabile a tutti i tenant, lasciare vuoto questo campo.

   Se non si dispone dell'autorizzazione di accesso root o dell'autorizzazione per gli account tenant, non è possibile selezionare i tenant dall'elenco. Immettere invece l'ID tenant o più ID come stringa delimitata da virgole.

4. Facoltativamente, specificare i bucket S3 o i container Swift a cui si applica questa regola.

Se si seleziona **Applica a tutti i bucket** (impostazione predefinita), la regola si applica a tutti i bucket S3 o contenitori Swift.

5. Per i tenant S3, selezionare **Yes** (Sì) per applicare la regola solo alle versioni di oggetti precedenti nei bucket S3 che hanno attivato il controllo delle versioni.

   Se si seleziona **Sì**, l'opzione "ora non corrente" viene selezionata automaticamente per ora di riferimento in "Passaggio 2 della creazione guidata di una regola ILM".

   > L'ora non corrente si applica solo agli oggetti S3 nei bucket abilitati per il controllo delle versioni. Vedere "Operazioni su benne, PutBucketVersioning" e. "Gestire gli oggetti con S3 Object Lock".

   È possibile utilizzare questa opzione per ridurre l'impatto dello storage degli oggetti con versione filtrando le versioni degli oggetti non correnti. Vedere "Esempio 4: Regole ILM e policy per gli oggetti con versione S3".

6. In alternativa, selezionare **Aggiungi un filtro avanzato** per specificare filtri aggiuntivi.

   Se non si configura il filtraggio avanzato, la regola si applica a tutti gli oggetti che corrispondono ai filtri di base. Per ulteriori informazioni sui filtri avanzati, vedere Utilizzare filtri avanzati nelle regole ILM e. Specificare più tipi di metadati e valori.

7. Selezionare **continua**. "Fase 2 (definizione delle posizioni)" Viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare filtri avanzati nelle regole ILM

Il filtraggio avanzato consente di creare regole ILM applicabili solo a oggetti specifici in base ai metadati. Quando si imposta il filtraggio avanzato per una regola, si seleziona il tipo di metadati che si desidera associare, si seleziona un operatore e si specifica un valore di metadati. Quando si valutano gli oggetti, la regola ILM viene applicata solo agli oggetti che hanno metadati corrispondenti al filtro avanzato.

La tabella mostra i tipi di metadati che è possibile specificare nei filtri avanzati, gli operatori che è possibile utilizzare per ogni tipo di metadati e i valori di metadati previsti.

Tipo di metadati	Operatori supportati	Valore dei metadati
Tempo di acquisizione	• è • non lo è • è prima • è acceso o prima • è dopo • sia acceso o dopo	Ora e data di acquisizione dell'oggetto. **Nota:** per evitare problemi di risorse quando si attiva un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Ingest Time in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare Ingest Time (tempo di acquisizione) su un valore maggiore o uguale al tempo approssimativo in cui la nuova policy verrà applicata per garantire che gli oggetti esistenti non vengano spostati inutilmente.

Tipo di metadati	Operatori supportati	Valore dei metadati
Chiave	• uguale a • non uguale • contiene • non contiene • inizia con • non inizia con • termina con • non finisce con	Tutto o parte di una chiave oggetti S3 o Swift univoca. Ad esempio, è possibile associare gli oggetti che terminano con `.txt` oppure inizia con `test-object/`.
Ora dell'ultimo accesso	• è • non lo è • è prima • è acceso o prima • è dopo • sia acceso o dopo	Ora e data dell'ultimo recupero dell'oggetto (letto o visualizzato). **Nota:** se si prevede di "usa l'ultimo tempo di accesso" Come filtro avanzato, gli ultimi aggiornamenti del tempo di accesso devono essere attivati per il bucket S3 o il container Swift.
Vincolo di posizione (solo S3)	• uguale a • non uguale	La regione in cui è stato creato un bucket S3. Utilizzare **ILM** > **regioni** per definire le regioni visualizzate. **Nota:** Un valore di US-East-1 corrisponde agli oggetti nei bucket creati nella regione US-East-1 e agli oggetti nei bucket che non hanno alcuna regione specificata. Vedere "Configurazione delle regioni (opzionale e solo S3)".
Dimensione dell'oggetto	• uguale a • non uguale • inferiore a. • minore o uguale a. • maggiore di • maggiore o uguale a.	La dimensione dell'oggetto. L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

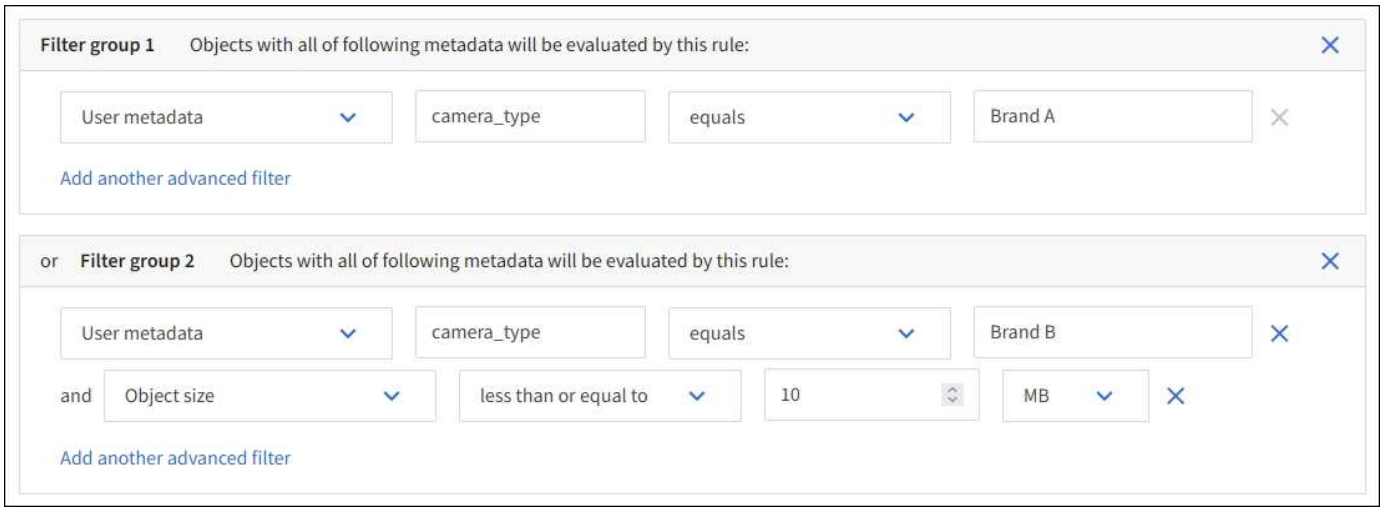
Tipo di metadati	Operatori supportati	Valore dei metadati
Metadati dell'utente	• contiene • termina con • uguale a • esiste • inizia con • non contiene • non finisce con • non uguale • non esiste • non inizia con	Coppia valore-chiave, dove **Nome metadati utente** è la chiave e **valore metadati** è il valore. Ad esempio, per filtrare gli oggetti con metadati utente di `color=blue`, specificare `color` Per **Nome metadati utente**, `equals` per l'operatore, e. `blue` Per **valore metadati**. **Nota:** i nomi dei metadati utente non distinguono tra maiuscole e minuscole; i valori dei metadati utente distinguono tra maiuscole e minuscole.
Tag Object (solo S3)	• contiene • termina con • uguale a • esiste • inizia con • non contiene • non finisce con • non uguale • non esiste • non inizia con	Coppia key-value, dove **nome tag oggetto** è la chiave e **valore tag oggetto** è il valore. Ad esempio, per filtrare gli oggetti che hanno un tag Object di `Image=True`, specificare `Image` Per **nome tag oggetto**, `equals` per l'operatore, e. `True` Per **valore tag oggetto**. **Nota:** i nomi dei tag degli oggetti e i valori dei tag degli oggetti fanno distinzione tra maiuscole e minuscole. È necessario inserire questi elementi esattamente come sono stati definiti per l'oggetto.

Specificare più tipi di metadati e valori

Quando si definisce il filtraggio avanzato, è possibile specificare più tipi di metadati e più valori di metadati. Ad esempio, se si desidera che una regola corrisponda a oggetti di dimensioni comprese tra 10 MB e 100 MB, selezionare il tipo di metadati **Object size** e specificare due valori di metadati.

- Il primo valore di metadati specifica oggetti superiori o uguali a 10 MB.
- Il secondo valore di metadati specifica gli oggetti inferiori o uguali a 100 MB.

L'utilizzo di più voci consente di avere un controllo preciso su quali oggetti vengono associati. Nell'esempio seguente, la regola si applica agli oggetti che hanno il marchio A o il marchio B come valore dei metadati utente camera_TYPE. Tuttavia, la regola si applica solo agli oggetti Brand B di dimensioni inferiori a 10 MB.



Fase 2 di 3: Definizione delle posizioni

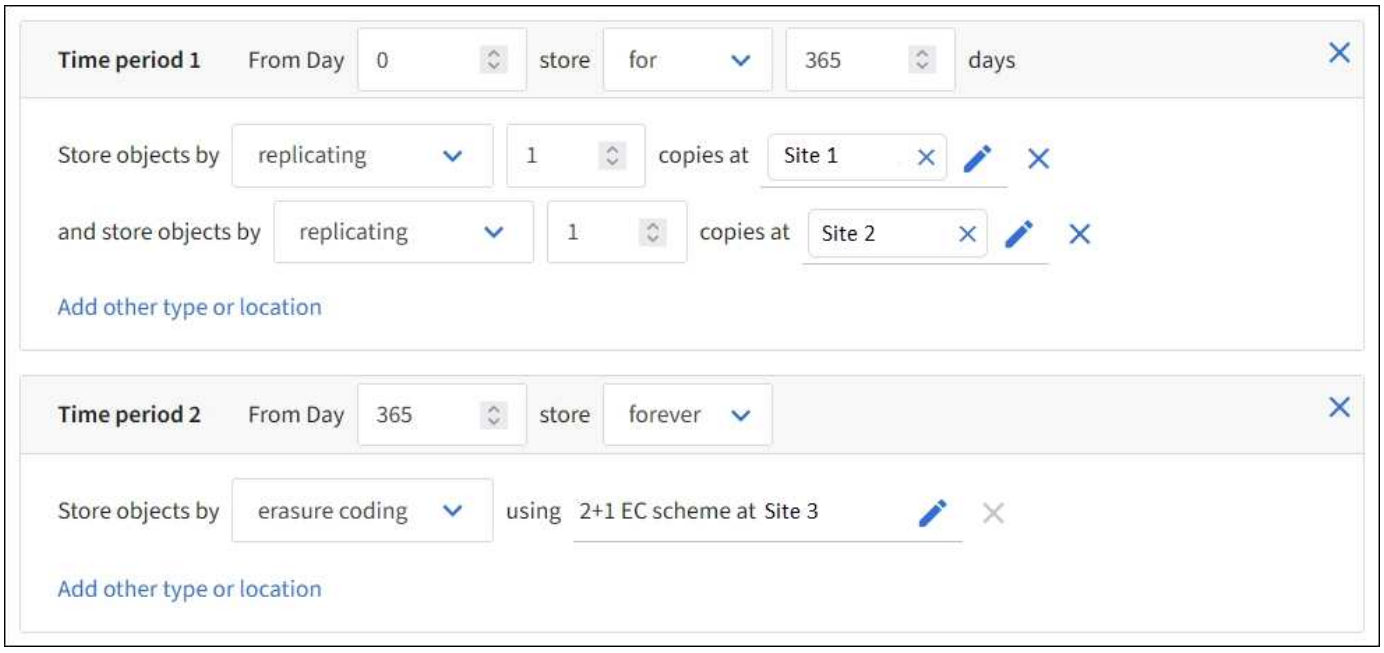
La fase **Definisci posizionamenti** della procedura guidata Crea regola ILM consente di definire le istruzioni di posizionamento che determinano la durata dell'archiviazione degli oggetti, il tipo di copie (replicate o sottoposte a erasure coding), la posizione di archiviazione e il numero di copie.

A proposito di questa attività

Una regola ILM può includere una o più istruzioni di posizionamento. Ogni istruzione di posizionamento si applica a un singolo periodo di tempo. Quando si utilizzano più istruzioni, i periodi di tempo devono essere contigui e almeno un'istruzione deve iniziare il giorno 0. Le istruzioni possono continuare per sempre o fino a quando non sono più necessarie copie di oggetti.

Ogni istruzione di posizionamento può avere più righe se si desidera creare diversi tipi di copie o utilizzare posizioni diverse durante tale periodo di tempo.

In questo esempio, la regola ILM memorizza una copia replicata nel sito 1 e una copia replicata nel sito 2 per il primo anno. Dopo un anno, viene creata una copia 2+1 con codice di cancellazione e salvata in un solo sito.



Fasi

1. Per **Reference Time** (tempo di riferimento), selezionare il tipo di tempo da utilizzare per il calcolo dell'ora di inizio di un'istruzione di posizionamento.

Opzione	Descrizione
Tempo di acquisizione	L'ora in cui l'oggetto è stato acquisito.
Ora dell'ultimo accesso	L'ora in cui l'oggetto è stato recuperato per l'ultima volta (letto o visualizzato). **Nota:** per utilizzare questa opzione, è necessario attivare gli aggiornamenti dell'ultimo tempo di accesso per il bucket S3 o il container Swift. Vedere "USA l'ultimo tempo di accesso nelle regole ILM".
Tempo di creazione definito dall'utente	Tempo specificato nei metadati definiti dall'utente.
Ora non corrente	L'opzione "ora non corrente" viene selezionata automaticamente se si seleziona **Sì** per la domanda "Applica questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?" pollici "Fase 1 della creazione guidata di una regola ILM".

> Se si desidera creare una regola conforme, selezionare **Ingest Time**. Vedere "Gestire gli oggetti con S3 Object Lock".

2. Nella sezione **periodo di tempo e posizionamenti**, inserire un'ora di inizio e una durata per il primo periodo di tempo.

   Ad esempio, è possibile specificare dove memorizzare gli oggetti per il primo anno (*dal giorno 0 memorizzare per 365 giorni*). Almeno un'istruzione deve iniziare al giorno 0.

3. Se si desidera creare copie replicate:
   a. Dall'elenco a discesa **Memorizza oggetti per**, selezionare **replica**.
   b. Selezionare il numero di copie che si desidera eseguire.

      Se si modifica il numero di copie in 1, viene visualizzato un avviso. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Vedere "Perché non utilizzare la replica a copia singola".

      Per evitare il rischio, effettuare una o più delle seguenti operazioni:

      - Aumentare il numero di copie per il periodo di tempo.
      - Aggiungere copie ad altri pool di storage o a un pool di storage cloud.
      - Selezionare **erasure coding** invece di **Replicing**.

      È possibile ignorare questo avviso se questa regola crea già più copie per tutti i periodi di tempo.

   c. Nel campo **Copies at**, selezionare i pool di storage che si desidera aggiungere.

Se si specifica un solo pool di storage, tenere presente che StorageGRID può memorizzare solo una copia replicata di un oggetto su un nodo di storage specifico. Se la griglia include tre nodi di storage e si seleziona 4 come numero di copie, verranno eseguite solo tre copie e 8212 una copia per ciascun nodo di storage.

> Viene attivato l'avviso **ILM placement unachievable** per indicare che la regola ILM non può essere applicata completamente.

Se si specificano più pool di storage, tenere presenti le seguenti regole:

- Il numero di copie non può essere superiore al numero di pool di storage.
- Se il numero di copie corrisponde al numero di pool di storage, viene memorizzata una copia dell'oggetto in ciascun pool di storage.
- Se il numero di copie è inferiore al numero di pool di storage, una copia viene memorizzata nel sito di acquisizione e il sistema distribuisce le copie rimanenti per mantenere bilanciato l'utilizzo del disco tra i pool, garantendo che nessun sito riceva più di una copia di un oggetto.
- Se i pool di storage si sovrappongono (contengono gli stessi nodi di storage), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. Per questo motivo, non specificare il pool di storage di tutti i nodi di storage (StorageGRID 11.6 e versioni precedenti) e un altro pool di storage.

4. Se si desidera creare una copia con codice di cancellazione:
   a. Dall'elenco a discesa **Memorizza oggetti per**, selezionare **erasure coding**.

      > L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

   b. Se non è stato aggiunto un filtro delle dimensioni dell'oggetto per un valore superiore a 200 KB, selezionare **precedente** per tornare al passaggio 1. Quindi, selezionare **Aggiungi un filtro avanzato** e impostare un filtro **dimensione oggetto** su qualsiasi valore maggiore di 200 KB.
   c. Selezionare il pool di storage che si desidera aggiungere e lo schema di erasure coding che si desidera utilizzare.

      La posizione dello storage per una copia sottoposta a erasure coding include il nome dello schema di erasure coding, seguito dal nome del pool di storage.

5. Facoltativamente:
   a. Selezionare **Aggiungi altro tipo o ubicazione** per creare copie aggiuntive in posizioni diverse.
   b. Selezionare **Add another time period** (Aggiungi un altro periodo di tempo) per aggiungere diversi periodi di tempo.

      > Gli oggetti vengono eliminati automaticamente alla fine del periodo di tempo finale, a meno che un altro periodo di tempo non termini con **per sempre**.

6. Se si desidera memorizzare oggetti in un pool di storage cloud:
   a. Nell'elenco a discesa **Memorizza oggetti per**, selezionare **replica**.
   b. Selezionare il campo **Copies at**, quindi selezionare un Cloud Storage Pool.

      Quando si utilizzano i Cloud Storage Pool, tenere presenti le seguenti regole:

- Non puoi selezionare più di un Cloud Storage Pool in una singola istruzione di posizionamento. Allo stesso modo, non è possibile selezionare un Cloud Storage Pool e un pool di storage nelle stesse istruzioni di posizionamento.
- È possibile memorizzare solo una copia di un oggetto in un determinato pool di storage cloud. Se si imposta **copie** su 2 o più, viene visualizzato un messaggio di errore.
- Non è possibile memorizzare più copie di un oggetto contemporaneamente in nessun Cloud Storage Pool. Viene visualizzato un messaggio di errore se più posizioni che utilizzano un pool di storage cloud presentano date sovrapposte o se più righe nello stesso posizionamento utilizzano un pool di storage cloud.
- È possibile memorizzare un oggetto in un Cloud Storage Pool contemporaneamente all'archiviazione dell'oggetto come copie replicate o con erasure coding in StorageGRID. Tuttavia, è necessario includere più di una riga nelle istruzioni di posizionamento per il periodo di tempo, in modo da poter specificare il numero e il tipo di copie per ciascuna posizione.

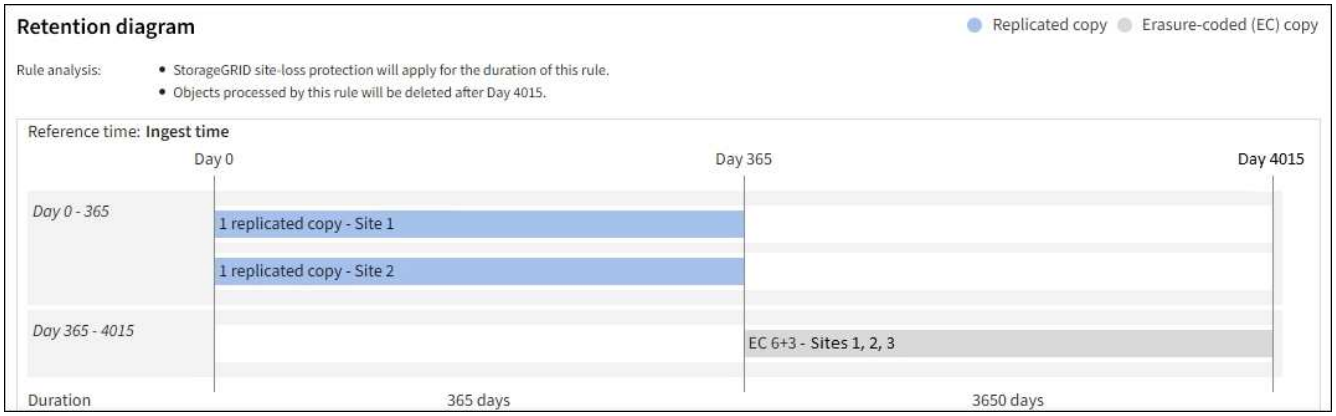
7. Nel diagramma di conservazione, confermare le istruzioni per il posizionamento.

   In questo esempio, la regola ILM memorizza una copia replicata nel sito 1 e una copia replicata nel sito 2 per il primo anno. Dopo un anno e per altri 10 anni, una copia con codice di cancellazione 6+3 verrà salvata in tre sedi. Dopo 11 anni totali, gli oggetti verranno cancellati da StorageGRID.

   La sezione analisi delle regole del diagramma di conservazione riporta:

   - La protezione contro la perdita di sito di StorageGRID verrà applicata per tutta la durata di questa regola.
   - Gli oggetti elaborati da questa regola verranno cancellati dopo il giorno 4015.

     Vedere "Abilita la protezione contro la perdita di sito."



8. Selezionare **continua**. "Fase 3 (selezionare il comportamento di acquisizione)" Viene visualizzata la procedura guidata Crea una regola ILM.

USA l'ultimo tempo di accesso nelle regole ILM

In una regola ILM, è possibile utilizzare l'ultimo tempo di accesso come ora di riferimento. Ad esempio, è possibile lasciare oggetti che sono stati visualizzati negli ultimi tre mesi sui nodi di storage locali, mentre si spostano oggetti che non sono stati visualizzati di recente in una posizione off-site. È inoltre possibile utilizzare l'ultimo tempo di accesso come filtro avanzato se si desidera che una regola ILM si applichi solo agli oggetti a cui è stato effettuato l'ultimo accesso in una data specifica.

A proposito di questa attività

Prima di utilizzare l'ultimo tempo di accesso in una regola ILM, esaminare le seguenti considerazioni:

- Quando si utilizza l'ultimo tempo di accesso come tempo di riferimento, tenere presente che la modifica dell'ultimo tempo di accesso per un oggetto non attiva una valutazione ILM immediata. Al contrario, le posizioni dell'oggetto vengono valutate e l'oggetto viene spostato come richiesto quando ILM in background valuta l'oggetto. Questa operazione potrebbe richiedere due settimane o più dopo l'accesso all'oggetto.

  Tenere conto di questa latenza durante la creazione di regole ILM basate sull'ultimo tempo di accesso ed evitare posizionamenti che utilizzano brevi periodi di tempo (meno di un mese).

- Quando si utilizza l'ultima ora di accesso come filtro avanzato o come ora di riferimento, è necessario attivare gli ultimi aggiornamenti dell'ora di accesso per i bucket S3. È possibile utilizzare "Manager tenant" o il "API di gestione del tenant".

> Gli ultimi aggiornamenti dell'orario di accesso sono sempre attivati per i container Swift, ma sono disattivati per impostazione predefinita per i bucket S3.

> Tenere presente che l'attivazione degli ultimi aggiornamenti del tempo di accesso può ridurre le performance, soprattutto nei sistemi con oggetti di piccole dimensioni. L'impatto delle performance si verifica perché StorageGRID deve aggiornare gli oggetti con nuovi timestamp ogni volta che gli oggetti vengono recuperati.

La tabella seguente riassume se l'ora dell'ultimo accesso viene aggiornata per tutti gli oggetti nel bucket per diversi tipi di richieste.

Tipo di richiesta	Se l'ora dell'ultimo accesso viene aggiornata quando gli ultimi aggiornamenti dell'ora di accesso sono disattivati	Se l'ora dell'ultimo accesso viene aggiornata quando sono attivati gli ultimi aggiornamenti dell'ora di accesso
Richiesta di recuperare un oggetto, il relativo elenco di controllo degli accessi o i relativi metadati	No	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì
Richiesta di copia di un oggetto da un bucket all'altro	• No, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione
Richiesta di completare un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Fase 3 di 3: Selezionare il comportamento di acquisizione

La fase **Select ingest behavior** della procedura guidata Create ILM Rule consente di scegliere come proteggere gli oggetti filtrati da questa regola durante l'acquisizione.

A proposito di questa attività

StorageGRID può eseguire copie temporanee e mettere in coda gli oggetti per la valutazione ILM in un secondo momento, oppure può eseguire copie per soddisfare immediatamente le istruzioni di posizionamento della regola.

Fasi

1. Selezionare "comportamento di acquisizione" da utilizzare.

   Per ulteriori informazioni, vedere "Vantaggi, svantaggi e limitazioni delle opzioni di acquisizione".

   > Non è possibile utilizzare l'opzione bilanciato o rigoroso se la regola utilizza uno dei seguenti posizionamenti:
   >
   > - Un pool di storage cloud al giorno 0
   > - Un nodo di archivio al giorno 0
   > - Un Cloud Storage Pool o un nodo di archivio quando la regola utilizza un tempo di creazione definito dall'utente come tempo di riferimento
   >
   > Vedere "Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione".

2. Selezionare **Crea**.

   Viene creata la regola ILM. La regola non diventa attiva fino a quando non viene aggiunta a un "Policy ILM" e che la policy sia attivata.

   Per visualizzare i dettagli della regola, selezionare il nome della regola nella pagina delle regole ILM.

Creare una regola ILM predefinita

Prima di creare un criterio ILM, è necessario creare una regola predefinita per inserire nel criterio gli oggetti non corrispondenti a un'altra regola. La regola predefinita non può utilizzare alcun filtro. Deve essere applicato a tutti i tenant, a tutti i bucket e a tutte le versioni degli oggetti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

La regola predefinita è l'ultima regola da valutare in un criterio ILM, quindi non può utilizzare alcun filtro. Le istruzioni di posizionamento per la regola predefinita vengono applicate a tutti gli oggetti che non corrispondono a un'altra regola del criterio.

In questo criterio di esempio, la prima regola si applica solo agli oggetti appartenenti a test-tenant-1. La regola predefinita, ultima, si applica agli oggetti appartenenti a tutti gli altri account tenant.

Quando si crea la regola predefinita, tenere presenti i seguenti requisiti:

- La regola predefinita viene posizionata automaticamente come ultima regola quando viene aggiunta a un criterio.
- La regola predefinita non può utilizzare filtri di base o avanzati.
- La regola predefinita deve essere applicata a tutte le versioni degli oggetti.
- La regola predefinita dovrebbe creare copie replicate.

> Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per un criterio. Le regole di erasure coding devono utilizzare un filtro avanzato per evitare che gli oggetti più piccoli vengano sottoposti a erasure coding.

- In generale, la regola predefinita deve conservare gli oggetti per sempre.
- Se si utilizza (o si prevede di abilitare) l'impostazione blocco oggetti S3 globale, la regola predefinita deve essere conforme.

Fasi

1. Selezionare **ILM** > **regole**.
2. Selezionare **Crea**.

   Viene visualizzata la fase 1 (immettere i dettagli) della creazione guidata regola ILM.

3. Immettere un nome univoco per la regola nel campo **Nome regola**.
4. Se si desidera, inserire una breve descrizione per la regola nel campo **Descrizione**.
5. Lasciare vuoto il campo **account tenant**.

   La regola predefinita deve essere applicata a tutti gli account tenant.

6. Lasciare la selezione a discesa Nome bucket come **si applica a tutti i bucket**.

   La regola predefinita deve essere applicata a tutti i bucket S3 e ai container Swift.

7. Mantenere la risposta predefinita, **No**, per la domanda, "applicare questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?"
8. Non aggiungere filtri avanzati.

   La regola predefinita non può specificare alcun filtro.

9. Selezionare **Avanti**.

   Viene visualizzato il punto 2 (definizione delle posizioni).

10. Per Reference Time (ora di riferimento), selezionare un'opzione qualsiasi.

    Se è stata mantenuta la risposta predefinita, **No**, per la domanda "applicare questa regola solo alle versioni precedenti degli oggetti?" L'ora non corrente non verrà inclusa nell'elenco a discesa. La regola predefinita deve applicare tutte le versioni degli oggetti.

11. Specificare le istruzioni di posizionamento per la regola predefinita.
    - La regola predefinita deve conservare gli oggetti per sempre. Quando si attiva un nuovo criterio, viene visualizzato un avviso se la regola predefinita non conserva gli oggetti per sempre. Devi confermare che questo è il comportamento che ti aspetti.
    - La regola predefinita dovrebbe creare copie replicate.

      > Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per un criterio. Le regole di erasure coding devono includere il filtro avanzato **dimensione oggetto (MB) maggiore di 200 KB** per evitare che gli oggetti più piccoli vengano sottoposti a erasure coding.

    - Se si utilizza (o si intende attivare) l'impostazione globale S3 Object Lock (blocco oggetto S3), la regola predefinita deve essere conforme:
      - Deve creare almeno due copie di oggetti replicate o una copia con codice di cancellazione.
      - Queste copie devono esistere nei nodi di storage per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
      - Impossibile salvare le copie degli oggetti in un Cloud Storage Pool.
      - Impossibile salvare le copie degli oggetti nei nodi di archiviazione.
      - Almeno una riga delle istruzioni di posizionamento deve iniziare al giorno 0, utilizzando l'ora di inizio come ora di riferimento.
      - Almeno una riga delle istruzioni di posizionamento deve essere "per sempre".
12. Consultare il diagramma di conservazione per confermare le istruzioni di posizionamento.
13. Selezionare **continua**.

    Viene visualizzato il passaggio 3 (selezionare il comportamento di acquisizione).

14. Selezionare l'opzione di acquisizione da utilizzare e selezionare **Crea**.

Gestire le policy ILM

Criteri ILM: Panoramica

Un criterio ILM (Information Lifecycle Management) è un insieme ordinato di regole ILM che determina il modo in cui il sistema StorageGRID gestisce i dati degli oggetti nel tempo.

> Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Policy ILM predefinita

Quando si installa StorageGRID e si aggiungono siti, viene creato automaticamente un criterio ILM predefinito, come segue:

- Se la griglia contiene un sito, il criterio predefinito contiene una regola predefinita che replica due copie di ciascun oggetto in quel sito.
- Se la griglia contiene più siti, la regola predefinita replica una copia di ciascun oggetto in ciascun sito.

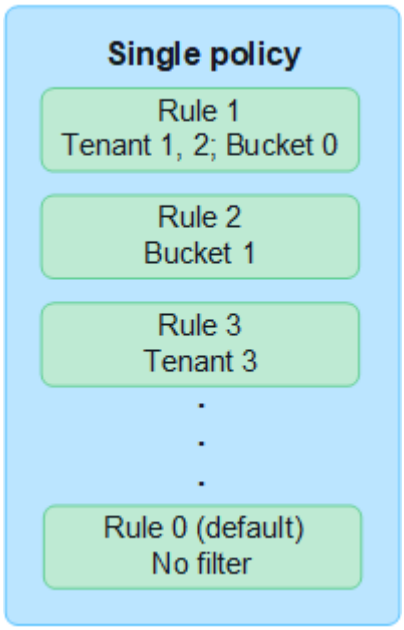
Se il criterio predefinito non soddisfa i requisiti di storage, è possibile creare regole e policy personalizzate. Vedere "Creare una regola ILM" e. "Creare un criterio ILM".

Una o più policy ILM attive?

È possibile disporre di uno o più criteri ILM attivi alla volta.

Un'unica policy

Se il grid usa un semplice schema di data Protection con poche regole specifiche del tenant e del bucket, utilizza una singola policy ILM attiva. Le regole ILM possono contenere filtri per gestire bucket o tenant diversi.



Quando si dispone di un solo criterio e i requisiti di un tenant cambiano, è necessario creare un nuovo criterio

ILM o clonare il criterio esistente per applicare le modifiche, simulare e attivare quindi il nuovo criterio ILM. Le modifiche alla policy ILM possono comportare spostamenti degli oggetti che possono richiedere molti giorni e causare la latenza del sistema.

Policy multiple

Per offrire opzioni di qualità del servizio diverse ai tenant, è possibile disporre di più policy attive alla volta. Ogni policy può gestire tenant specifici, bucket S3 e oggetti. Quando si applicano o si modifica una policy per un insieme specifico di tenant o oggetti, le policy applicate agli altri tenant e oggetti non verranno influenzate.

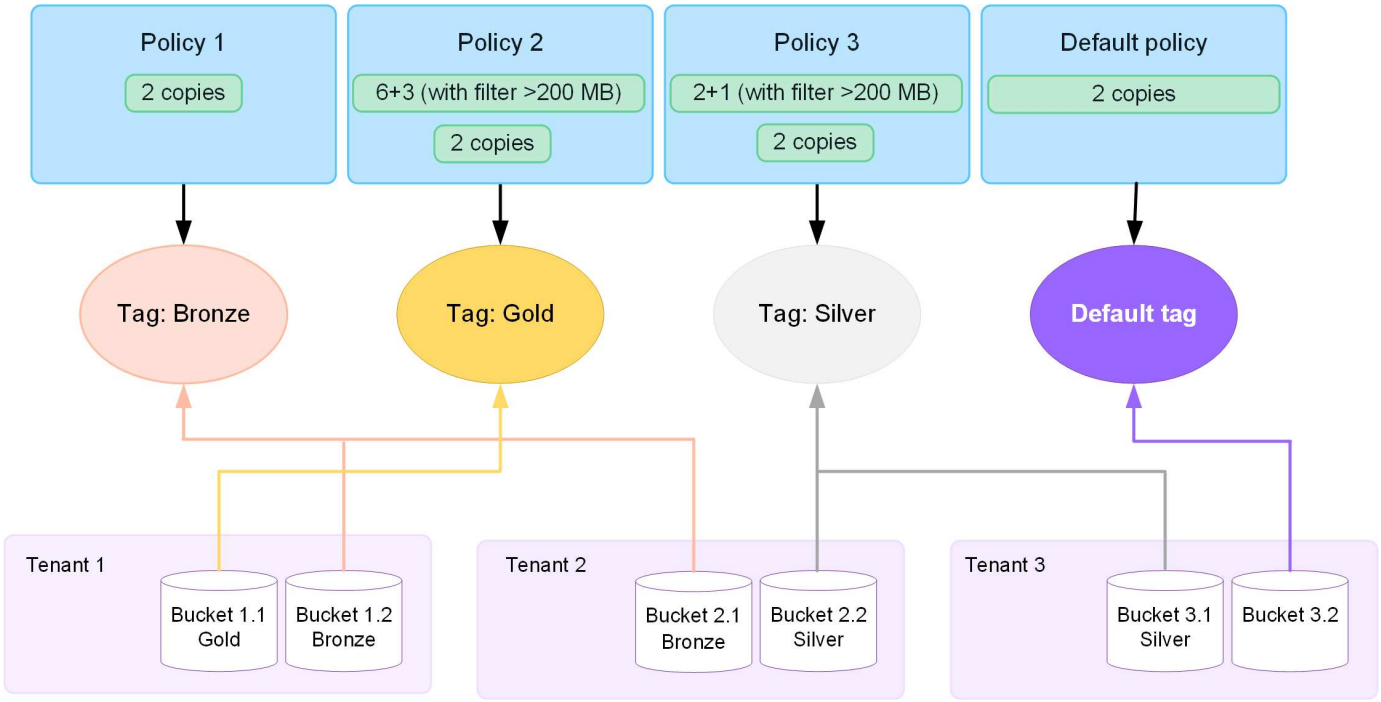
Tag dei criteri ILM

Se desideri consentire ai tenant di alternare facilmente tra più policy di data Protection in base al bucket, utilizza policy ILM multiple con *tag policy ILM*. Ogni policy ILM viene assegnata a un tag, quindi i tenant etichettano un bucket per applicare la policy a quel bucket. È possibile impostare tag di policy ILM solo su bucket S3.

Ad esempio, potresti avere tre tag denominati Gold, Silver e Bronze. È possibile assegnare un criterio ILM a ciascun tag in base alla durata e alla posizione in cui tale criterio memorizza gli oggetti. I tenant possono scegliere la policy da utilizzare contrassegnando i propri bucket. Un bucket con tag Gold viene gestito dalla policy Gold e riceve il livello Gold di data Protection e performance.

Tag criterio ILM predefinito

Quando si installa StorageGRID, viene creato automaticamente un tag di criterio ILM predefinito. Ogni griglia deve avere un criterio attivo assegnato al tag predefinito. La policy predefinita si applica a tutti gli oggetti nei container Swift e a tutti i bucket S3 non contrassegnati.



In che modo un criterio ILM valuta gli oggetti?

Una policy ILM attiva controlla il posizionamento, la durata e la protezione dei dati degli oggetti.

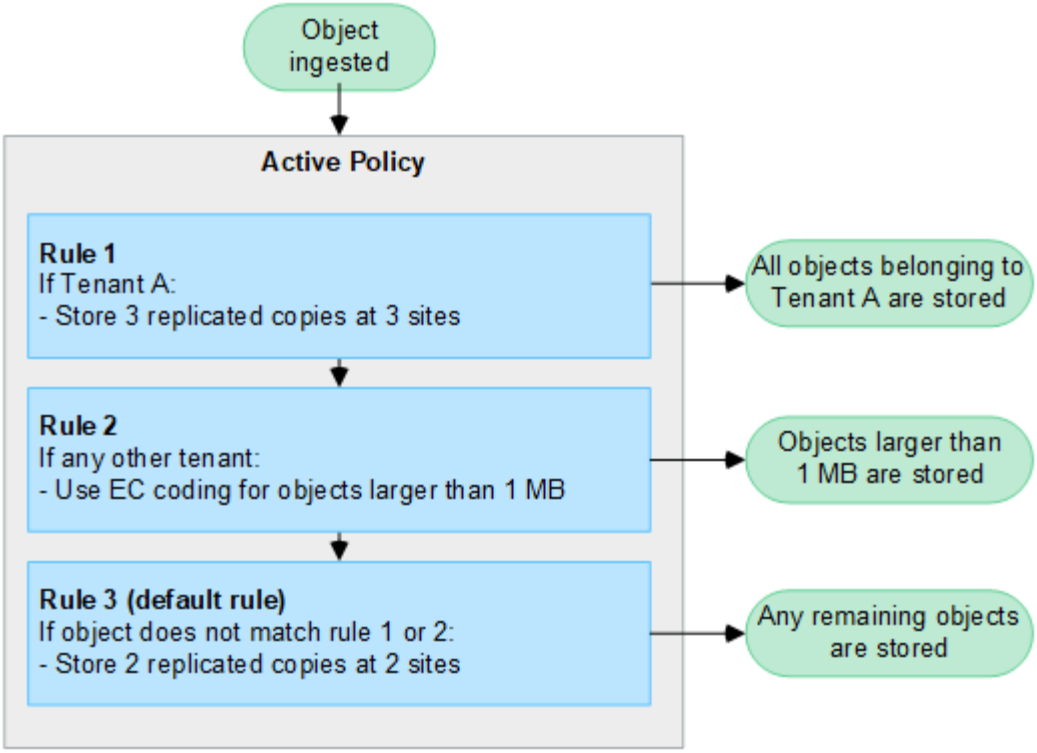
Quando i client salvano gli oggetti in StorageGRID, gli oggetti vengono valutati in base all'insieme ordinato di regole ILM nel criterio, come segue:

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. La regola predefinita deve essere applicata a tutti i tenant, a tutti i bucket S3 o ai container Swift e a tutte le versioni degli oggetti e non può utilizzare alcun filtro avanzato.

Esempio di policy ILM

Ad esempio, un criterio ILM potrebbe contenere tre regole ILM che specificano quanto segue:

- **Regola 1: Copie replicate per il tenant A**
  - Abbina tutti gli oggetti appartenenti al tenant A.
  - Memorizzare questi oggetti 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.
- **Regola 2: Erasure coding per oggetti superiori a 1 MB**
  - Associare 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.
  - Non corrisponde a oggetti di dimensioni pari o inferiori a 1 MB, pertanto questi oggetti vengono valutati in base alla regola 3.
- **Regola 3: 2 copie 2 data center** (impostazione predefinita)
  - È l'ultima regola predefinita del criterio. Non utilizza filtri.
  - Creare 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).



Cosa sono i criteri attivi e inattivi?

Ogni sistema StorageGRID deve avere almeno una policy ILM attiva. Se si desidera disporre di più criteri ILM attivi, è necessario creare tag dei criteri ILM e assegnare un criterio a ciascun tag. I tenant applicano quindi i tag ai bucket S3. Il criterio predefinito viene applicato a tutti gli oggetti nei bucket che non hanno un tag di criterio assegnato.

Quando si crea per la prima volta un criterio ILM, selezionare una o più regole ILM e disporle in un ordine specifico. Dopo aver simulato il criterio per confermarne il comportamento, lo si attiva.

Quando si attiva un criterio ILM, StorageGRID utilizza tale criterio per gestire tutti gli oggetti, inclusi gli oggetti esistenti e gli oggetti appena acquisiti. Gli oggetti esistenti potrebbero essere spostati in nuove posizioni quando vengono implementate le regole ILM nel nuovo criterio.

Se si attivano più policy ILM alla volta e i tenant applicano tag ai bucket S3, gli oggetti in ogni bucket vengono gestiti in base alla policy assegnata al tag.

Un sistema StorageGRID tiene traccia della cronologia delle policy attivate o disattivate.

Considerazioni per la creazione di un criterio ILM

- Utilizzare solo il criterio fornito dal sistema, il criterio di base 2 copie, nei sistemi di test. Per StorageGRID 11.6 e versioni precedenti, la regola Make 2 Copies in questo criterio utilizza il pool di storage All Storage Node, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.

> Il pool di storage All Storage Node viene creato automaticamente durante l'installazione di StorageGRID 11.6 e versioni precedenti. Se si esegue l'aggiornamento a una versione successiva di StorageGRID, il pool di tutti i nodi di storage continuerà a esistere. Se si installa StorageGRID 11.7 o versione successiva come nuova installazione, il pool di tutti i nodi di storage non viene creato.

- Durante la progettazione di un nuovo criterio, considerare tutti i diversi tipi di oggetti che potrebbero essere inseriti nella griglia. Assicurarsi che il criterio includa regole per la corrispondenza e posizionare questi oggetti secondo necessità.
- Mantenere la policy ILM il più semplice possibile. In questo modo si evitano situazioni potenzialmente pericolose in cui i dati degli oggetti non sono protetti come previsto quando nel tempo vengono apportate modifiche al sistema StorageGRID.
- Assicurarsi che le regole della policy siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio. Ad esempio, se la prima regola di un criterio corrisponde a un oggetto, tale oggetto non verrà valutato da altre regole.
- L'ultima regola in ogni policy ILM è la regola ILM predefinita, che non può utilizzare alcun filtro. Se un oggetto non è stato associato da un'altra regola, la regola predefinita controlla la posizione e il tempo di conservazione dell'oggetto.
- Prima di attivare un nuovo criterio, esaminare le modifiche apportate dal criterio al posizionamento degli oggetti esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Creare policy ILM

Create una o più policy ILM per soddisfare i vostri requisiti di qualità del servizio.

La presenza di una policy ILM attiva ti consente di applicare le stesse regole ILM a tutti i tenant e bucket.

La disponibilità di più policy ILM attive ti consente di applicare le regole ILM appropriate a tenant e bucket specifici per soddisfare più requisiti di qualità del servizio.

Creare un criterio ILM

A proposito di questa attività

Prima di creare una policy personalizzata, verificare che "Policy ILM predefinita" non soddisfa i requisiti di storage.

> Utilizzare solo i criteri forniti dal sistema, 2 Copies Policy (per le griglie a un sito) o 1 Copy per Site (per le griglie a più siti), nei sistemi di test. Per StorageGRID 11.6 e versioni precedenti, la regola predefinita in questo criterio utilizza il pool di storage All Storage Node, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.

> Se il "L'impostazione Global S3 Object Lock (blocco oggetti S3 globale) è stata attivata", È necessario assicurarsi che il criterio ILM sia conforme ai requisiti dei bucket che hanno attivato il blocco oggetti S3. In questa sezione, seguire le istruzioni relative all'attivazione del blocco oggetti S3.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "autorizzazioni di accesso richieste".
- Lo hai fatto "Regole ILM create" In base all'attivazione o meno di S3 Object Lock.

Blocco oggetti S3 non abilitato

- Lo hai fatto "Creazione delle regole ILM" da aggiungere al criterio. Se necessario, è possibile salvare un criterio, creare regole aggiuntive e quindi modificarlo per aggiungerne di nuove.
- Lo hai fatto "Creazione di una regola ILM predefinita" che non contiene filtri.

Blocco oggetti S3 attivato

- Il "L'impostazione Global S3 Object Lock (blocco oggetti S3 globale) è già attivata" Per il sistema StorageGRID.
- Lo hai fatto "Creazione delle regole ILM conformi e non conformi" da aggiungere al criterio. Se necessario, è possibile salvare un criterio, creare regole aggiuntive e quindi modificarlo per aggiungerne di nuove.
- Lo hai fatto "Creazione di una regola ILM predefinita" per i criteri conformi.

- Facoltativamente, hai guardato il video: "Video: Politiche di gestione del ciclo di vita delle informazioni in StorageGRID 11,8"

Vedere anche "Creare una policy ILM: Panoramica".

Fasi

1. Selezionare **ILM** > **Policy**.

   Se l'impostazione blocco oggetti S3 globale è attivata, la pagina dei criteri ILM indica quali regole ILM sono conformi.

2. Stabilire come si desidera creare il criterio ILM.

   Creare una nuova policy

   a. Selezionare **Crea policy**.

   Clonazione della policy esistente

   a. Selezionare la casella di controllo relativa al criterio che si desidera iniziare, quindi selezionare **Clona**.

   Modifica criterio esistente

   a. Se un criterio è inattivo, è possibile modificarlo. Selezionare la casella di controllo per il criterio inattivo che si desidera iniziare, quindi selezionare **Modifica**.

3. Nel campo **Nome criterio**, immettere un nome univoco per la policy.
4. Facoltativamente, nel campo **motivo della modifica**, immettere il motivo per cui si sta creando un nuovo criterio.
5. Per aggiungere regole al criterio, selezionare **Seleziona regole**. Selezionare il nome di una regola per visualizzare le relative impostazioni.

   Se si sta clonando un criterio:

   - Vengono selezionate le regole utilizzate dal criterio che si sta clonando.

- Se il criterio da clonare utilizza regole senza filtri che non erano la regola predefinita, viene richiesto di rimuovere tutte le regole tranne una di queste.
- Se la regola predefinita utilizza un filtro, viene richiesto di selezionare una nuova regola predefinita.
- Se la regola predefinita non è l'ultima, è possibile spostarla alla fine del nuovo criterio.

Blocco oggetti S3 non abilitato

a. Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, selezionare **pagina regole ILM**.

   La regola predefinita si applica a tutti gli oggetti che non corrispondono a un'altra regola del criterio. La regola predefinita non può utilizzare alcun filtro e viene sempre valutata per ultima.

   > Non utilizzare la regola di creazione di 2 copie come regola predefinita per un criterio. La regola Make 2 copies utilizza un singolo pool di storage, tutti i nodi di storage, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.

Blocco oggetti S3 attivato

a. Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, selezionare **pagina regole ILM**.

   L'elenco delle regole contiene solo le regole che sono conformi e non utilizzano filtri.

   > Non utilizzare la regola di creazione di 2 copie come regola predefinita per un criterio. La regola Make 2 copies utilizza un singolo pool di storage, tutti i nodi di storage, che contiene tutti i siti. Se si utilizza questa regola, sullo stesso sito potrebbero essere collocate più copie di un oggetto.

b. Se è necessaria una regola "predefinita" diversa per gli oggetti nei bucket S3 non conformi, selezionare **Includi una regola senza filtri per i bucket S3 non conformi** e selezionare una regola non conforme che non utilizza un filtro.

   Ad esempio, è possibile utilizzare un Cloud Storage Pool per memorizzare oggetti in bucket che non hanno attivato il blocco oggetti S3.

   > È possibile selezionare solo una regola non conforme che non utilizza un filtro.

Vedere anche "Esempio 7: Policy ILM conforme per il blocco oggetti S3".

6. Una volta selezionata la regola predefinita, selezionare **continua**.
7. Per il passo altre regole, selezionare le altre regole che si desidera aggiungere al criterio. Queste regole utilizzano almeno un filtro (account tenant, nome bucket, filtro avanzato o tempo di riferimento non corrente). Quindi selezionare **Seleziona**.

   La finestra Crea un criterio elenca ora le regole selezionate. La regola predefinita è alla fine, con le altre regole sopra di essa.

   Se S3 Object Lock è attivato e è stata selezionata anche una regola "predefinita" non conforme, tale regola viene aggiunta come regola dalla seconda all'ultima nel criterio.

Viene visualizzato un avviso se una regola non mantiene gli oggetti per sempre. Quando si attiva questo criterio, è necessario confermare che si desidera che StorageGRID elimini gli oggetti quando sono trascorse le istruzioni di posizionamento per la regola predefinita (a meno che un ciclo di vita del bucket non mantenga gli oggetti per un periodo di tempo più lungo).

8. Trascinare le righe per le regole non predefinite per determinare l'ordine in cui verranno valutate queste regole.

   Impossibile spostare la regola predefinita. Se S3 Object Lock è attivato, non è possibile spostare la regola "predefinita" non conforme se ne è stata selezionata una.

   Verificare che le regole ILM siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio.

9. Se necessario, selezionare **Select rules** (Seleziona regole) per aggiungere o rimuovere le regole.
10. Al termine, selezionare **Salva**.
11. Ripetere questa procedura per creare ulteriori criteri ILM.
12. Simulare un criterio ILM. È necessario simulare sempre un criterio prima di attivarlo per assicurarsi che funzioni come previsto.

Simulare una policy

Simula una policy sugli oggetti di test prima di attivarla e applicarla ai dati di produzione.

Prima di iniziare

- Conosci il bucket S3/object-key o il container Swift/object-name per ogni oggetto che desideri testare.

Fasi

1. Utilizzando un client S3 o Swift o il "S3 Console", acquisire gli oggetti necessari per testare ciascuna regola.
2. Nella pagina criteri ILM, selezionare la casella di controllo relativa al criterio, quindi selezionare **simula**.
3. Nel campo **oggetto**, immettere S3 `bucket/object-key` O il Swift `container/object-name` per un oggetto di test. Ad esempio, `bucket-01/filename.png`.
4. Se la versione S3 è attivata, è possibile immettere un ID versione per l'oggetto nel campo **ID versione**.
5. Selezionare **simulate**.
6. Nella sezione risultati di Simulation, verificare che ogni oggetto sia stato associato alla regola corretta.
7. Per determinare quale profilo di pool storage o erasure coding è in vigore, seleziona il nome della regola abbinata e vai alla pagina dei dettagli della regola.

Esaminare eventuali modifiche al posizionamento degli oggetti replicati e con erasure coding esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Risultati

Eventuali modifiche alle regole del criterio verranno riflesse nei risultati di Simulation e mostreranno la nuova corrispondenza e la corrispondenza precedente. La finestra dei criteri di simulazione conserva gli oggetti testati fino a quando non si seleziona **Cancella tutto** o l'icona di rimozione ✕ Per ogni oggetto nell'elenco

risultati di Simulation.

Informazioni correlate

"Esempi di simulazioni dei criteri ILM"

Attivare un criterio

Quando si attiva un singolo nuovo criterio ILM, gli oggetti esistenti e gli oggetti appena acquisiti vengono gestiti da tale criterio. Quando si attivano più policy, i tag dei criteri ILM assegnati ai bucket determinano gli oggetti da gestire.

Prima di attivare un nuovo criterio:

1. Simulare il criterio per confermare che si comporta come previsto.
2. Esaminare eventuali modifiche al posizionamento degli oggetti replicati e con erasure coding esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile.

A proposito di questa attività

Quando si attiva un criterio ILM, il sistema distribuisce il nuovo criterio a tutti i nodi. Tuttavia, il nuovo criterio attivo potrebbe non essere effettivo fino a quando tutti i nodi della griglia non saranno disponibili per ricevere il nuovo criterio. In alcuni casi, il sistema attende l'implementazione di una nuova policy attiva per garantire che gli oggetti Grid non vengano rimossi accidentalmente. In particolare:

- Se si apportano modifiche ai criteri che **aumentano la ridondanza o la durata dei dati**, tali modifiche vengono implementate immediatamente. Ad esempio, se si attiva un nuovo criterio che include una regola di tre copie invece di una regola di due copie, tale criterio verrà implementato immediatamente perché aumenta la ridondanza dei dati.
- Se si apportano modifiche ai criteri che **potrebbero ridurre la ridondanza o la durata dei dati**, tali modifiche non verranno implementate finché non saranno disponibili tutti i nodi della griglia. Ad esempio, se si attiva un nuovo criterio che utilizza una regola di due copie invece di una regola di tre copie, il nuovo criterio viene visualizzato nella scheda criterio attivo, ma non avrà effetto fino a quando tutti i nodi non saranno online e disponibili.

Fasi

Seguire la procedura per attivare uno o più criteri:

Attivare un criterio

Se si dispone di un solo criterio attivo, procedere come segue. Se si dispone già di uno o più criteri attivi e si stanno attivando criteri aggiuntivi, seguire la procedura per l'attivazione di più criteri.

1. Quando si è pronti ad attivare un criterio, selezionare **ILM** > **Criteri**.

   In alternativa, è possibile attivare un singolo criterio dalla pagina **ILM** > **Policy tags**.

2. Nella scheda Criteri, selezionare la casella di controllo relativa al criterio che si desidera attivare, quindi selezionare **attiva**.
3. Seguire la procedura appropriata:
   - Se viene visualizzato un messaggio di avviso che richiede di confermare l'attivazione del criterio, selezionare **OK**.
   - Se viene visualizzato un messaggio di avviso contenente i dettagli relativi al criterio:
     i. Esaminare i dettagli per assicurarsi che i criteri gestiscano i dati come previsto.
     ii. Se la regola predefinita memorizza gli oggetti per un numero limitato di giorni, esaminare il diagramma di conservazione e digitare il numero di giorni nella casella di testo.
     iii. Se la regola predefinita memorizza gli oggetti per sempre, ma una o più altre regole hanno una conservazione limitata, digitare **yes** nella casella di testo.
     iv. Selezionare **attiva criterio**.

Attivare più policy

Per attivare più criteri, è necessario creare tag e assegnare un criterio a ciascun tag.

> Quando vengono utilizzati più tag, se i tenant riassegnano frequentemente i tag delle policy ai bucket, le performance del grid potrebbero risentirne. Se si dispone di tenant non attendibili, utilizzare solo il tag predefinito.

1. Selezionare **ILM** > **Policy tag**.
2. Selezionare **Crea**.
3. Nella finestra di dialogo Crea tag criterio, digitare un nome di tag e, facoltativamente, una descrizione per il tag.

   > I nomi e le descrizioni dei tag sono visibili ai locatari. Scegli valori che aiuteranno i tenant a prendere una decisione informata quando selezionano i tag dei criteri da assegnare ai loro bucket. Ad esempio, se il criterio assegnato eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni riservate in questi campi.

4. Selezionare **Crea tag**.
5. Nella tabella tag criteri ILM, utilizzare il menu a discesa per selezionare un criterio da assegnare al tag.
6. Se gli avvisi vengono visualizzati nella colonna limitazioni criteri, selezionare **Visualizza dettagli criteri** per rivedere il criterio.
7. Assicurarsi che ogni policy gestisca i dati come previsto.
8. Selezionare **attiva criteri assegnati**. In alternativa, selezionare **Cancella modifiche** per rimuovere

l'assegnazione dei criteri.

9. Nella finestra di dialogo attiva criteri con nuovi tag, rivedere le descrizioni di come ciascun tag, criterio e regola gestirà gli oggetti. Apportare le modifiche necessarie per garantire che le policy gestiscano gli oggetti nel modo previsto.
10. Quando si è certi di voler attivare i criteri, digitare **yes** nella casella di testo, quindi selezionare **Activate policies** (attiva criteri).

Informazioni correlate

"Esempio 6: Modifica di un criterio ILM"

Esempi di simulazioni dei criteri ILM

Gli esempi di simulazioni dei criteri ILM forniscono linee guida per strutturare e modificare le simulazioni per l'ambiente in uso.

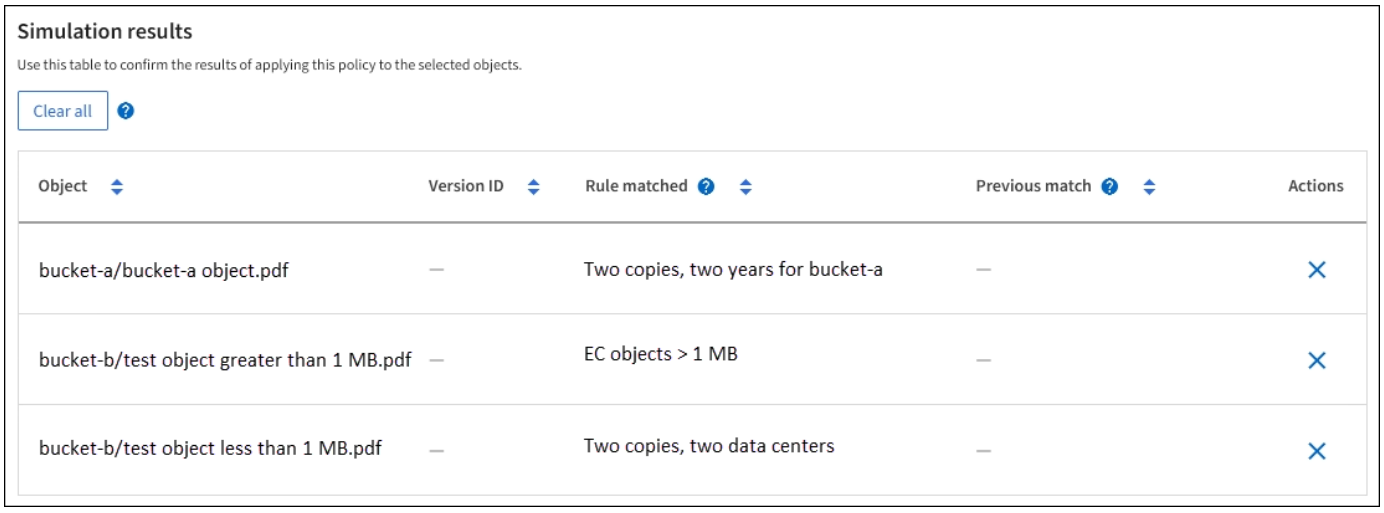
Esempio 1: Verifica delle regole durante la simulazione di un criterio ILM

In questo esempio viene descritto come verificare le regole durante la simulazione di un criterio.

In questo esempio, la **policy ILM di esempio** viene simulata rispetto agli oggetti acquisiti in due bucket. La policy include tre regole, come segue:

- La prima regola, **due copie, due anni per bucket-a**, si applica solo agli oggetti nel bucket-a.
- La seconda regola, **EC objects > 1 MB**, si applica a tutti i bucket, ma ai filtri sugli oggetti superiori a 1 MB.
- La terza regola, **due copie, due data center**, è la regola predefinita. Non include filtri e non utilizza il tempo di riferimento non corrente.

Dopo aver simulato il criterio, verificare che ogni oggetto sia stato associato alla regola corretta.



In questo esempio:

- `bucket-a/bucket-a object.pdf` corrisponde correttamente alla prima regola, che filtra sugli oggetti in `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf` è in `bucket-b`, quindi non corrisponde alla prima regola. Al contrario, è stata associata correttamente dalla seconda regola, che filtra su oggetti

superiori a 1 MB.

- `bucket-b/test object less than 1 MB.pdf` i filtri non corrispondono alle prime due regole, quindi verranno posizionati in base alla regola predefinita, che non include filtri.

Esempio 2: Riordinare le regole durante la simulazione di un criterio ILM

Questo esempio mostra come è possibile riordinare le regole per modificare i risultati durante la simulazione di un criterio.

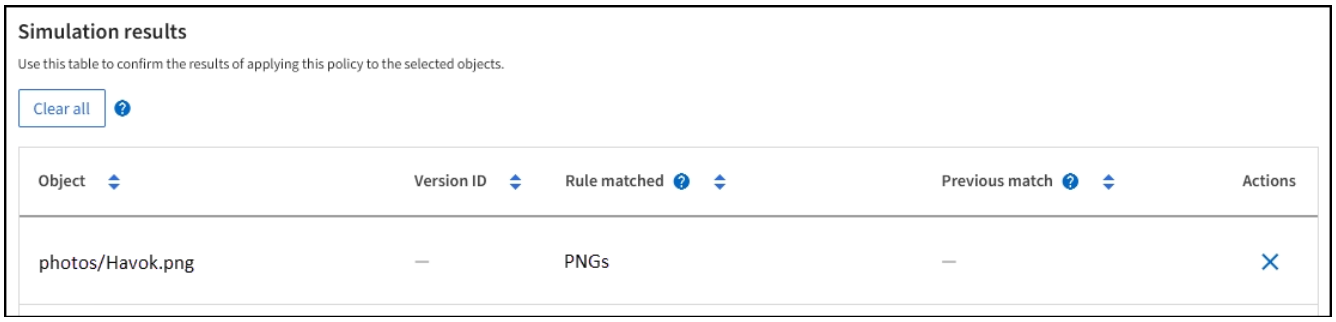
In questo esempio, viene simulata la policy **Demo**. Questo criterio, che ha lo scopo di trovare oggetti con metadati utente series=x-men, include tre regole, come segue:

- La prima regola, **PNG**, filtra i nomi delle chiavi che terminano `.png`.
- La seconda regola, **X-MEN**, si applica solo agli oggetti per il tenant A e ai filtri per `series=x-men` metadati dell'utente.
- L'ultima regola, **due copie due data center**, è la regola predefinita, che corrisponde a tutti gli oggetti che non corrispondono alle prime due regole.

Fasi

1. Dopo aver aggiunto le regole e salvato il criterio, selezionare **simulate**.
2. Nel campo **oggetto**, immettere il bucket S3/object-key o il container Swift/object-name per un oggetto di test e selezionare **simulate**.

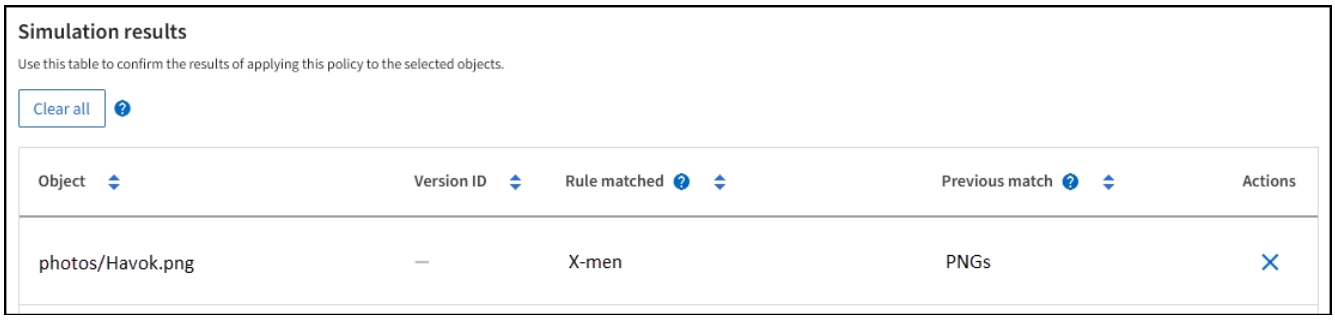
   Vengono visualizzati i risultati di Simulation, che indicano che il `Havok.png` L'oggetto è stato associato dalla regola **PNG**.



   Tuttavia, `Havok.png` Doveva testare la regola **X-MEN**.

3. Per risolvere il problema, riordinare le regole.
   a. Selezionare **fine** per chiudere la finestra Simula policy ILM.
   b. Selezionare **Edit** (Modifica) per modificare la policy.
   c. Trascinare la regola **X-MEN** all'inizio dell'elenco.
   d. Selezionare **Salva**.
4. Selezionare **simulate**.

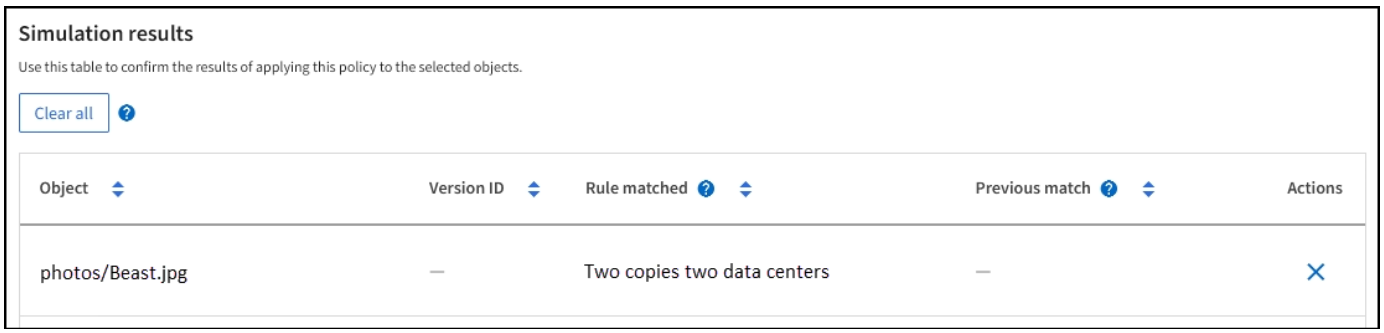
   Gli oggetti precedentemente testati vengono rivalutati in base alla policy aggiornata e vengono visualizzati i risultati della nuova simulazione. Nell'esempio, la colonna Rule Matched mostra che il `Havok.png` L'oggetto ora corrisponde alla regola dei metadati X-MEN, come previsto. La colonna di confronto precedente mostra che la regola PNG corrisponde all'oggetto nella simulazione precedente.



Esempio 3: Correggere una regola durante la simulazione di un criterio ILM

Questo esempio mostra come simulare una policy, correggere una regola nella policy e continuare la simulazione.

In questo esempio, viene simulata la policy **Demo**. Questo criterio è destinato a trovare gli oggetti che hanno `series=x-men` metadati dell'utente. Tuttavia, si sono verificati risultati imprevisti durante la simulazione di questa policy rispetto a. `Beast.jpg` oggetto. Invece di corrispondere alla regola dei metadati X-MEN, l'oggetto corrisponde alla regola predefinita, due copie di due data center.



Quando un oggetto di test non corrisponde alla regola prevista nel criterio, è necessario esaminare ciascuna regola del criterio e correggere eventuali errori.

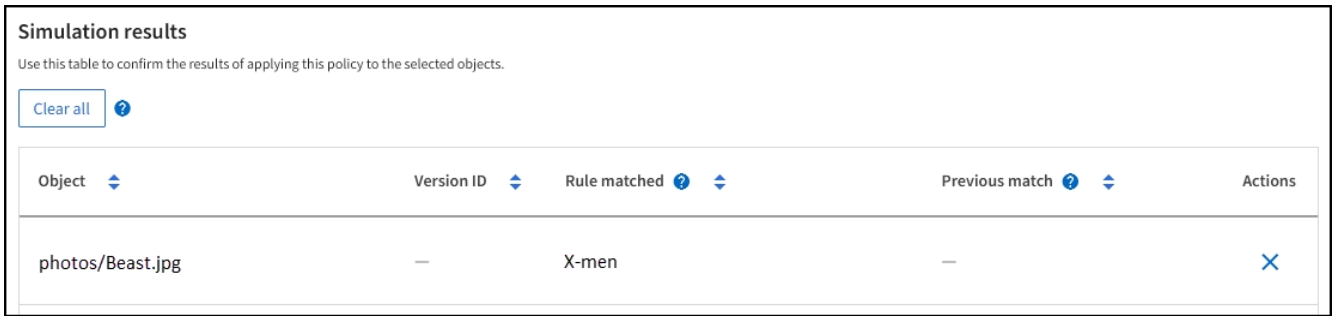
Fasi

1. Selezionare **fine** per chiudere la finestra di dialogo Simula policy. Nella pagina dei dettagli del criterio, selezionare **diagramma di conservazione**. Quindi, selezionare **Espandi tutto** o **Visualizza dettagli** per ogni regola in base alle necessità.
2. Esaminare l'account tenant della regola, il tempo di riferimento e i criteri di filtraggio.

   Ad esempio, supponiamo che i metadati per la regola X-men siano stati immessi come "x-men01" invece di "x-men".

3. Per risolvere l'errore, correggere la regola come segue:
   - Se la regola fa parte del criterio, è possibile clonarla o rimuoverla dal criterio e modificarla.
   - Se la regola fa parte del criterio attivo, è necessario clonarla. Non è possibile modificare o rimuovere una regola dal criterio attivo.
4. Eseguire nuovamente la simulazione.

   In questo esempio, la regola corretta X-men corrisponde ora a. `Beast.jpg` oggetto basato su `series=x-men` metadati dell'utente, come previsto.



Gestire i tag dei criteri ILM

È possibile visualizzare i dettagli dei tag dei criteri ILM, modificare un tag o rimuovere un tag.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "autorizzazioni di accesso richieste".

Visualizzare i dettagli dei tag dei criteri ILM

Per visualizzare i dettagli di un tag:

1. Selezionare **ILM** > **Policy tag**.
2. Selezionare il nome del criterio dalla tabella. Viene visualizzata la pagina dei dettagli del tag.
3. Nella pagina dei dettagli, visualizzare la cronologia precedente dei criteri assegnati.
4. Consente di visualizzare un criterio selezionandolo.

Modifica tag criterio ILM

> I nomi e le descrizioni dei tag sono visibili ai locatari. Scegli valori che aiuteranno i tenant a prendere una decisione informata quando selezionano i tag dei criteri da assegnare ai loro bucket. Ad esempio, se il criterio assegnato eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni riservate in questi campi.

Per modificare la descrizione di un tag esistente:

1. Selezionare **ILM** > **Policy tag**.
2. Seleziona la casella di controllo per il tag, quindi seleziona **Modifica**.

   In alternativa, selezionare il nome del tag. Viene visualizzata la pagina dei dettagli del tag ed è possibile selezionare **Modifica** in quella pagina.

3. Modificare la descrizione del tag secondo necessità
4. Selezionare **Salva**.

Rimuovere il tag criterio ILM

Quando si rimuove un tag di criterio, a tutti i bucket a cui è assegnato tale tag verrà applicato il criterio predefinito.

Per rimuovere un'etichetta:

1. Selezionare **ILM** > **Policy tag**.
2. Selezionare la casella di controllo per il tag, quindi selezionare **Rimuovi**. Viene visualizzata una finestra di dialogo di conferma.

   In alternativa, selezionare il nome del tag. Viene visualizzata la pagina dei dettagli del tag ed è possibile selezionare **Rimuovi** in quella pagina.

3. Selezionare **Sì** per eliminare il tag.

Verificare un criterio ILM con la ricerca dei metadati degli oggetti

Dopo aver attivato un criterio ILM, è necessario acquisire oggetti di test rappresentativi nel sistema StorageGRID. Quindi, eseguire una ricerca dei metadati degli oggetti per confermare che le copie vengono eseguite come previsto e collocate nelle posizioni corrette.

Prima di iniziare

- Si dispone di un identificatore di oggetto, che può essere uno dei seguenti:
  - **UUID**: Identificativo universalmente univoco dell'oggetto. Inserire l'UUID in tutte le lettere maiuscole.
  - **CBID**: Identificatore univoco dell'oggetto all'interno di StorageGRID. È possibile ottenere il CBID di un oggetto dal log di audit. Inserire il CBID in tutte le lettere maiuscole.
  - **S3 bucket e chiave oggetto**: Quando un oggetto viene acquisito tramite l'interfaccia S3, l'applicazione client utilizza una combinazione di bucket e chiave oggetto per memorizzare e identificare l'oggetto. Se il bucket S3 è dotato di versione e si desidera cercare una versione specifica di un oggetto S3 utilizzando il bucket e la chiave Object, si dispone dell' **version ID**.
  - **Swift container and object name**: Quando un oggetto viene acquisito tramite l'interfaccia Swift, l'applicazione client utilizza una combinazione di container e object name per memorizzare e identificare l'oggetto.

Fasi

1. Acquisire l'oggetto.
2. Selezionare **ILM** > **Object metadata lookup**.
3. Digitare l'identificativo dell'oggetto nel campo **Identifier**. È possibile immettere UUID, CBID, S3 bucket/object-key o Swift container/object-name.
4. Facoltativamente, inserire un ID versione per l'oggetto (solo S3).
5. Selezionare **Cerca**.

   Vengono visualizzati i risultati della ricerca dei metadati dell'oggetto. In questa pagina sono elencati i seguenti tipi di informazioni:

   - Metadati del sistema, tra cui:
     - ID oggetto (UUID)
     - nome oggetto
     - nome del contenitore
     - Tipo di risultato (oggetto, marker di eliminazione, bucket S3 o contenitore Swift)

        - Nome o ID dell'account tenant
        - dimensione logica dell'oggetto
        - data e ora in cui l'oggetto è stato creato per la prima volta
        - data e ora dell'ultima modifica dell'oggetto
    - Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
    - Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
    - Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
    - Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
    - Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
    - Per oggetti segmentati e multiparte, un elenco di segmenti di oggetti che include identificatori di segmenti e dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono visualizzati solo i primi 100 segmenti.
    - Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.

    Nell'esempio seguente vengono illustrati i risultati della ricerca dei metadati degli oggetti per un oggetto di test S3 memorizzato come due copie replicate.

    > La seguente schermata è un esempio. I risultati variano a seconda della versione di StorageGRID in uso.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


6. Verificare che l'oggetto sia memorizzato nella posizione o nelle posizioni corrette e che si tratti del tipo di copia corretto.

> Se l'opzione Audit è attivata, è anche possibile monitorare il registro di audit per il messaggio ORLM Object Rules Met. Il messaggio di audit ORLM può fornire ulteriori informazioni sullo stato del processo di valutazione ILM, ma non può fornire informazioni sulla correttezza del posizionamento dei dati dell'oggetto o sulla completezza della policy ILM. È necessario valutarlo da soli. Per ulteriori informazioni, vedere "Esaminare i registri di audit".

Informazioni correlate

- "UTILIZZARE L'API REST S3"
- "Utilizzare l'API REST di Swift"

Utilizzare le policy ILM e le regole ILM

In caso di cambiamento dei requisiti di storage, potrebbe essere necessario

implementare criteri aggiuntivi o modificare le regole ILM associate a un criterio. È possibile visualizzare le metriche ILM per determinare le performance del sistema.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Visualizza i criteri ILM

Per visualizzare i criteri ILM attivi e inattivi e la cronologia di attivazione dei criteri:

1. Selezionare **ILM** > **Policy**.
2. Selezionare **Criteri** per visualizzare un elenco di criteri attivi e inattivi. La tabella elenca il nome di ciascun criterio, i tag a cui è assegnato il criterio e se il criterio è attivo o inattivo.
3. Selezionare **Cronologia attivazioni** per visualizzare un elenco delle date di inizio e di fine delle attivazioni per i criteri.
4. Selezionare il nome di un criterio per visualizzarne i dettagli.

> Se si visualizzano i dettagli di un criterio il cui stato è modificato o eliminato, viene visualizzato un messaggio che spiega che si sta visualizzando la versione del criterio che era attiva per l'intervallo di tempo specificato e che è stata successivamente modificata o eliminata.

Modificare un criterio ILM

È possibile modificare solo un criterio inattivo. Se si desidera modificare un criterio attivo, disattivarlo o creare un clone e modificarlo.

Per modificare un criterio:

1. Selezionare **ILM** > **Policy**.
2. Selezionare la casella di controllo relativa al criterio che si desidera modificare, quindi selezionare **Modifica**.
3. Modificare il criterio seguendo le istruzioni riportate in "Creare policy ILM".
4. Simulare il criterio prima di riattivarlo.

> Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Clonazione di una policy ILM

Per clonare un criterio ILM:

1. Selezionare **ILM** > **Policy**.
2. Selezionare la casella di controllo relativa al criterio da clonare, quindi selezionare **Clona**.
3. Creare un nuovo criterio a partire dal criterio clonato seguendo le istruzioni riportate in "Creare policy ILM".

Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Rimuovere un criterio ILM

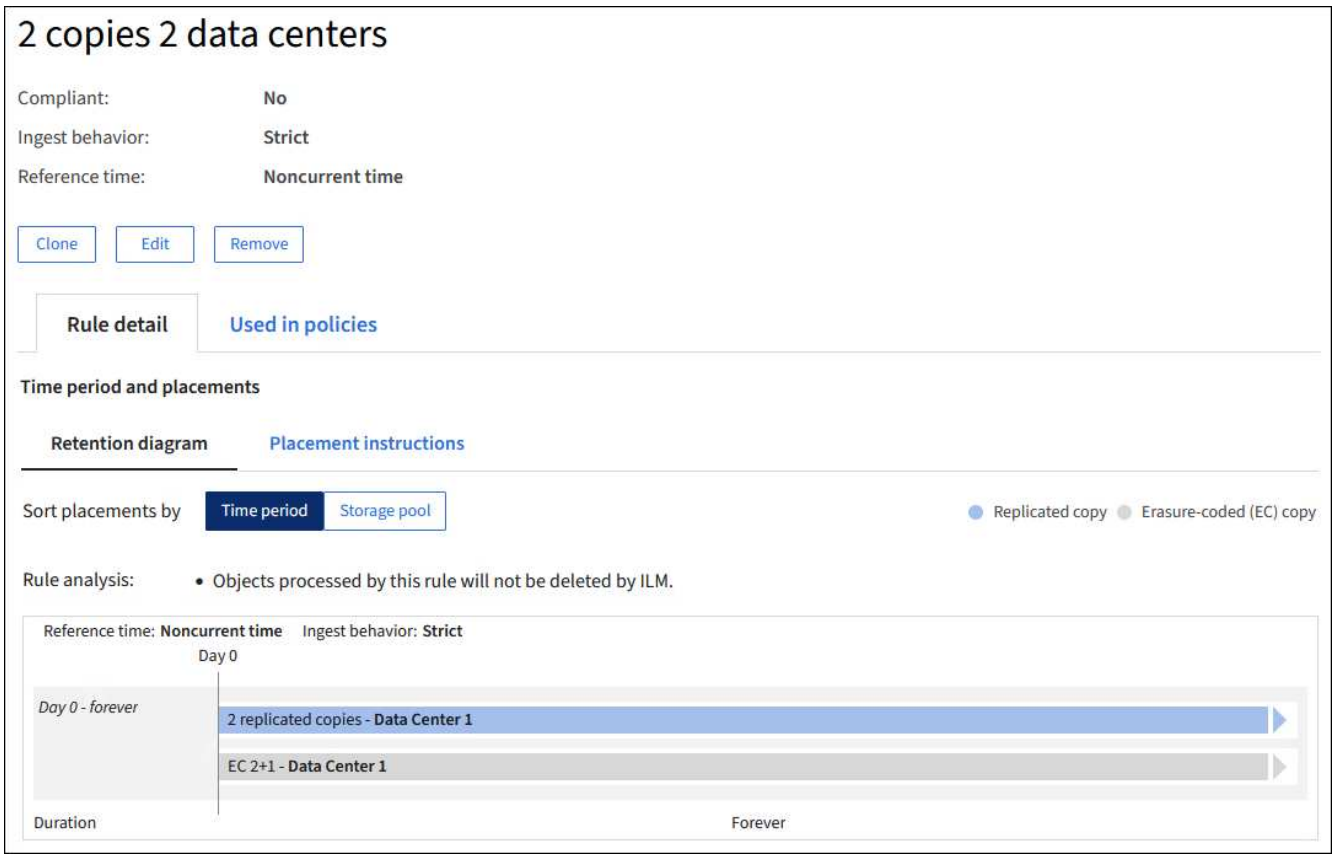
È possibile rimuovere un criterio ILM solo se è inattivo. Per rimuovere un criterio:

1. Selezionare **ILM** > **Policy**.
2. Selezionare la casella di controllo relativa al criterio inattivo che si desidera rimuovere.
3. Selezionare **Rimuovi**.

Visualizza i dettagli della regola ILM

Per visualizzare i dettagli di una regola ILM, inclusi il diagramma di conservazione e le istruzioni di posizionamento della regola:

1. Selezionare **ILM** > **regole**.
2. Selezionare il nome della regola di cui si desidera visualizzare i dettagli. Esempio:



Inoltre, è possibile utilizzare la pagina dei dettagli per clonare, modificare o rimuovere una regola. Non è possibile modificare o rimuovere una regola se utilizzata in alcun criterio.

Clonare una regola ILM

È possibile clonare una regola esistente se si desidera creare una nuova regola che utilizzi alcune delle impostazioni della regola esistente. Se è necessario modificare una regola utilizzata in qualsiasi criterio, è

necessario clonare la regola e apportare le modifiche al clone. Una volta apportate le modifiche al clone, è possibile rimuovere la regola originale dal criterio e sostituirla con la versione modificata, se necessario.

> Non è possibile clonare una regola ILM se è stata creata utilizzando StorageGRID versione 10.2 o precedente.

Fasi

1. Selezionare **ILM** > **regole**.
2. Selezionare la casella di controllo della regola da clonare, quindi selezionare **Clone**. In alternativa, selezionare il nome della regola, quindi selezionare **Clone** dalla pagina dei dettagli della regola.
3. Aggiornare la regola clonata seguendo la procedura descritta in Modifica di una regola ILM e. "Utilizzo di filtri avanzati nelle regole ILM".

   Quando si clonano una regola ILM, è necessario immettere un nuovo nome.

Modificare una regola ILM

Potrebbe essere necessario modificare una regola ILM per modificare un filtro o un'istruzione di posizionamento.

Non è possibile modificare una regola se utilizzata in qualsiasi criterio ILM. Invece, è possibile clonare la regola e apportare le modifiche necessarie alla copia clonata.

> Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Fasi

1. Selezionare **ILM** > **regole**.
2. Verificare che la regola che si desidera modificare non sia utilizzata in alcun criterio ILM.
3. Se la regola che si desidera modificare non è in uso, selezionare la casella di controllo corrispondente e selezionare **azioni** > **Modifica**. In alternativa, selezionare il nome della regola, quindi selezionare **Modifica** nella pagina dei dettagli della regola.
4. Completare i passaggi della procedura guidata Modifica regola ILM. Se necessario, seguire i passaggi per "Creazione di una regola ILM" e. "Utilizzo di filtri avanzati nelle regole ILM".

   Quando si modifica una regola ILM, non è possibile modificarne il nome.

Rimuovere una regola ILM

Per mantenere gestibile l'elenco delle regole ILM correnti, rimuovi tutte le regole ILM che non sei in grado di utilizzare.

Fasi

Per rimuovere una regola ILM attualmente utilizzata in un criterio attivo:

1. Clonazione della policy.
2. Rimuovere la regola ILM dal clone dei criteri.
3. Salvare, simulare e attivare il nuovo criterio per assicurarsi che gli oggetti siano protetti come previsto.

4. Passare alla procedura per la rimozione di una regola ILM attualmente utilizzata in un criterio inattivo.

Per rimuovere una regola ILM attualmente utilizzata in un criterio inattivo:

1. Selezionare il criterio inattivo.
2. Rimuovere la regola ILM dal criterio o. rimuovere il criterio.
3. Passare alla procedura per la rimozione di una regola ILM non attualmente utilizzata.

Per rimuovere una regola ILM attualmente non utilizzata:

1. Selezionare **ILM** > **regole**.
2. Verificare che la regola che si desidera rimuovere non venga utilizzata in alcun criterio.
3. Se la regola che si desidera rimuovere non è in uso, selezionarla e scegliere **azioni** > **Rimuovi**. È possibile selezionare più regole e rimuoverle tutte contemporaneamente.
4. Selezionare **Sì** per confermare che si desidera rimuovere la regola ILM.

Visualizza metriche ILM

È possibile visualizzare le metriche per ILM, ad esempio il numero di oggetti nella coda e il tasso di valutazione. È possibile monitorare queste metriche per determinare le performance del sistema. Una grande coda o un tasso di valutazione potrebbe indicare che il sistema non è in grado di tenere il passo con la velocità di acquisizione, che il carico dalle applicazioni client è eccessivo o che esistono condizioni anomale.

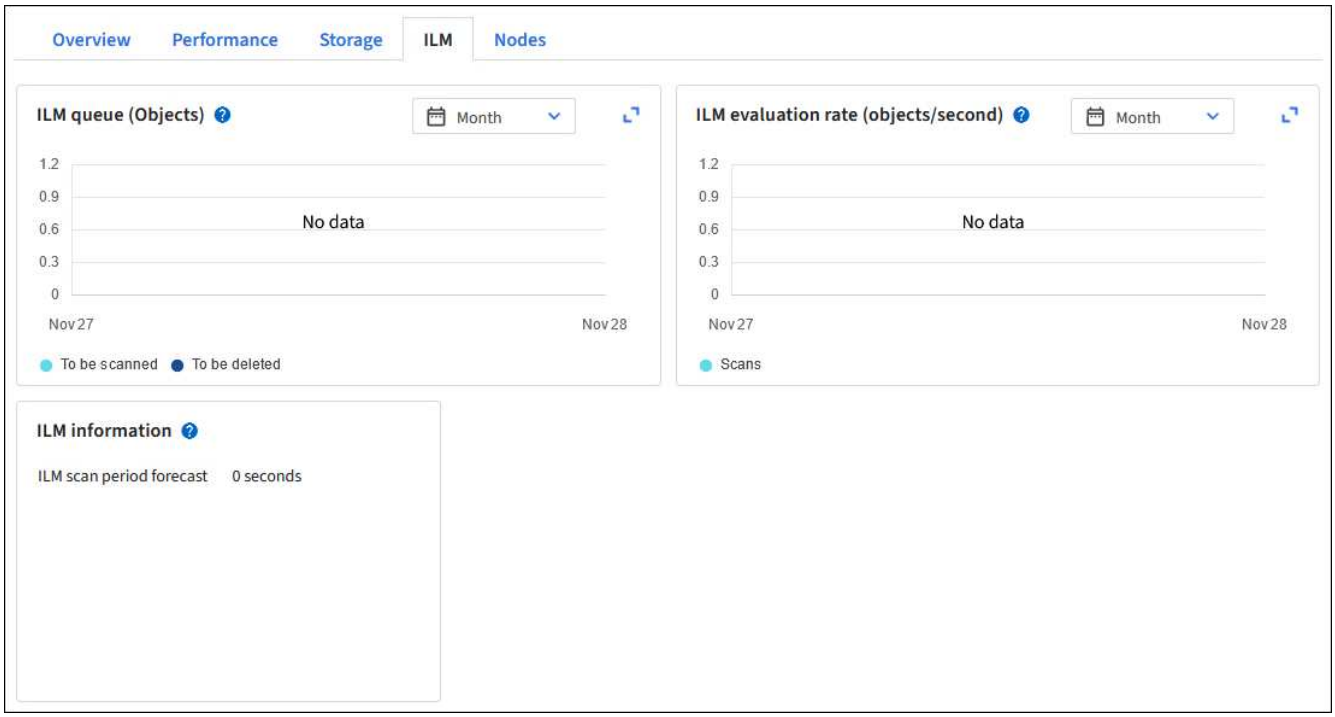
Fasi

1. Selezionare **Dashboard** > **ILM**.

   Poiché la dashboard può essere personalizzata, la scheda ILM potrebbe non essere disponibile.

2. Monitorare le metriche nella scheda ILM.

   È possibile selezionare il punto interrogativo Per visualizzare una descrizione degli elementi nella scheda ILM.



USA blocco oggetti S3

Gestire gli oggetti con S3 Object Lock

In qualità di amministratore di rete, è possibile attivare il blocco oggetti S3 per il sistema StorageGRID e implementare un criterio ILM conforme per garantire che gli oggetti in specifici bucket S3 non vengano cancellati o sovrascritti per un periodo di tempo specificato.

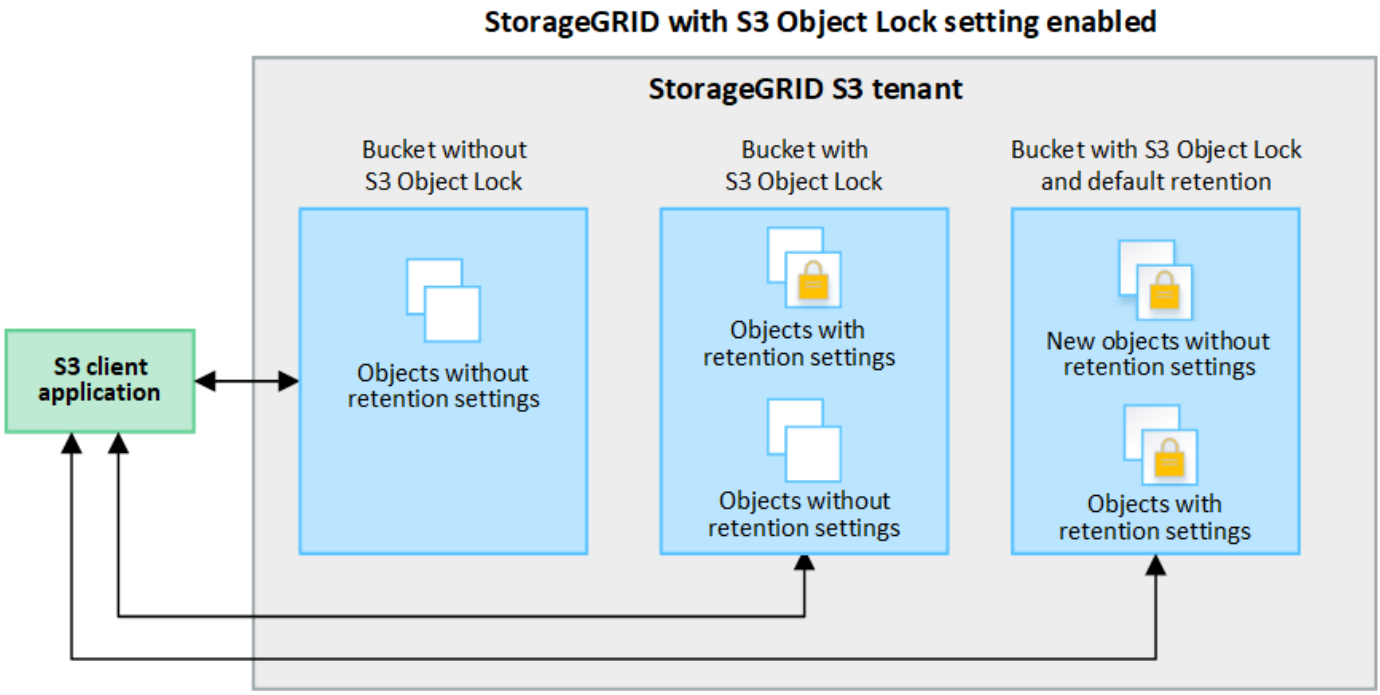
Che cos'è il blocco oggetti S3?

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).

Come mostrato nella figura, quando l'impostazione globale S3 Object Lock è attivata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se un bucket ha S3 Object Lock attivato, è necessario il controllo della versione del bucket e viene attivato automaticamente.

Se un bucket ha attivato il blocco oggetti S3, le applicazioni client S3 possono specificare le impostazioni di conservazione per qualsiasi versione di oggetto salvata in quel bucket.

Inoltre, un bucket con S3 Object Lock attivato può avere una modalità di conservazione e un periodo di conservazione predefiniti. Le impostazioni predefinite si applicano solo agli oggetti aggiunti al bucket senza le proprie impostazioni di conservazione.



Modalità di conservazione

La funzione blocco oggetti di StorageGRID S3 supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità equivalgono alle modalità di conservazione Amazon S3.

- In modalità compliance:
  - L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
  - La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità governance:
  - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare alcune impostazioni di conservazione.
  - Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
  - Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

Impostazioni di conservazione per le versioni degli oggetti

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono utilizzare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ogni oggetto aggiunto al bucket:

- **Modalità di conservazione**: Conformità o governance.
- **Mantieni-fino-data**: Se la data di conservazione di una versione dell'oggetto è futura, l'oggetto può essere recuperato, ma non può essere cancellato.
- **Conservazione legale**: L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa. Le conservazioni legali sono

indipendenti dalla conservazione fino alla data odierna.

> Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Per ulteriori informazioni sulle impostazioni dell'oggetto, vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

Impostazione di conservazione predefinita per i bucket

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita**: Conformità o governance.
- **Default Retention Period** (periodo di conservazione predefinito): Per quanto tempo le nuove versioni degli oggetti aggiunte a questo bucket devono essere conservate, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non dispongono di proprie impostazioni di conservazione. Gli oggetti bucket esistenti non vengono influenzati quando si aggiungono o si modificano queste impostazioni predefinite.

Vedere "Creare un bucket S3" e. "Aggiorna la conservazione predefinita del blocco oggetti S3".

Confronto tra blocco oggetti S3 e conformità legacy

Il blocco oggetti S3 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Poiché la funzione blocco oggetto S3 è conforme ai requisiti Amazon S3, depreca la funzione di conformità proprietaria di StorageGRID, che ora viene chiamata "conformità legacy".

> L'impostazione di conformità globale è obsoleta. Se questa impostazione è stata attivata utilizzando una versione precedente di StorageGRID, l'impostazione blocco oggetti S3 viene attivata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per ulteriori informazioni, vedere "Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5".

Se è stata utilizzata la funzionalità di conformità legacy in una versione precedente di StorageGRID, fare riferimento alla tabella seguente per informazioni sul confronto con la funzione blocco oggetti S3 di StorageGRID.

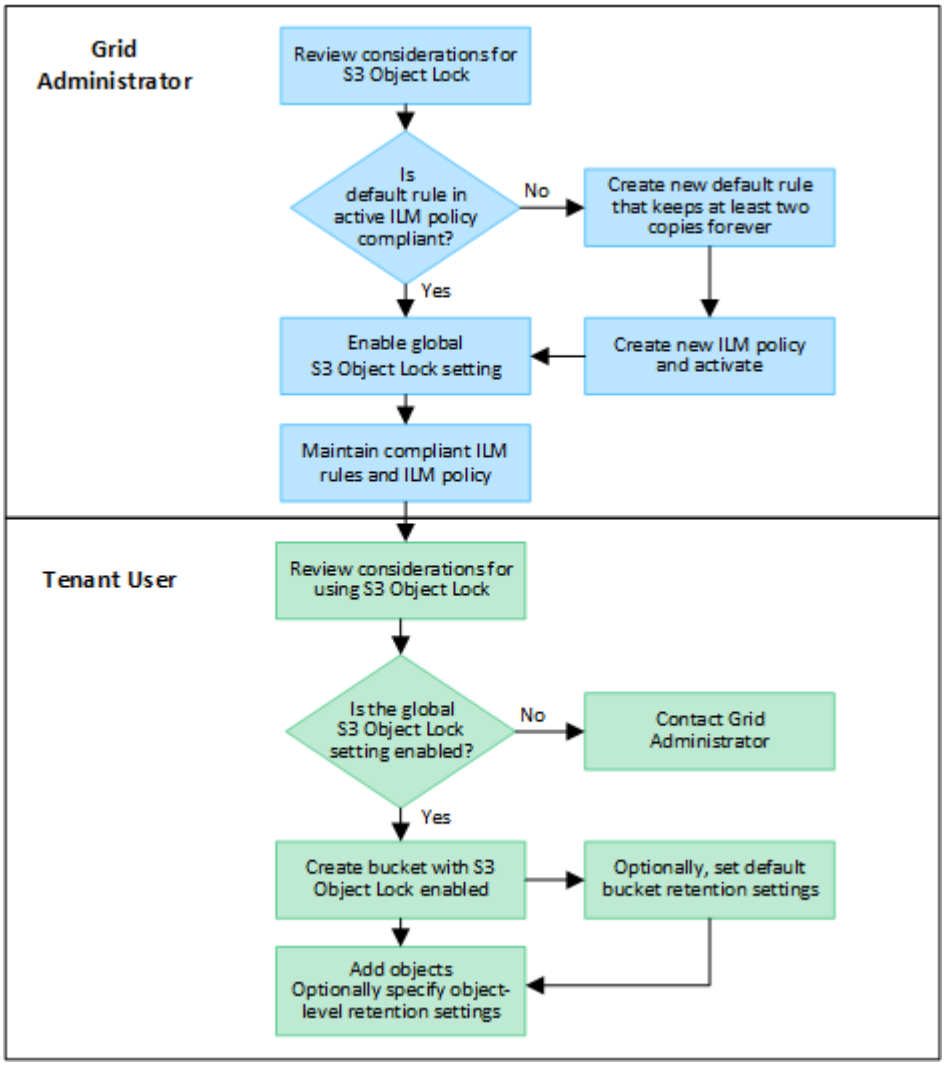
	Blocco oggetti S3	**Compliance (legacy)**
In che modo la funzionalità è abilitata a livello globale?	Da Grid Manager, selezionare **CONFIGURATION** > **System** > **S3 Object Lock**.	Non più supportato.
In che modo è abilitata la funzione per un bucket?	Gli utenti devono attivare il blocco oggetti S3 quando creano un nuovo bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3.	Non più supportato.

	Blocco oggetti S3	Compliance (legacy)
La versione del bucket è supportata?	Sì. La versione del bucket è obbligatoria e viene attivata automaticamente quando il blocco oggetti S3 è attivato per il bucket.	No
Come viene impostata la conservazione degli oggetti?	Gli utenti possono impostare un periodo di conservazione fino alla data di scadenza per ciascuna versione dell'oggetto oppure impostare un periodo di conservazione predefinito per ciascun bucket.	Gli utenti devono impostare un periodo di conservazione per l'intero bucket. Il periodo di conservazione si applica a tutti gli oggetti nel bucket.
È possibile modificare il periodo di conservazione?	• In modalità compliance, è possibile aumentare il periodo di conservazione fino alla data di una versione a oggetti, ma non ridurlo mai. • In modalità governance, gli utenti con autorizzazioni speciali possono ridurre o persino rimuovere le impostazioni di conservazione di un oggetto.	Il periodo di conservazione di un bucket può essere aumentato ma non ridotto.
Dove viene controllata la conservazione legale?	Gli utenti possono porre un blocco legale o revocare un blocco legale per qualsiasi versione di oggetto nel bucket.	Un blocco legale viene posizionato sul bucket e influisce su tutti gli oggetti nel bucket.
Quando è possibile eliminare gli oggetti?	• In modalità compliance, è possibile eliminare una versione dell'oggetto dopo aver raggiunto la data di conservazione, presupponendo che l'oggetto non sia sottoposto a conservazione legale. • In modalità governance, gli utenti con autorizzazioni speciali possono eliminare un oggetto prima che venga raggiunta la data di conservazione, presupponendo che l'oggetto non sia sottoposto a conservazione legale.	È possibile eliminare un oggetto dopo la scadenza del periodo di conservazione, presupponendo che il bucket non sia sottoposto a conservazione legale. Gli oggetti possono essere cancellati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	Sì	No

Workflow per blocco oggetti S3

In qualità di amministratore della griglia, è necessario coordinare strettamente gli utenti tenant per garantire che gli oggetti siano protetti in modo da soddisfare i requisiti di conservazione.

Il diagramma del flusso di lavoro mostra i passaggi di alto livello per l'utilizzo di S3 Object Lock. Questi passaggi vengono eseguiti dall'amministratore della griglia e dagli utenti del tenant.



Attività dell'amministratore di rete

Come mostra il diagramma del flusso di lavoro, un amministratore della griglia deve eseguire due attività di alto livello prima che gli utenti del tenant S3 possano utilizzare il blocco oggetti S3:

1. Creare almeno una regola ILM conforme e impostarla come regola predefinita in un criterio ILM attivo.
2. Attivare l'impostazione globale S3 Object Lock per l'intero sistema StorageGRID.

Attività utente tenant

Una volta attivata l'impostazione globale S3 Object Lock, i tenant possono eseguire le seguenti attività:

1. Creare bucket con S3 Object Lock attivato.

2. Facoltativamente, specificare le impostazioni di conservazione predefinite per il bucket. Tutte le impostazioni predefinite del bucket vengono applicate solo a nuovi oggetti che non dispongono di impostazioni di conservazione personalizzate.
3. Aggiungere oggetti a tali bucket e specificare facoltativamente i periodi di conservazione a livello di oggetto e le impostazioni di conservazione a livello legale.
4. Come richiesto, aggiornare la conservazione predefinita per il bucket o aggiornare il periodo di conservazione o l'impostazione di conservazione legale per un singolo oggetto.

Requisiti per il blocco oggetti S3

È necessario esaminare i requisiti per l'attivazione dell'impostazione globale di blocco oggetti S3, i requisiti per la creazione di regole ILM e criteri ILM conformi e le restrizioni applicate da StorageGRID ai bucket e agli oggetti che utilizzano il blocco oggetti S3.

Requisiti per l'utilizzo dell'impostazione globale S3 Object Lock

- È necessario attivare l'impostazione globale S3 Object Lock utilizzando Grid Manager o l'API Grid Management prima che qualsiasi tenant S3 possa creare un bucket con S3 Object Lock attivato.
- L'attivazione dell'impostazione globale S3 Object Lock consente a tutti gli account tenant S3 di creare bucket con S3 Object Lock attivato.
- Dopo aver attivato l'impostazione di blocco oggetti S3 globale, non è possibile disattivare l'impostazione.
- Non è possibile attivare il blocco oggetto S3 globale a meno che la regola predefinita in tutti i criteri ILM attivi non sia *conforme* (vale a dire, la regola predefinita deve essere conforme ai requisiti dei bucket con blocco oggetto S3 abilitato).
- Quando l'impostazione blocco oggetti S3 globale è attivata, non è possibile creare un nuovo criterio ILM o attivare un criterio ILM esistente a meno che la regola predefinita nel criterio non sia conforme. Una volta attivata l'impostazione globale S3 Object Lock, le pagine delle regole ILM e dei criteri ILM indicano quali regole ILM sono conformi.

Requisiti per le regole ILM conformi

Se si desidera attivare l'impostazione blocco oggetto S3 globale, è necessario verificare che la regola predefinita in tutti i criteri ILM attivi sia conforme. Una regola conforme soddisfa i requisiti di entrambi i bucket con blocco oggetti S3 attivato e di tutti i bucket esistenti con conformità legacy attivata:

- Deve creare almeno due copie di oggetti replicate o una copia con codice di cancellazione.
- Queste copie devono esistere nei nodi di storage per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
- Impossibile salvare le copie degli oggetti in un Cloud Storage Pool.
- Impossibile salvare le copie degli oggetti nei nodi di archiviazione.
- Almeno una riga delle istruzioni di posizionamento deve iniziare al giorno 0, utilizzando **Ingest Time** come ora di riferimento.
- Almeno una riga delle istruzioni di posizionamento deve essere "per sempre".

Requisiti per le policy ILM

Quando l'impostazione blocco oggetto S3 globale è attivata, i criteri ILM attivi e inattivi possono includere regole conformi e non conformi.

- La regola predefinita in un criterio ILM attivo o inattivo deve essere conforme.
- Le regole non conformi si applicano solo agli oggetti nei bucket che non hanno attivato il blocco oggetti S3 o che non hanno la funzionalità Compliance legacy attivata.
- Le regole conformi possono essere applicate agli oggetti in qualsiasi bucket; non è necessario attivare il blocco oggetti S3 o la conformità legacy per il bucket.

Un criterio ILM conforme potrebbe includere le seguenti tre regole:

1. Regola conforme che crea copie con codifica in cancellazione degli oggetti in un bucket specifico con blocco oggetti S3 attivato. Le copie EC vengono memorizzate nei nodi di storage dal giorno 0 a sempre.
2. Una regola non conforme che crea due copie di oggetti replicate sui nodi di storage per un anno, quindi sposta una copia di oggetti nei nodi di archivio e memorizza la copia per sempre. Questa regola si applica solo ai bucket che non hanno attivato il blocco oggetti S3 o la compliance legacy perché memorizza una sola copia dell'oggetto per sempre e utilizza i nodi di archiviazione.
3. Una regola predefinita e conforme che crea due copie di oggetti replicate sui nodi di storage dal giorno 0 a sempre. Questa regola si applica a qualsiasi oggetto in qualsiasi bucket che non è stato filtrato dalle prime due regole.

Requisiti per i bucket con S3 Object Lock attivato

- Se l'impostazione blocco oggetto S3 globale è attivata per il sistema StorageGRID, è possibile utilizzare Gestione tenant, API di gestione tenant o API REST S3 per creare bucket con blocco oggetto S3 attivato.
- Se si intende utilizzare il blocco oggetti S3, è necessario attivare il blocco oggetti S3 quando si crea il bucket. Impossibile attivare il blocco oggetti S3 per un bucket esistente.
- Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket. Non puoi disattivare il blocco oggetti S3 o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione e un periodo di conservazione predefiniti per ciascun bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di proprie impostazioni di conservazione. È possibile eseguire l'override di queste impostazioni predefinite specificando una modalità di conservazione e conservarla fino alla data per ogni versione dell'oggetto al momento del caricamento.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con blocco oggetti S3 attivato.
- La replica di CloudMirror non è supportata per i bucket con blocco oggetti S3 attivato.

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

- Per proteggere una versione dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure le impostazioni di conservazione per ciascuna versione dell'oggetto. È possibile specificare le impostazioni di conservazione a livello di oggetto utilizzando l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni di oggetti. Una versione a oggetti può avere un'impostazione di conservazione fino alla data e un'impostazione di conservazione legale, una ma non l'altra o nessuna delle due. La specifica di un'impostazione di conservazione fino a data o di conservazione legale per un oggetto protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

Ciclo di vita degli oggetti nei bucket con S3 Object Lock attivato

Ogni oggetto salvato in un bucket con S3 Object Lock attivato passa attraverso le seguenti fasi:

1. **Acquisizione oggetto**

   Quando una versione dell'oggetto viene aggiunta al bucket con S3 Object Lock attivato, le impostazioni di conservazione vengono applicate come segue:

   - Se per l'oggetto sono specificate le impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.
   - Se non sono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se presenti.
   - Se non sono specificate impostazioni di conservazione per l'oggetto o il bucket, l'oggetto non è protetto da S3 Object Lock.

   Se vengono applicate le impostazioni di conservazione, vengono protetti sia l'oggetto che i metadati S3 definiti dall'utente.

2. **Conservazione ed eliminazione degli oggetti**

   StorageGRID memorizza più copie di ciascun oggetto protetto per il periodo di conservazione specificato. Il numero e il tipo esatti delle copie degli oggetti e le posizioni dello storage sono determinati dalle regole di conformità nelle policy ILM attive. La possibilità di eliminare un oggetto protetto prima che venga raggiunta la data di conservazione dipende dalla modalità di conservazione.

   - Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Informazioni correlate

- "Creare un bucket S3"
- "Aggiornare la conservazione predefinita del blocco degli oggetti S3"
- "Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
- "Esempio 7: Policy ILM conforme per il blocco oggetti S3"

Attiva il blocco oggetti S3 a livello globale

Se un account tenant S3 deve rispettare i requisiti normativi durante il salvataggio dei dati degli oggetti, è necessario attivare il blocco oggetti S3 per l'intero sistema StorageGRID. L'attivazione dell'impostazione globale S3 Object Lock consente a qualsiasi utente del tenant S3 di creare e gestire bucket e oggetti con S3 Object Lock.

Prima di iniziare

- Hai il "Autorizzazione di accesso root".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai esaminato il flusso di lavoro S3 Object Lock e hai compreso le considerazioni.
- La regola predefinita nel criterio ILM attivo è conforme. Vedere "Creare una regola ILM predefinita" per ulteriori informazioni.

A proposito di questa attività

Un amministratore della griglia deve attivare l'impostazione globale S3 Object Lock per consentire agli utenti tenant di creare nuovi bucket con S3 Object Lock attivato. Una volta attivata, questa impostazione non può essere disattivata.

> L'impostazione di conformità globale è obsoleta. Se questa impostazione è stata attivata utilizzando una versione precedente di StorageGRID, l'impostazione blocco oggetti S3 viene attivata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per ulteriori informazioni, vedere "Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5".

Fasi

1. Selezionare **CONFIGURATION** > **System** > **S3 Object Lock**.

   Viene visualizzata la pagina S3 Object Lock Settings (Impostazioni blocco oggetti S3).

2. Selezionare **Enable S3 Object Lock** (attiva blocco oggetti S3).
3. Selezionare **Applica**.

   Viene visualizzata una finestra di dialogo di conferma che ricorda che non è possibile disattivare il blocco oggetti S3 dopo che è stato attivato.

4. Se si è certi di voler abilitare in modo permanente il blocco oggetti S3 per l'intero sistema, selezionare **OK**.

   Quando si seleziona **OK**:

   - Se la regola predefinita nel criterio ILM attivo è conforme, il blocco oggetti S3 è ora attivato per l'intera griglia e non può essere disattivato.
   - Se la regola predefinita non è conforme, viene visualizzato un errore. È necessario creare e attivare un nuovo criterio ILM che includa una regola conforme come regola predefinita. Selezionare **OK**. Quindi, creare una nuova policy, simularla e attivarla. Vedere "Creare un criterio ILM" per istruzioni.

Risolvi gli errori di coerenza durante l'aggiornamento della configurazione blocco oggetti S3 o Compliance legacy

Se un sito del data center o più nodi di storage in un sito non sono più disponibili, potrebbe essere necessario aiutare gli utenti del tenant S3 ad applicare le modifiche alla configurazione S3 Object Lock o legacy Compliance.

Gli utenti tenant che hanno bucket con S3 Object Lock (o Compliance legacy) abilitato possono modificare alcune impostazioni. Ad esempio, un utente tenant che utilizza il blocco oggetti S3 potrebbe dover mettere una versione dell'oggetto sotto il blocco legale.

Quando un utente tenant aggiorna le impostazioni di un bucket S3 o di una versione a oggetti, StorageGRID tenta di aggiornare immediatamente il bucket o i metadati dell'oggetto nella griglia. Se il sistema non è in grado di aggiornare i metadati perché un sito del data center o più nodi di storage non sono disponibili, viene visualizzato un errore:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Per risolvere questo errore, attenersi alla seguente procedura:

1. Tentare di rendere nuovamente disponibili tutti i nodi o i siti di storage il prima possibile.
2. Se non si riesce a rendere disponibile una quantità sufficiente di nodi di storage in ogni sito, contattare il supporto tecnico, che può aiutare a ripristinare i nodi e garantire che le modifiche vengano applicate in modo coerente in tutta la griglia.
3. Una volta risolto il problema sottostante, ricordare all'utente tenant di ripetere le modifiche alla configurazione.

Informazioni correlate

- "Utilizzare un account tenant"
- "UTILIZZARE L'API REST S3"
- "Ripristino e manutenzione"

Esempio di regole e policy ILM

Esempio 1: Regole ILM e policy per lo storage a oggetti

È possibile utilizzare le seguenti regole e policy di esempio come punto di partenza per la definizione di un criterio ILM in modo da soddisfare i requisiti di protezione e conservazione degli oggetti.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

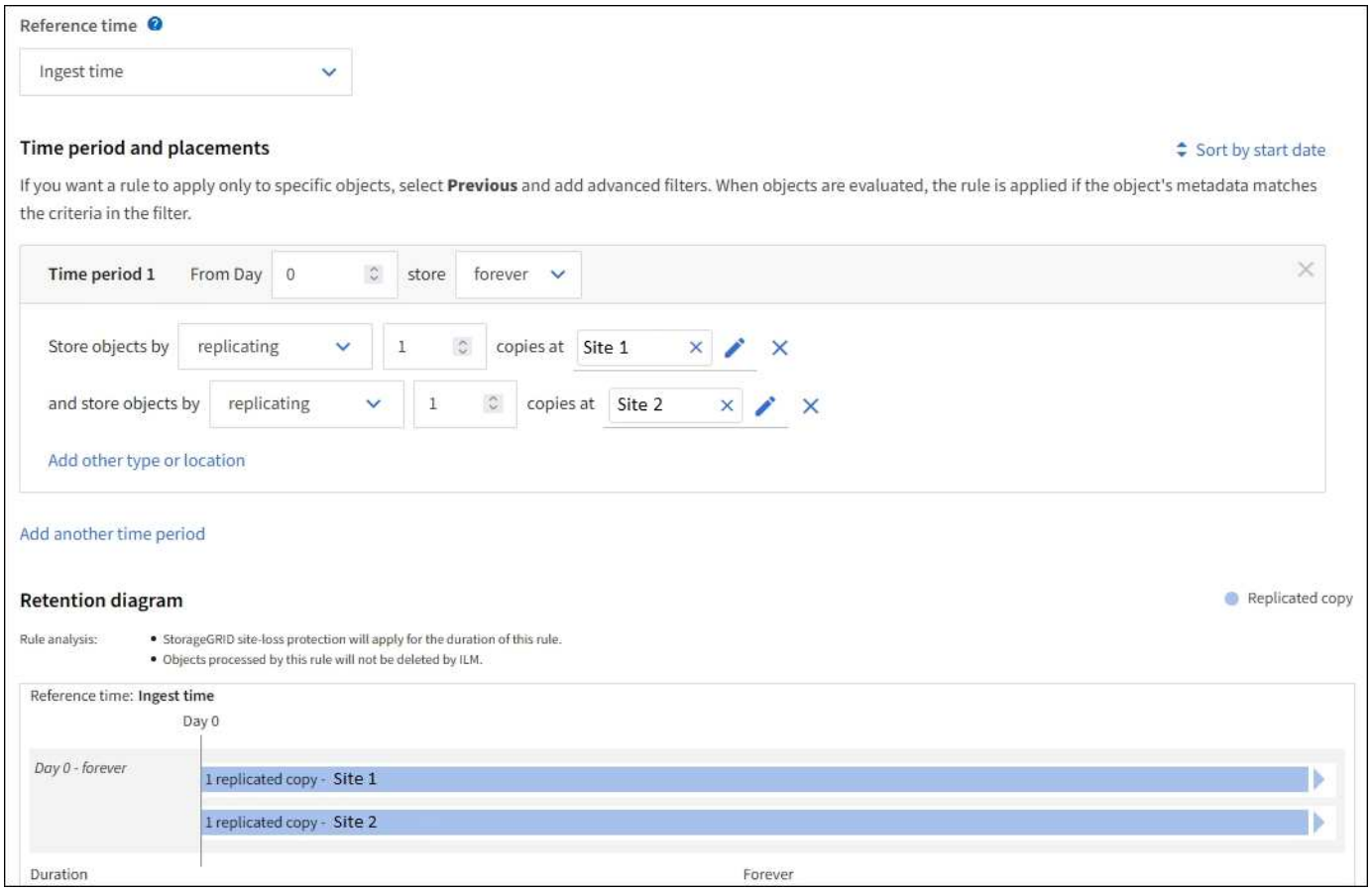
ILM regola 1 per esempio 1: Copia dei dati degli oggetti in due siti

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due siti.

Definizione della regola	Valore di esempio
Pool di storage one-site	Due pool di storage, ciascuno contenente diversi siti, denominati Sito 1 e Sito 2.
Nome della regola	Due copie di due siti
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 al giorno per sempre, conservare una copia replicata nel sito 1 e una copia replicata nel sito 2.

La sezione analisi delle regole del diagramma di conservazione riporta:

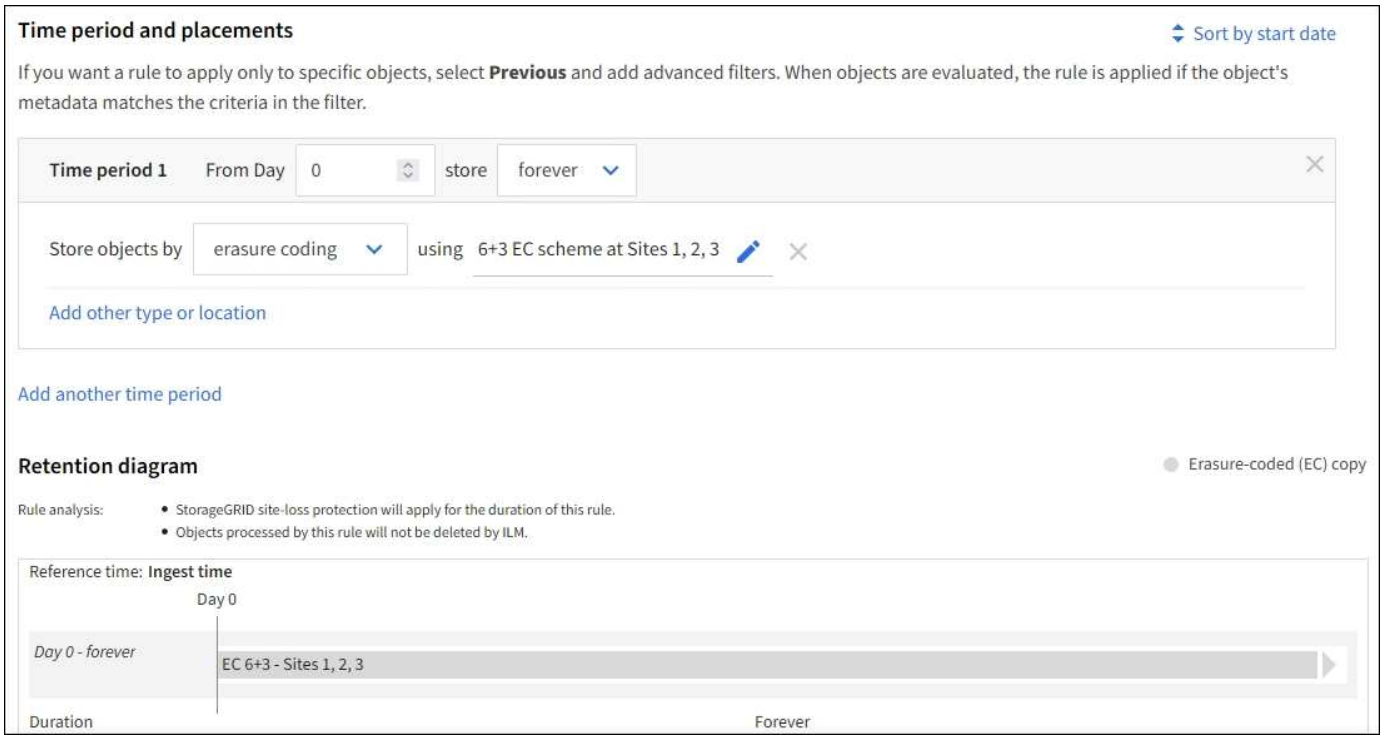
- La protezione contro la perdita di sito di StorageGRID verrà applicata per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola non verranno eliminati da ILM.



Regola ILM 2 per l'esempio 1: Profilo di erasure coding con abbinamento bucket

Questa regola ILM di esempio utilizza un profilo di erasure coding e un bucket S3 per determinare dove e per quanto tempo l'oggetto viene memorizzato.

Definizione della regola	Valore di esempio
Pool di storage con più siti	• Un pool di storage in tre siti (siti 1, 2, 3) • Utilizzare uno schema di erasure coding 6+3
Nome della regola	Record finanziari di S3 Bucket
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Per gli oggetti nel bucket S3 denominato Finance-records, creare una copia con erasure coding nel pool specificato dal profilo di erasure coding. Conserva questa copia per sempre.

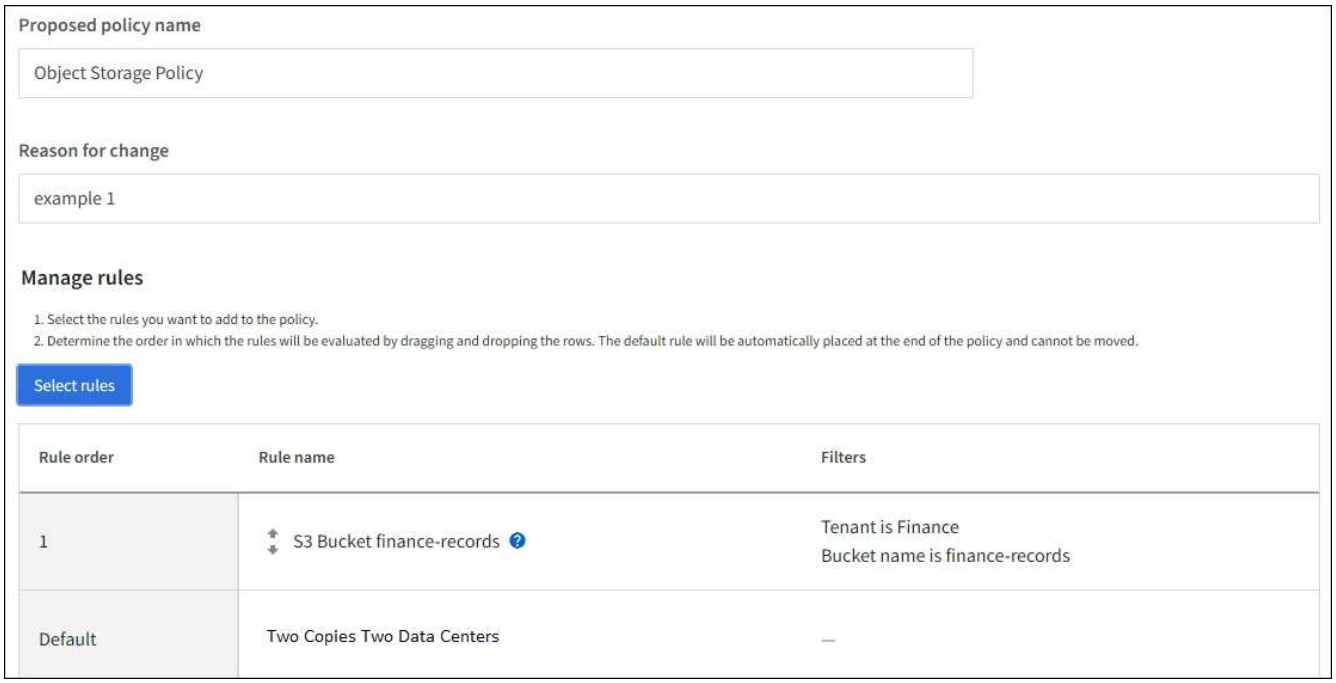


Politica ILM ad esempio 1

In pratica, la maggior parte delle policy ILM è semplice, anche se il sistema StorageGRID consente di progettare policy ILM sofisticate e complesse.

Un tipico criterio ILM per un grid multi-sito potrebbe includere regole ILM come le seguenti:

- All'acquisizione, memorizzare tutti gli oggetti appartenenti al bucket S3 denominato `finance-records` in un pool di storage che contiene tre siti. Utilizzare la codifica di cancellazione 6+3.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita del criterio, due copie due data center, per memorizzare una copia di tale oggetto nel sito 1 e una copia nel sito 2.



Informazioni correlate

- "Criteri ILM: Panoramica"
- "Creare policy ILM"

Esempio 2: Regole ILM e policy per il filtraggio delle dimensioni degli oggetti EC

È possibile utilizzare le seguenti regole e policy di esempio come punti di partenza per definire un criterio ILM che filtra in base alle dimensioni dell'oggetto per soddisfare i requisiti EC consigliati.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 2: Utilizzare EC per oggetti superiori a 1 MB

In questo esempio, la cancellazione della regola ILM codifica gli oggetti superiori a 1 MB.

> L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

Definizione della regola	Valore di esempio
Nome della regola	Solo oggetti EC > 1 MB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto superiore a 1 MB
Posizionamenti	Creare una copia 2+1 con codifica per la cancellazione utilizzando tre siti

ILM regola 2 per esempio 2: Due copie replicate

Questa regola ILM di esempio crea due copie replicate e non filtra in base alle dimensioni dell'oggetto. Questa regola è la regola predefinita per il criterio. Poiché la prima regola filtra tutti gli oggetti superiori a 1 MB, questa regola si applica solo agli oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Nome della regola	Due copie replicate

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per la dimensione dell'oggetto	Nessuno
Posizionamenti	Dal giorno 0 al giorno per sempre, conservare una copia replicata nel sito 1 e una copia replicata nel sito 2.

Criterio ILM per esempio 2: Utilizzare EC per oggetti superiori a 1 MB

Questo esempio di policy ILM include due regole ILM:

- La prima regola di cancellazione codifica tutti gli oggetti superiori a 1 MB.
- La seconda regola ILM (predefinita) crea due copie replicate. Poiché gli oggetti superiori a 1 MB sono stati filtrati dalla regola 1, la regola 2 si applica solo agli oggetti di dimensioni pari o inferiori a 1 MB.

Esempio 3: Regole e policy ILM per una migliore protezione dei file di immagine

È possibile utilizzare le regole e i criteri di esempio seguenti per garantire che le immagini di dimensioni superiori a 1 MB siano sottoposte a erasure coding e che vengano create due copie di immagini di dimensioni inferiori.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

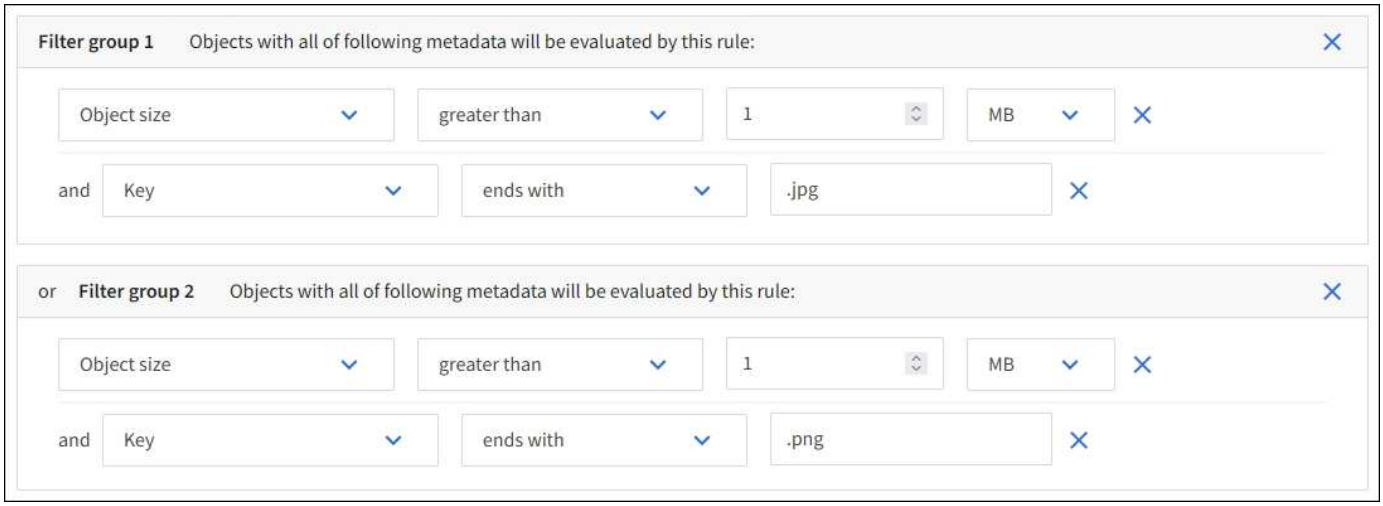
ILM regola 1 per esempio 3: Utilizzare EC per file di immagini superiori a 1 MB

Questa regola ILM di esempio utilizza il filtraggio avanzato per codificare tutti i file di immagine con dimensioni superiori a 1 MB.

> L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

Definizione della regola	Valore di esempio
Nome della regola	File immagine EC > 1 MB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto superiore a 1 MB
Filtri avanzati per Key	• Termina con .jpg • Termina con .png

Definizione della regola	Valore di esempio
Posizionamenti	Creare una copia 2+1 con codifica per la cancellazione utilizzando tre siti



Poiché questa regola è configurata come prima regola del criterio, l'istruzione di posizionamento della codifica di cancellazione si applica solo ai file .jpg e .png che sono superiori a 1 MB.

Regola ILM 2 per esempio 3: Creare 2 copie replicate per tutti i file di immagine rimanenti

Questa regola ILM di esempio utilizza un filtro avanzato per specificare che i file di immagine più piccoli devono essere replicati. Poiché la prima regola del criterio ha già trovato corrispondenza tra file di immagine superiori a 1 MB, questa regola si applica ai file di immagine di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Nome della regola	2 copie per i file immagine
Tempo di riferimento	Tempo di acquisizione
Filtri avanzati per Key	• Termina con .jpg • Termina con .png
Posizionamenti	Creare 2 copie replicate in due pool di storage

Policy ILM per esempio 3: Migliore protezione per i file di immagine

Questo esempio di policy ILM include tre regole:

- La prima regola di cancellazione codifica tutti i file di immagine superiori a 1 MB.
- La seconda regola consente di creare due copie dei file immagine rimanenti (ovvero, immagini di dimensioni pari o inferiori a 1 MB).
- La regola predefinita si applica a tutti gli oggetti rimanenti (ovvero a tutti i file non immagine).

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Esempio 4: Regole ILM e policy per gli oggetti con versione S3

Se si dispone di un bucket S3 con versione abilitata, è possibile gestire le versioni non correnti degli oggetti includendo regole nel criterio ILM che utilizzano "tempo non corrente" come tempo di riferimento.

> Se si specifica un tempo di conservazione limitato per gli oggetti, questi verranno eliminati in modo permanente una volta raggiunto il periodo di tempo. Assicurarsi di comprendere per quanto tempo gli oggetti verranno conservati.

Come illustrato in questo esempio, è possibile controllare la quantità di storage utilizzata dagli oggetti con versione utilizzando istruzioni di posizionamento diverse per le versioni degli oggetti non correnti.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

> Per eseguire la simulazione dei criteri ILM su una versione non corrente di un oggetto, è necessario conoscere l'UUID o il CBID della versione dell'oggetto. Per trovare UUID e CBID, utilizzare "ricerca dei metadati degli oggetti" mentre l'oggetto è ancora attuale.

Informazioni correlate

- "Modalità di eliminazione degli oggetti"

ILM regola 1 per esempio 4: Salva tre copie per 10 anni

Questa regola ILM di esempio memorizza una copia di ciascun oggetto in tre siti per 10 anni.

Questa regola si applica a tutti gli oggetti, indipendentemente dal fatto che siano con versione.

Definizione della regola	Valore di esempio
Pool di storage	Tre pool di storage, ciascuno costituito da diversi data center, denominati Sito 1, Sito 2 e Sito 3.
Nome della regola	Tre copie dieci anni

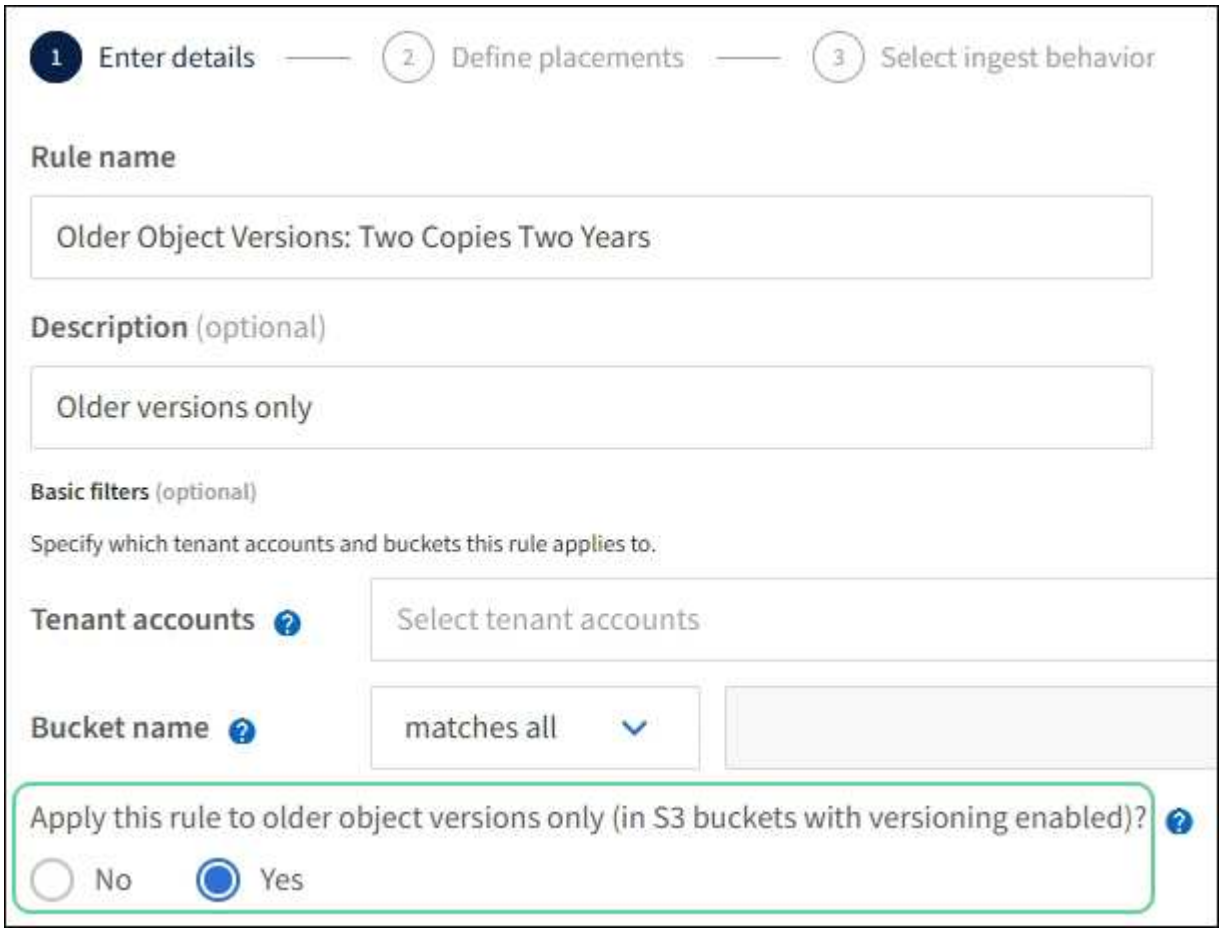
Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Il giorno 0, conserva tre copie replicate per 10 anni (3,652 giorni), una nel sito 1, una nel sito 2 e una nel sito 3. Alla fine dei 10 anni, eliminare tutte le copie dell'oggetto.

ILM regola 2 per esempio 4: Salva due copie di versioni non correnti per 2 anni

Questa regola ILM di esempio memorizza due copie delle versioni non correnti di un oggetto con versione S3 per 2 anni.

Poiché la regola ILM 1 si applica a tutte le versioni dell'oggetto, è necessario creare un'altra regola per filtrare le versioni non correnti.

Per creare una regola che utilizza "ora non corrente" come ora di riferimento, selezionare **Sì** per la domanda "Applica questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?" Nel passaggio 1 (immettere i dettagli) della procedura guidata Crea una regola ILM. Quando si seleziona **Sì**, viene automaticamente selezionata l'opzione *ora non corrente* per l'ora di riferimento e non è possibile selezionare un'ora di riferimento diversa.



In questo esempio, vengono memorizzate solo due copie delle versioni non correnti, che verranno memorizzate per due anni.

Definizione della regola	Valore di esempio
Pool di storage	Due pool di storage, ciascuno in diversi data center, sito 1 e sito 2.
Nome della regola	Versioni non correnti: Due copie per due anni
Tempo di riferimento	Ora non corrente Selezionato automaticamente quando si seleziona **Sì** per la domanda "Applica questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?" Nella procedura guidata Crea una regola ILM.
Posizionamenti	Il giorno 0 relativo all'ora non corrente (ovvero, a partire dal giorno in cui la versione dell'oggetto diventa la versione non corrente), mantenere due copie replicate delle versioni dell'oggetto non correnti per 2 anni (730 giorni), una nel sito 1 e una nel sito 2. Alla fine di 2 anni, eliminare le versioni non aggiornate.

Policy ILM per esempio 4: Oggetti con versione S3

Se si desidera gestire le versioni precedenti di un oggetto in modo diverso dalla versione corrente, le regole che utilizzano l'ora non corrente come ora di riferimento devono essere visualizzate nel criterio ILM prima delle regole applicabili alla versione corrente dell'oggetto.

Un criterio ILM per gli oggetti con versione S3 potrebbe includere regole ILM come le seguenti:

- Mantenere le versioni precedenti (non aggiornate) di ciascun oggetto per 2 anni, a partire dal giorno in cui la versione è diventata non aggiornata.

> Le regole "tempo non corrente" devono essere visualizzate nel criterio prima delle regole che si applicano alla versione dell'oggetto corrente. In caso contrario, le versioni degli oggetti non correnti non verranno mai abbinate alla regola "tempo non corrente".

- Al momento dell'acquisizione, creare tre copie replicate e memorizzare una copia in ciascuno dei tre siti. Conserva le copie della versione corrente dell'oggetto per 10 anni.

Quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- Qualsiasi versione dell'oggetto non corrente verrebbe associata dalla prima regola. Se una versione dell'oggetto non corrente ha più di 2 anni, viene eliminata in modo permanente da ILM (tutte le copie della versione non corrente vengono rimosse dalla griglia).
- La seconda regola corrisponde alla versione corrente dell'oggetto. Quando la versione corrente dell'oggetto è stata archiviata per 10 anni, il processo ILM aggiunge un marcatore di eliminazione come versione corrente dell'oggetto e rende la versione precedente "non corrente". La prossima volta che si verifica la valutazione ILM, questa versione non corrente corrisponde alla prima regola. Di conseguenza, la copia del sito 3 viene eliminata e le due copie del sito 1 e del sito 2 vengono memorizzate per altri 2 anni.

Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione

È possibile utilizzare un filtro di posizione e il rigoroso comportamento di acquisizione in

una regola per impedire che gli oggetti vengano salvati in una determinata posizione del data center.

In questo esempio, un tenant con sede a Parigi non desidera memorizzare alcuni oggetti al di fuori dell'UE a causa di problemi normativi. Altri oggetti, inclusi tutti gli oggetti di altri account tenant, possono essere memorizzati nel data center di Parigi o nel data center statunitense.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

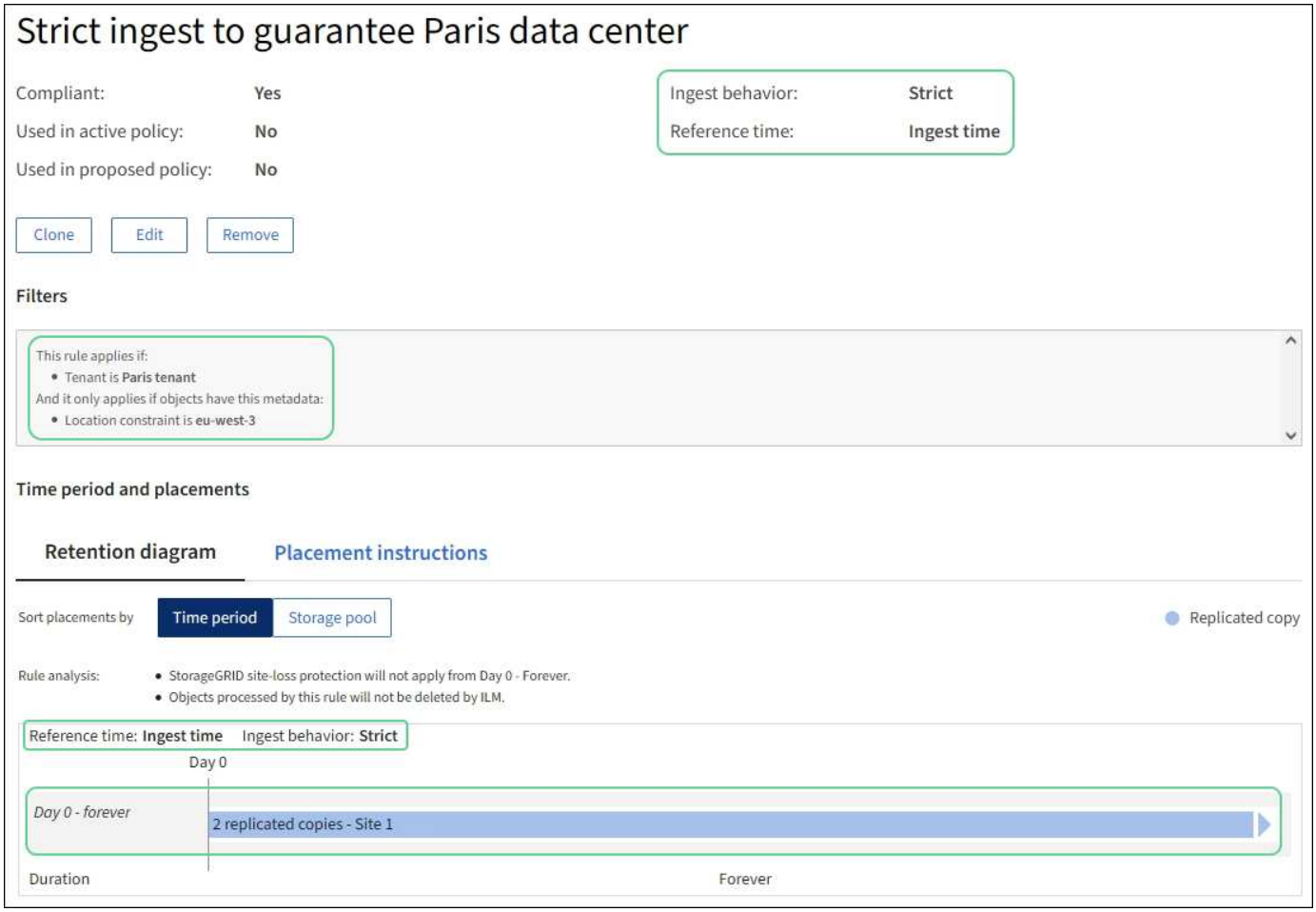
- "Opzioni di acquisizione"
- "Create ILM rule (Crea regola ILM): Selezionare il comportamento di acquisizione"

ILM regola 1 per esempio 5: Ingest rigoroso per garantire il data center di Parigi

Questa regola ILM di esempio utilizza il comportamento rigoroso dell'acquisizione per garantire che gli oggetti salvati da un tenant basato su Parigi nei bucket S3 con la regione impostata su ue-West-3 (Parigi) non vengano mai memorizzati nel data center statunitense.

Questa regola si applica agli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 (Parigi).

Definizione della regola	Valore di esempio
Account tenant	Tenant di Parigi
Filtro avanzato	Il vincolo di posizione equivale a eu-West-3
Pool di storage	Sito 1 (Parigi)
Nome della regola	Un ingest rigoroso per garantire il data center di Parigi
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre nel sito 1 (Parigi)
Comportamento di acquisizione	Rigoroso. Utilizza sempre le posizioni di questa regola per l'acquisizione. L'acquisizione non riesce se non è possibile memorizzare due copie dell'oggetto nel data center di Parigi.



ILM regola 2 per esempio 5: Acquisizione bilanciata per altri oggetti

Questa regola ILM di esempio utilizza il comportamento di acquisizione bilanciata per fornire un'efficienza ILM ottimale per qualsiasi oggetto non associato alla prima regola. Verranno memorizzate due copie di tutti gli oggetti corrispondenti a questa regola: Una nel data center degli Stati Uniti e una nel data center di Parigi. Se la regola non può essere soddisfatta immediatamente, le copie temporanee vengono memorizzate in qualsiasi posizione disponibile.

Questa regola si applica agli oggetti che appartengono a qualsiasi tenant e a qualsiasi area.

Definizione della regola	Valore di esempio
Account tenant	Ignorare
Filtro avanzato	*Non specificato*
Pool di storage	Sito 1 (Parigi) e sito 2 (Stati Uniti)
Nome della regola	2 copie di 2 data center
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre in due data center

Definizione della regola	Valore di esempio
Comportamento di acquisizione	Bilanciato. Gli oggetti che corrispondono a questa regola vengono posizionati in base alle istruzioni di posizionamento della regola, se possibile. In caso contrario, le copie temporanee vengono eseguite in qualsiasi ubicazione disponibile.

Policy ILM per esempio 5: Combinazione di comportamenti di acquisizione

Il criterio ILM di esempio include due regole che hanno comportamenti di acquisizione diversi.

Un criterio ILM che utilizza due diversi comportamenti di acquisizione potrebbe includere regole ILM come le seguenti:

- Memorizzare gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 (Parigi) solo nel data center di Parigi. Non eseguire l'acquisizione se il data center di Parigi non è disponibile.
- Memorizzare tutti gli altri oggetti (inclusi quelli che appartengono al tenant di Parigi ma che hanno una regione bucket diversa) nel data center statunitense e nel data center di Parigi. Se le istruzioni di posizionamento non possono essere soddisfatte, eseguire copie temporanee in qualsiasi ubicazione disponibile.

Quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- Tutti gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 vengono abbinati alla prima regola e memorizzati nel data center di Parigi. Poiché la prima regola utilizza un ingest rigoroso, questi oggetti non vengono mai memorizzati nel data center statunitense. Se i nodi di storage nel data center di Parigi non sono disponibili, l'acquisizione non riesce.
- Tutti gli altri oggetti sono abbinati dalla seconda regola, inclusi gli oggetti che appartengono al tenant di Parigi e che non hanno la regione del bucket S3 impostata su eu-West-3. Una copia di ciascun oggetto viene salvata in ciascun data center. Tuttavia, poiché la seconda regola utilizza l'acquisizione bilanciata, se un data center non è disponibile, vengono salvate due copie temporanee in qualsiasi posizione disponibile.

Esempio 6: Modificare un criterio ILM

Se è necessario modificare la protezione dei dati o aggiungere nuovi siti, è possibile creare e attivare una nuova policy ILM.

Prima di modificare una policy, è necessario comprendere in che modo le modifiche apportate ai posizionamenti ILM possono influire temporaneamente sulle prestazioni generali di un sistema StorageGRID.

In questo esempio, è stato aggiunto un nuovo sito StorageGRID in un'espansione e occorre implementare una nuova policy ILM attiva per memorizzare i dati nel nuovo sito. Per implementare un nuovo criterio attivo, innanzitutto "creare un criterio". Successivamente, devi "simulare" e poi "attivare" la nuova policy.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

In che modo la modifica di un criterio ILM influisce sulle performance

Quando si attiva un nuovo criterio ILM, le prestazioni del sistema StorageGRID potrebbero risentirne

temporaneamente, soprattutto se le istruzioni di posizionamento nel nuovo criterio richiedono lo spostamento di molti oggetti esistenti in nuove posizioni.

Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Per garantire che un nuovo criterio ILM non influisca sul posizionamento degli oggetti replicati e codificati in cancellazione esistenti, è possibile "Creare una regola ILM con un filtro per l'ora di acquisizione". Ad esempio, **Ingest Time *è attivo o successivo a <date and time>***, in modo che la nuova regola si applichi solo agli oggetti acquisiti in data e ora specificate o successive.

I tipi di modifiche ai criteri ILM che possono influire temporaneamente sulle prestazioni di StorageGRID includono:

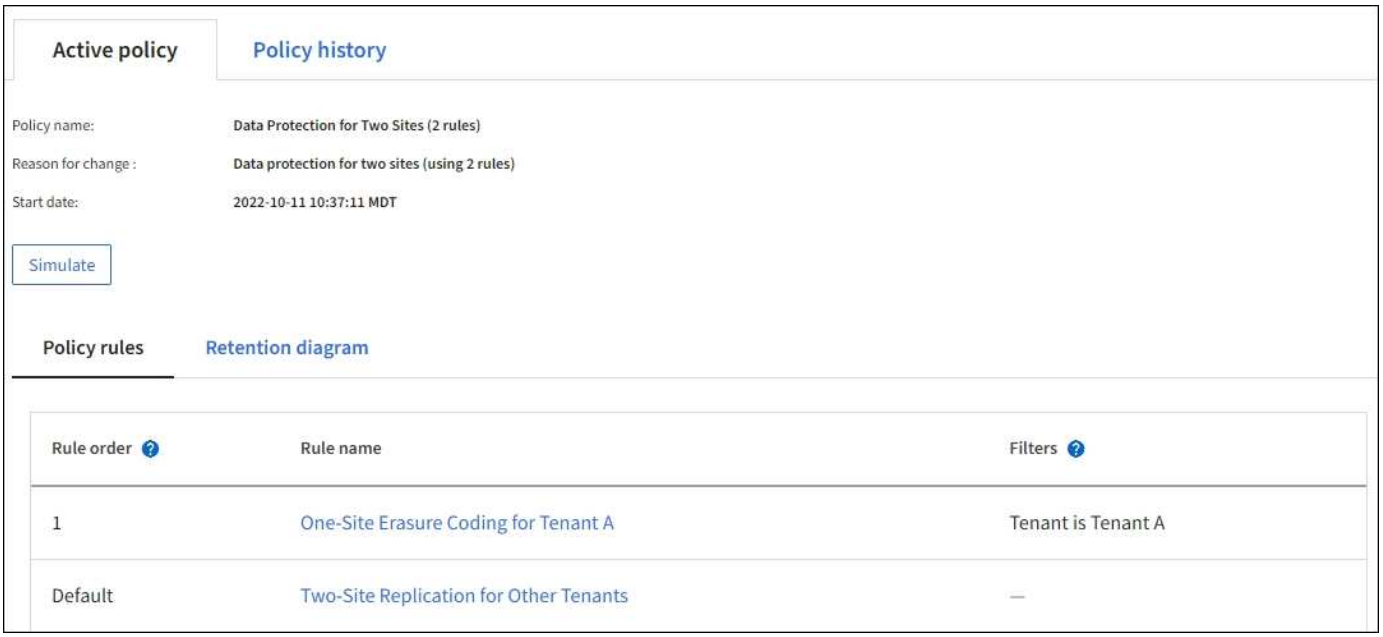
- Applicazione di un profilo di erasure coding diverso agli oggetti esistenti sottoposti a erasure coding.

> StorageGRID considera ogni profilo di erasure coding come univoco e non riutilizza i frammenti di erasure coding quando viene utilizzato un nuovo profilo.

- Modifica del tipo di copie richieste per gli oggetti esistenti; ad esempio, conversione di una grande percentuale di oggetti replicati in oggetti con codifica per la cancellazione.
- Spostamento di copie di oggetti esistenti in una posizione completamente diversa; ad esempio, spostamento di un numero elevato di oggetti da o verso un Cloud Storage Pool o da o verso un sito remoto.

Policy ILM attiva ad esempio 6: Protezione dei dati in due siti

In questo esempio, la policy ILM attiva è stata inizialmente progettata per un sistema StorageGRID a due siti e utilizza due regole ILM.



In questa policy ILM, gli oggetti appartenenti al tenant A sono protetti da una codifica di cancellazione 2+1 in un singolo sito, mentre gli oggetti appartenenti a tutti gli altri tenant sono protetti in due siti utilizzando la replica

a 2 copie.

Regola 1: Erasure coding per un sito per il tenant A.

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione one-site per il tenant A.
Account tenant	Tenant A.
Pool di storage	Sito 1
Posizionamenti	2+1 erasure coding in Site 1 dal giorno 0 a per sempre

Regola 2: Replica a due siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a due siti per altri tenant
Account tenant	Ignorare
Pool di storage	Sito 1 e sito 2
Posizionamenti	Due copie replicate dal giorno 0 a sempre: Una copia nel sito 1 e una nel sito 2.

Criterio ILM per esempio 6: Protezione dei dati in tre siti

In questo esempio, la policy ILM viene sostituita con una nuova policy per un sistema StorageGRID a tre siti.

Dopo aver eseguito un'espansione per aggiungere il nuovo sito, l'amministratore della griglia ha creato due nuovi pool di storage: Un pool di storage per il sito 3 e un pool di storage contenente tutti e tre i siti (non lo stesso del pool di storage predefinito di tutti i nodi di storage). Quindi, l'amministratore ha creato due nuove regole ILM e un nuovo criterio ILM, progettato per proteggere i dati in tutti e tre i siti.

Quando viene attivata questa nuova policy ILM, gli oggetti appartenenti al tenant A saranno protetti da una cancellazione 2+1 in tre siti, mentre gli oggetti appartenenti ad altri tenant (e gli oggetti più piccoli appartenenti al tenant A) saranno protetti in tre siti utilizzando la replica a 3 copie.

Regola 1: Erasure coding a tre siti per il tenant A.

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione a tre siti per il tenant A.
Account tenant	Tenant A.
Pool di storage	Tutti e 3 i siti (inclusi Sito 1, Sito 2 e Sito 3)

Definizione della regola	Valore di esempio
Posizionamenti	2+1 erasure coding in tutti e 3 i siti dal giorno 0 a per sempre

Regola 2: Replica a tre siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a tre siti per altri tenant
Account tenant	Ignorare
Pool di storage	Sito 1, sito 2 e sito 3
Posizionamenti	Tre copie replicate dal giorno 0 a sempre: Una copia presso il sito 1, una copia presso il sito 2 e una copia presso il sito 3.

Attivazione del criterio ILM ad esempio 6

Quando si attiva un nuovo criterio ILM, è possibile spostare gli oggetti esistenti in nuove posizioni o creare nuove copie degli oggetti per gli oggetti esistenti, in base alle istruzioni di posizionamento nelle regole nuove o aggiornate.

> Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile. Esaminare attentamente e simulare la policy prima di attivarla per confermare che funzionerà come previsto.

> Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Cosa succede quando cambiano le istruzioni di erasure coding

Nel criterio ILM attualmente attivo, per questo esempio, gli oggetti appartenenti al tenant A sono protetti utilizzando la codifica di cancellazione 2+1 nel sito 1. Nella nuova policy ILM, gli oggetti appartenenti al tenant A saranno protetti mediante erasure coding 2+1 nei siti 1, 2 e 3.

Quando viene attivato il nuovo criterio ILM, si verificano le seguenti operazioni ILM:

- I nuovi oggetti acquisiti dal tenant A vengono suddivisi in due frammenti di dati e viene aggiunto un frammento di parità. Quindi, ciascuno dei tre frammenti viene memorizzato in un sito diverso.
- Gli oggetti esistenti appartenenti al tenant A vengono rivalutati durante il processo di scansione ILM in corso. Poiché le istruzioni di posizionamento dell'ILM utilizzano un nuovo profilo di erasure coding, vengono creati e distribuiti ai tre siti frammenti completamente nuovi e codificati tramite erasure coding.

I frammenti 2+1 esistenti nel sito 1 non vengono riutilizzati. StorageGRID considera ogni profilo di erasure coding come univoco e non riutilizza i frammenti di erasure coding quando viene utilizzato un nuovo profilo.

Cosa succede quando cambiano le istruzioni di replica

Nella policy ILM attualmente attiva per questo esempio, gli oggetti appartenenti ad altri tenant sono protetti utilizzando due copie replicate nei pool di storage dei siti 1 e 2. Nella nuova policy ILM, gli oggetti appartenenti ad altri tenant verranno protetti attraverso tre copie replicate nei pool di storage dei siti 1, 2 e 3.

Quando viene attivato il nuovo criterio ILM, si verificano le seguenti operazioni ILM:

- Quando un tenant diverso dal tenant A acquisisce un nuovo oggetto, StorageGRID crea tre copie e salva una copia in ogni sito.
- Gli oggetti esistenti appartenenti a questi altri tenant vengono rivalutati durante il processo di scansione ILM in corso. Poiché le copie degli oggetti esistenti nei siti 1 e 2 continuano a soddisfare i requisiti di replica della nuova regola ILM, StorageGRID deve creare solo una nuova copia dell'oggetto per il sito 3.

Impatto delle performance dell'attivazione di questa policy

Quando il criterio ILM in questo esempio è attivato, le prestazioni generali del sistema StorageGRID saranno temporaneamente influenzate. Per creare nuovi frammenti erasure-coded per gli oggetti esistenti del tenant A e nuove copie replicate nel sito 3 per gli oggetti esistenti degli altri tenant saranno necessari livelli di risorse grid superiori al normale.

Come conseguenza della modifica del criterio ILM, le richieste di lettura e scrittura del client potrebbero temporaneamente riscontrare latenze superiori al normale. Le latenze torneranno ai livelli normali dopo che le istruzioni di posizionamento sono state completamente implementate nella griglia.

Per evitare problemi di risorse quando si attiva un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Ingest Time in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare Ingest Time (tempo di acquisizione) su un valore maggiore o uguale al tempo approssimativo in cui la nuova policy verrà applicata per garantire che gli oggetti esistenti non vengano spostati inutilmente.

Contattare il supporto tecnico se è necessario rallentare o aumentare la velocità di elaborazione degli oggetti dopo una modifica della policy ILM.

Esempio 7: Policy ILM conforme per il blocco oggetti S3

È possibile utilizzare il bucket S3, le regole ILM e il criterio ILM in questo esempio come punto di partenza quando si definisce un criterio ILM per soddisfare i requisiti di protezione e conservazione degli oggetti nei bucket con blocco oggetti S3 attivato.

Se hai utilizzato la funzionalità di conformità legacy nelle versioni precedenti di StorageGRID, puoi anche utilizzare questo esempio per gestire qualsiasi bucket esistente con la funzionalità di conformità legacy attivata.

Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

- "Gestire gli oggetti con S3 Object Lock"
- "Creare un criterio ILM"

Esempio di bucket e oggetti per S3 Object Lock

In questo esempio, un account tenant S3 denominato Bank of ABC ha utilizzato il tenant Manager per creare un bucket con blocco oggetti S3 abilitato per memorizzare i record bancari critici.

Definizione del bucket	Valore di esempio
Nome account tenant	Banca di ABC
Nome bucket	banca-record
Area bucket	us-east-1 (impostazione predefinita)

Ogni versione di oggetto e oggetto aggiunta al bucket dei record bancari utilizzerà i seguenti valori per `retain-until-date` e. `legal hold` impostazioni.

Impostazione per ciascun oggetto	Valore di esempio
`retain-until-date`	"2030-12-30T23:59:59Z" (30 dicembre 2030) Ogni versione dell'oggetto ha il proprio `retain-until-date` impostazione. Questa impostazione può essere aumentata, ma non ridotta.
`legal hold`	"OFF" (non in vigore) È possibile mettere o revocare un blocco legale su qualsiasi versione oggetto in qualsiasi momento durante il periodo di conservazione. Se un oggetto è sottoposto a un blocco legale, non è possibile eliminarlo anche se `retain-until-date` è stato raggiunto.

Regola ILM 1 per blocco oggetto S3 esempio: Profilo di erasure coding con abbinamento bucket

Questa regola ILM di esempio si applica solo all'account tenant S3 denominato Bank of ABC. Corrisponde a qualsiasi oggetto in `bank-records` Bucket e quindi utilizza l'erasure coding per memorizzare l'oggetto sui nodi storage in tre siti di data center utilizzando un profilo di erasure coding 6+3. Questa regola soddisfa i requisiti dei bucket con blocco oggetti S3 attivato: Una copia viene conservata nei nodi di storage dal giorno 0 a per sempre, utilizzando l'ora di inizio come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Compliant Rule (regola conforme): Oggetti EC nel bucket dei record bancari - Bank of ABC
Account tenant	Banca di ABC

Definizione della regola	Valore di esempio
Nome bucket	`bank-records`
Filtro avanzato	Dimensione oggetto (MB) maggiore di 1 **Nota:** questo filtro garantisce che la codifica erasure non venga utilizzata per oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 memorizzare per sempre
Profilo di erasure coding	• Creare una copia con codifica di cancellazione sui nodi di storage in tre siti del data center • Utilizza uno schema di erasure coding 6+3

ILM regola 2 per S3 Object Lock esempio: Regola non conforme

Questa regola ILM di esempio memorizza inizialmente due copie di oggetti replicate sui nodi di storage. Dopo un anno, memorizza una copia su un Cloud Storage Pool per sempre. Poiché questa regola utilizza un Cloud Storage Pool, non è conforme e non si applica agli oggetti nei bucket con S3 Object Lock attivato.

Definizione della regola	Valore di esempio
Nome della regola	Regola non conforme: Utilizza il Cloud Storage Pool
Account tenant	Non specificato
Nome bucket	Non specificato, ma si applica solo ai bucket che non hanno S3 Object Lock (o la funzionalità Compliance legacy) abilitato.
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	• Il giorno 0, conserva due copie replicate sui nodi di storage nel data center 1 e nel data center 2 per 365 giorni • Dopo 1 anno, conserva per sempre una copia replicata in un Cloud Storage Pool

ILM regola 3 per S3 Object Lock esempio: Regola predefinita

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due data center. Questa regola di conformità è stata progettata per essere la regola predefinita nel criterio ILM. Non include alcun filtro, non utilizza il tempo di riferimento non corrente e soddisfa i requisiti dei bucket con S3 Object Lock abilitato: Due copie di oggetti vengono conservate sui nodi di storage dal giorno 0 a per sempre, utilizzando Ingest come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Regola di conformità predefinita: Due copie di due data center
Account tenant	Non specificato
Nome bucket	Non specificato
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 all'anno, conserva due copie replicate, una sui nodi di storage nel data center 1 e una sui nodi di storage nel data center 2.

Esempio di policy ILM conforme per S3 Object Lock

Per creare un criterio ILM che protegga efficacemente tutti gli oggetti del sistema, inclusi quelli nei bucket con S3 Object Lock attivato, è necessario selezionare le regole ILM che soddisfano i requisiti di storage per tutti gli oggetti. Quindi, è necessario simulare e attivare il criterio.

Aggiungere regole al criterio

In questo esempio, il criterio ILM include tre regole ILM, nel seguente ordine:

1. Regola conforme che utilizza la codifica erasure per proteggere oggetti superiori a 1 MB in un bucket specifico con blocco oggetti S3 attivato. Gli oggetti vengono memorizzati nei nodi di storage dal giorno 0 a sempre.
2. Una regola non conforme che crea due copie di oggetti replicate sui nodi di storage per un anno e sposta una copia di oggetto in un pool di storage cloud per sempre. Questa regola non si applica ai bucket con blocco oggetti S3 attivato perché utilizza un pool di storage cloud.
3. La regola di conformità predefinita che crea due copie di oggetti replicate sui nodi di storage dal giorno 0 a per sempre.

Simulare la policy

Dopo aver aggiunto regole al criterio, scelto una regola conforme predefinita e organizzato le altre regole, è necessario simulare il criterio testando gli oggetti dal bucket con blocco oggetti S3 attivato e da altri bucket. Ad esempio, quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- La prima regola corrisponde solo agli oggetti di test che sono superiori a 1 MB nei record di banco bucket per il tenant Bank of ABC.
- La seconda regola corrisponde a tutti gli oggetti in tutti i bucket non conformi per tutti gli altri account tenant.
- La regola predefinita corrisponde ai seguenti oggetti:
  - Oggetti di 1 MB o inferiori nei bucket bank-records per il tenant Bank of ABC.
  - Oggetti in qualsiasi altro bucket con S3 Object Lock attivato per tutti gli altri account tenant.

Attivare il criterio

Quando si è completamente soddisfatti del fatto che il nuovo criterio protegga i dati degli oggetti come previsto, è possibile attivarlo.

Esempio 8: Priorità per il ciclo di vita dei bucket S3 e la politica ILM

A seconda della configurazione del ciclo di vita, gli oggetti seguono le impostazioni di conservazione del ciclo di vita del bucket S3 o di un criterio ILM.

Esempio di priorità del ciclo di vita dei bucket rispetto alla policy ILM

Policy ILM

- Regola basata sul riferimento non corrente: Il giorno 0, tenere X copie per 20 giorni
- Regola basata sul riferimento al tempo di acquisizione (impostazione predefinita): Il giorno 0, conservare le X copie per 50 giorni

Ciclo di vita della benna

- `Filter: {Prefix: "docs/"}, Expiration: Days: 100, NoncurrentVersionExpiration: Days: 5`

Risultato

- Viene acquisito un oggetto denominato "docs/text". Corrisponde al filtro del ciclo di vita del bucket del prefisso "docs/".
  - Dopo 100 giorni viene creato un marker di eliminazione e "documenti/testo" diventa non corrente.
  - Dopo 5 giorni, un totale di 105 giorni dall'acquisizione, "documenti/testo" viene eliminato.
- Viene acquisito un oggetto denominato "video/filmato". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
  - Dopo 50 giorni viene creato un marker di eliminazione e "video/filmato" diventa non corrente.
  - Dopo 20 giorni, un totale di 70 giorni dall'acquisizione, "video/film" viene eliminato.

Esempio di ciclo di vita del bucket che mantiene implicitamente per sempre

Policy ILM

- Regola basata sul riferimento non corrente: Il giorno 0, tenere X copie per 20 giorni
- Regola basata sul riferimento al tempo di acquisizione (impostazione predefinita): Il giorno 0, conservare le X copie per 50 giorni

Ciclo di vita della benna

- `Filter: {Prefix: "docs/"}, Expiration: ExpiredObjectDeleteMarker: true`

Risultato

- Viene acquisito un oggetto denominato "docs/text". Corrisponde al filtro del ciclo di vita del bucket del prefisso "docs/".

  Il `Expiration` l'azione si applica solo ai marcatori di eliminazione scaduti, il che implica mantenere tutto il resto per sempre (a partire da "docs/").

  I marcatori di eliminazione che iniziano con "docs/" vengono rimossi quando diventano scaduti.

- Viene acquisito un oggetto denominato "video/filmato". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
  - Dopo 50 giorni viene creato un marker di eliminazione e "video/filmato" diventa non corrente.
  - Dopo 20 giorni, un totale di 70 giorni dall'acquisizione, "video/film" viene eliminato.

Esempio di utilizzo del ciclo di vita bucket per duplicare ILM e ripulire i marcatori di eliminazione scaduti

Policy ILM

- Regola basata sul riferimento non corrente: Il giorno 0, tenere X copie per 20 giorni
- Regola basata sul riferimento al tempo di acquisizione (impostazione predefinita): Il giorno 0, conservare le X copie per 50 giorni

Ciclo di vita della benna

- `Filter: {}, Expiration: Days: 50, NoncurrentVersionExpiration: Days: 20`

Risultato

- Il criterio ILM viene duplicato nel ciclo di vita del bucket.
- Un oggetto viene acquisito. Nessun filtro significa che il ciclo di vita del bucket si applica a tutti gli oggetti e sovrascrive le impostazioni di conservazione ILM.
  - Dopo 50 giorni viene creato un marker di eliminazione e l'oggetto diventa non corrente.
  - Dopo 20 giorni, per un totale di 70 giorni dall'acquisizione, l'oggetto non corrente viene eliminato e il marker di eliminazione diventa scaduto.
  - Dopo 30 giorni, per un totale di 100 giorni dall'acquisizione, il marker di eliminazione scaduto viene eliminato.

Protezione avanzata del sistema

Protezione avanzata del sistema: Panoramica

La protezione avanzata del sistema è il processo che consente di eliminare il maggior numero possibile di rischi per la sicurezza da un sistema StorageGRID.

Questo documento fornisce una panoramica delle linee guida per la protezione avanzata specifiche di StorageGRID. Queste linee guida integrano le Best practice standard di settore per la protezione avanzata dei sistemi. Ad esempio, queste linee guida presuppongono l'utilizzo di password complesse per StorageGRID, l'utilizzo di HTTPS invece di HTTP e l'attivazione dell'autenticazione basata su certificato, se disponibile.

Durante l'installazione e la configurazione di StorageGRID, è possibile utilizzare queste linee guida per soddisfare qualsiasi obiettivo di sicurezza prescritto in termini di riservatezza, integrità e disponibilità del sistema informativo.

StorageGRID segue il "Policy di gestione delle vulnerabilità di NetApp". Le vulnerabilità segnalate vengono verificate e risolte in base al processo di risposta agli incidenti di sicurezza del prodotto.

Considerazioni generali per la protezione avanzata dei sistemi StorageGRID

Quando si esegue la protezione avanzata di un sistema StorageGRID, è necessario considerare quanto segue:

- Quale delle tre reti StorageGRID è stata implementata? Tutti i sistemi StorageGRID devono utilizzare la rete griglia, ma è possibile utilizzare anche la rete di amministrazione, la rete client o entrambi. Ogni rete ha considerazioni di sicurezza diverse.
- Il tipo di piattaforme utilizzate per i singoli nodi nel sistema StorageGRID. I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un motore di container su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma dispone di un proprio set di Best practice per la protezione avanzata.
- Quanto sono affidabili gli account tenant. Se sei un provider di servizi con account tenant non attendibili, avrai problemi di sicurezza diversi rispetto all'utilizzo di tenant interni affidabili.
- Quali requisiti e convenzioni di sicurezza sono seguiti dalla tua organizzazione. Potrebbe essere necessario rispettare requisiti normativi o aziendali specifici.

Linee guida per la protezione avanzata degli aggiornamenti software

Per difenderti dagli attacchi, devi tenere aggiornato il tuo sistema StorageGRID e i servizi correlati.

Aggiornamenti al software StorageGRID

Se possibile, è necessario aggiornare il software StorageGRID alla versione principale più recente o alla versione principale precedente. Mantenere aggiornato StorageGRID aiuta a ridurre il tempo di attivazione delle vulnerabilità note e l'area complessiva della superficie di attacco. Inoltre, le versioni più recenti di StorageGRID contengono spesso funzionalità di protezione avanzata che non sono incluse nelle versioni precedenti.

Consultare "Tool di matrice di interoperabilità NetApp" (IMT) per determinare la versione del software StorageGRID da utilizzare. Quando è necessaria una correzione rapida, NetApp assegna la priorità alla creazione di aggiornamenti per le release più recenti. Alcune patch potrebbero non essere compatibili con le release precedenti.

- Per scaricare le versioni più recenti di StorageGRID e gli aggiornamenti rapidi, visitare il sito Web all'indirizzo "Download NetApp: StorageGRID".
- Per aggiornare il software StorageGRID, consultare "istruzioni per l'aggiornamento".
- Per applicare una correzione rapida, consultare "Procedura di hotfix StorageGRID".

Aggiornamenti a servizi esterni

I servizi esterni possono presentare vulnerabilità che influiscono indirettamente su StorageGRID. Devi assicurarti che i servizi da cui dipende StorageGRID siano sempre aggiornati. Questi servizi includono LDAP, KMS (o server KMIP), DNS e NTP.

Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Aggiornamenti agli hypervisor

Se i nodi StorageGRID sono in esecuzione su VMware o su un altro hypervisor, è necessario assicurarsi che il software e il firmware dell'hypervisor siano aggiornati.

Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Upgrade ai nodi Linux

Se i nodi StorageGRID utilizzano piattaforme host Linux, è necessario assicurarsi che gli aggiornamenti di sicurezza e del kernel siano applicati al sistema operativo host. Inoltre, è necessario applicare gli aggiornamenti del firmware all'hardware vulnerabile quando questi aggiornamenti diventano disponibili.

Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Linee guida per la protezione avanzata delle reti StorageGRID

Il sistema StorageGRID supporta fino a tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.

Per informazioni dettagliate sulle reti StorageGRID, consultare "Tipi di rete StorageGRID".

Linee guida per Grid Network

È necessario configurare una rete griglia per tutto il traffico StorageGRID interno. Tutti i nodi Grid si trovano sulla rete Grid e devono essere in grado di comunicare con tutti gli altri nodi.

Durante la configurazione della rete Grid, attenersi alle seguenti linee guida:

- Assicurarsi che la rete sia protetta da client non attendibili, ad esempio quelli su Internet aperto.
- Se possibile, utilizzare Grid Network 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.
- Se l'implementazione di StorageGRID si estende su più data center, utilizzare una rete privata virtuale (VPN) o equivalente sulla rete grid per fornire una protezione aggiuntiva per il traffico interno.
- Alcune procedure di manutenzione richiedono l'accesso Secure shell (SSH) sulla porta 22 tra il nodo di amministrazione primario e tutti gli altri nodi della griglia. Utilizzare un firewall esterno per limitare l'accesso SSH ai client attendibili.

Linee guida per la rete amministrativa

La rete di amministrazione viene generalmente utilizzata per le attività amministrative (dipendenti attendibili che utilizzano Grid Manager o SSH) e per la comunicazione con altri servizi attendibili come LDAP, DNS, NTP o KMS (o server KMIP). Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete di amministrazione, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete di amministrazione. Vedere "elenco delle porte interne".

- Se i client non attendibili possono accedere alla rete di amministrazione, bloccare l'accesso a StorageGRID sulla rete di amministrazione con un firewall esterno.

Linee guida per la rete client

La rete client viene generalmente utilizzata per i tenant e per le comunicazioni con servizi esterni, come il servizio di replica CloudMirror o un altro servizio della piattaforma. Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete client, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete client. Vedere "elenco delle porte interne".
- Accettare il traffico client in entrata solo su endpoint configurati esplicitamente. Consultare le informazioni su "gestione dei controlli firewall".

Linee guida per la protezione avanzata dei nodi StorageGRID

I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un motore di container su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma e ogni tipo di nodo dispone di un proprio set di Best practice per la protezione avanzata.

Controllare l'accesso IPMI remoto a BMC

È possibile attivare o disattivare l'accesso IPMI remoto per tutti i dispositivi che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello alle apparecchiature StorageGRID da parte di chiunque disponga di un account BMC e di una password. Se non è necessario l'accesso IPMI remoto al BMC, disattivare questa opzione.

- Per controllare l'accesso IPMI remoto al BMC in Grid Manager, accedere a **CONFIGURAZIONE** > **protezione** > **Impostazioni di protezione** > **dispositivi**:
  - Deselezionare la casella di controllo **Abilita accesso IPMI remoto** per disattivare l'accesso IPMI al BMC.
  - Selezionare la casella di controllo **Abilita accesso IPMI remoto** per abilitare l'accesso IPMI al BMC.

Configurazione del firewall

Nell'ambito del processo di protezione avanzata del sistema, è necessario rivedere le configurazioni dei firewall esterni e modificarle in modo che il traffico venga accettato solo dagli indirizzi IP e dalle porte da cui è strettamente necessario.

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della rete consentendo di controllare l'accesso alla rete. Dovresti "gestire i controlli firewall interni" per impedire l'accesso alla rete su tutte le porte, ad eccezione di quelle necessarie per l'implementazione della griglia specifica. Le modifiche apportate alla configurazione nella pagina di controllo Firewall vengono distribuite a ciascun nodo.

In particolare, è possibile gestire queste aree:

- **Privileged addresses** (indirizzi con privilegi): È possibile consentire agli indirizzi IP o alle subnet selezionate di accedere alle porte chiuse dalle impostazioni nella scheda Manage external access (Gestisci accesso esterno).

- **Manage external access** (Gestisci accesso esterno): È possibile chiudere le porte aperte per impostazione predefinita o riaprire le porte chiuse in precedenza.
- **Untrusted Client Network**: È possibile specificare se un nodo considera attendibile il traffico in entrata dalla rete client e le porte aggiuntive che si desidera aprire quando è configurata una rete client non attendibile.

Sebbene questo firewall interno offra un ulteriore livello di protezione contro alcune minacce comuni, non elimina la necessità di un firewall esterno.

Per un elenco di tutte le porte interne ed esterne utilizzate da StorageGRID, vedere "Riferimento porta di rete".

Disattivare i servizi inutilizzati

Per tutti i nodi StorageGRID, è necessario disattivare o bloccare l'accesso ai servizi inutilizzati. Ad esempio, se non si intende configurare l'accesso client alle condivisioni di controllo per NFS, bloccare o disattivare l'accesso a questi servizi.

Virtualizzazione, container e hardware condiviso

Per tutti i nodi StorageGRID, evitare di eseguire StorageGRID sullo stesso hardware fisico del software non attendibile. Non presupporre che le protezioni dell'hypervisor impediscano al malware di accedere ai dati protetti da StorageGRID se StorageGRID e il malware esistono sullo stesso hardware fisico. Ad esempio, gli attacchi Meltdown e Spectre sfruttano le vulnerabilità critiche dei processori moderni e consentono ai programmi di rubare dati in memoria sullo stesso computer.

Proteggere i nodi durante l'installazione

Non consentire agli utenti non attendibili di accedere ai nodi StorageGRID sulla rete durante l'installazione dei nodi. I nodi non sono completamente sicuri fino a quando non si sono Uniti alla griglia.

Linee guida per i nodi di amministrazione

I nodi di amministrazione forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. Quando si accede a Grid Manager o al tenant Manager, si sta effettuando la connessione a un nodo amministratore.

Seguire queste linee guida per proteggere i nodi di amministrazione nel sistema StorageGRID:

- Proteggere tutti i nodi di amministrazione da client non attendibili, ad esempio quelli su Internet aperto. Assicurarsi che nessun client non attendibile possa accedere a qualsiasi nodo Admin sulla rete Grid, sulla rete amministrativa o sulla rete client.
- I gruppi StorageGRID controllano l'accesso alle funzioni di gestione griglia e di gestione tenant. Concedere a ciascun gruppo di utenti le autorizzazioni minime richieste per il proprio ruolo e utilizzare la modalità di accesso in sola lettura per impedire agli utenti di modificare la configurazione.
- Quando si utilizzano gli endpoint del bilanciamento del carico StorageGRID, utilizzare i nodi gateway invece dei nodi di amministrazione per il traffico client non attendibile.
- Se si dispone di tenant non attendibili, non consentire loro di accedere direttamente al tenant Manager o all'API di gestione tenant. I tenant non attendibili devono invece utilizzare un portale tenant o un sistema di gestione tenant esterno, che interagisce con l'API di gestione tenant.
- In alternativa, utilizzare un proxy amministratore per un maggiore controllo sulle comunicazioni AutoSupport dai nodi amministrativi al supporto NetApp. Consultare la procedura per "creazione di un proxy amministratore".

- Facoltativamente, utilizzare le porte limitate 8443 e 9443 per separare le comunicazioni di Grid Manager e Tenant Manager. Bloccare la porta condivisa 443 e limitare le richieste del tenant alla porta 9443 per una protezione aggiuntiva.
- Facoltativamente, utilizzare nodi di amministrazione separati per gli amministratori di grid e gli utenti del tenant.

Per ulteriori informazioni, consultare le istruzioni di "Amministrazione di StorageGRID".

Linee guida per i nodi di storage

I nodi di storage gestiscono e memorizzano i dati e i metadati degli oggetti. Seguire queste linee guida per proteggere i nodi di storage nel sistema StorageGRID.

- Non consentire ai client non attendibili di connettersi direttamente ai nodi di storage. Utilizzare un endpoint di bilanciamento del carico servito da un nodo gateway o da un bilanciamento del carico di terze parti.
- Non abilitare i servizi in uscita per tenant non attendibili. Ad esempio, quando si crea l'account per un tenant non attendibile, non consentire al tenant di utilizzare la propria origine di identità e non consentire l'utilizzo dei servizi della piattaforma. Consultare la procedura per "creazione di un account tenant".
- Utilizzare un bilanciamento del carico di terze parti per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.
- In alternativa, puoi utilizzare un proxy storage per un maggiore controllo sui pool di cloud storage e sulle comunicazioni dei servizi della piattaforma dai nodi storage ai servizi esterni. Consultare la procedura per "creazione di un proxy di archiviazione".
- Se lo si desidera, connettersi a servizi esterni utilizzando la rete client. Quindi, selezionare **CONFIGURATION** > **Security** > **Firewall control** > **Untrusted Client Networks** e indicare che la rete client sul nodo di storage non è attendibile. Il nodo di storage non accetta più alcun traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita per Platform Services.

Linee guida per i nodi gateway

I nodi gateway forniscono un'interfaccia opzionale per il bilanciamento del carico che le applicazioni client possono utilizzare per connettersi a StorageGRID. Attenersi alle seguenti linee guida per proteggere i nodi gateway nel sistema StorageGRID:

- Configurare e utilizzare gli endpoint del bilanciamento del carico. Vedere "Considerazioni per il bilanciamento del carico".
- Utilizzare un bilanciamento del carico di terze parti tra il client e il nodo gateway o i nodi di storage per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi. Se si utilizza un bilanciamento del carico di terze parti, il traffico di rete può comunque essere configurato in modo opzionale per passare attraverso un endpoint interno di bilanciamento del carico o essere inviato direttamente ai nodi di storage.
- Se si utilizzano endpoint di bilanciamento del carico, è possibile che i client si connettano tramite la rete client. Quindi, selezionare **CONFIGURATION** > **Security** > **Firewall control** > **Untrusted Client Networks** (reti client non attendibili) e indicare che la rete client sul nodo gateway non è attendibile. Il nodo gateway accetta solo il traffico in entrata sulle porte esplicitamente configurate come endpoint del bilanciamento del carico.

Linee guida per i nodi dell'appliance hardware

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.

Segui queste linee guida per proteggere i nodi dell'appliance hardware nel tuo sistema StorageGRID:

- Se l'appliance utilizza Gestione di sistema di SANtricity per la gestione del controller di storage, impedire ai client non attendibili di accedere a Gestione di sistema di SANtricity tramite la rete.
- Se l'appliance dispone di un BMC (Baseboard Management Controller), tenere presente che la porta di gestione BMC consente un accesso hardware di basso livello. Collegare la porta di gestione BMC solo a una rete di gestione interna sicura e affidabile. Se tale rete non è disponibile, lasciare la porta di gestione BMC disconnessa o bloccata, a meno che non venga richiesta una connessione BMC dal supporto tecnico.
- Se l'appliance supporta la gestione remota dell'hardware del controller su Ethernet utilizzando lo standard IPMI (Intelligent Platform Management Interface), bloccare il traffico non attendibile sulla porta 623.

> ⓘ È possibile attivare o disattivare l'accesso IPMI remoto per tutti i dispositivi che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello alle apparecchiature StorageGRID da parte di chiunque disponga di un account BMC e di una password. Se non è necessario l'accesso IPMI remoto al BMC, disattivare questa opzione utilizzando uno dei seguenti metodi:
> In Grid Manager, andare a **CONFIGURAZIONE** > **sicurezza** > **Impostazioni di protezione** > **dispositivi** e deselezionare la casella di controllo **Abilita accesso IPMI remoto**.
> Nell'API di gestione griglia, utilizzare l'endpoint privato: `PUT /private/bmc`.

- Per i modelli di appliance contenenti dischi SED, FDE o NL-SAS FIPS gestiti con SANtricity System Manager, "Abilitare e configurare la protezione dell'unità SANtricity".
- Per i modelli di appliance che contengono SSD SED o FIPS NVMe gestiti tramite il programma di installazione dell'appliance StorageGRID e il Grid Manager, "Abilitare e configurare la crittografia dell'unità StorageGRID".
- Per le appliance senza SED, FDE o FIPS, abilitare e configurare la crittografia dei nodi software StorageGRID "Utilizzo di un server di gestione delle chiavi (KMS, Key Management Server)".

Linee guida per la protezione avanzata di TLS e SSH

È necessario sostituire i certificati predefiniti creati durante l'installazione e selezionare il criterio di protezione appropriato per le connessioni TLS e SSH.

Linee guida per la protezione avanzata dei certificati

È necessario sostituire i certificati predefiniti creati durante l'installazione con certificati personalizzati.

Per molte organizzazioni, il certificato digitale autofirmato per l'accesso Web a StorageGRID non è conforme alle policy di sicurezza delle informazioni. Nei sistemi di produzione, è necessario installare un certificato digitale con firma CA da utilizzare per l'autenticazione di StorageGRID.

In particolare, è necessario utilizzare certificati server personalizzati anziché i seguenti certificati predefiniti:

- **Certificato dell'interfaccia di gestione**: Utilizzato per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API.
- **Certificato API S3 e Swift**: Utilizzato per proteggere l'accesso ai nodi di storage e ai nodi gateway, utilizzati dalle applicazioni client S3 e Swift per caricare e scaricare i dati degli oggetti.

Vedere "Gestire i certificati di sicurezza" per dettagli e istruzioni.

> StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciamento del carico. Per configurare i certificati di bilanciamento del carico, vedere "Configurare gli endpoint del bilanciamento del carico".

Quando si utilizzano certificati server personalizzati, attenersi alle seguenti linee guida:

- I certificati devono avere un *`subjectAltName`* Che corrisponde alle voci DNS per StorageGRID. Per ulteriori informazioni, vedere la sezione 4,2.1,6, "Nome alternativo oggetto" in "RFC 5280: Certificato PKIX e profilo CRL".
- Se possibile, evitare l'utilizzo di certificati con caratteri jolly. Un'eccezione a questa linea guida è il certificato per un endpoint di stile host virtuale S3, che richiede l'utilizzo di un carattere jolly se i nomi dei bucket non sono noti in anticipo.
- Quando è necessario utilizzare i caratteri jolly nei certificati, è necessario adottare ulteriori misure per ridurre i rischi. Utilizzare un modello con caratteri jolly come `*.s3.example.com`e non utilizzare `s3.example.com` suffisso per altre applicazioni. Questo modello funziona anche con l'accesso S3 di tipo path, ad esempio `dc1-s1.s3.example.com/mybucket`.
- Impostare i tempi di scadenza del certificato su brevi (ad esempio, 2 mesi) e utilizzare l'API Grid Management per automatizzare la rotazione del certificato. Ciò è particolarmente importante per i certificati con caratteri jolly.

Inoltre, i client devono utilizzare un rigoroso controllo del nome host quando comunicano con StorageGRID.

Linee guida per la protezione avanzata dei criteri TLS e SSH

È possibile selezionare un criterio di protezione per determinare quali protocolli e cifrature utilizzare per stabilire connessioni TLS sicure con applicazioni client e connessioni SSH sicure ai servizi StorageGRID interni.

Il criterio di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. Come procedura consigliata, è necessario disattivare le opzioni di crittografia non necessarie per la compatibilità delle applicazioni. Utilizzare il criterio moderno predefinito, a meno che il sistema non debba essere conforme ai criteri comuni o non sia necessario utilizzare altre crittografia.

Vedere "Gestire i criteri TLS e SSH" per dettagli e istruzioni.

Altre linee guida per la protezione avanzata

Oltre a seguire le linee guida per la protezione avanzata per reti e nodi StorageGRID, è necessario seguire le linee guida per la protezione avanzata per altre aree del sistema StorageGRID.

Registri e messaggi di audit

Proteggere sempre i log StorageGRID e l'output dei messaggi di controllo in modo sicuro. I registri e i messaggi di audit di StorageGRID forniscono informazioni preziose dal punto di vista del supporto e della disponibilità del sistema. Inoltre, le informazioni e i dettagli contenuti nei registri StorageGRID e nell'output dei messaggi di audit sono generalmente di natura sensibile.

Configurare StorageGRID per inviare eventi di sicurezza a un server syslog esterno. Se si utilizza l'esportazione syslog, selezionare TLS e RELP/TLS per i protocolli di trasporto.

Vedere "Riferimenti ai file di log" Per ulteriori informazioni sui registri StorageGRID. Vedere "Messaggi di audit" Per ulteriori informazioni sui messaggi di controllo di StorageGRID.

NetApp AutoSupport

La funzione AutoSupport di StorageGRID consente di monitorare in modo proattivo lo stato del sistema e di inviare automaticamente i pacchetti al sito di supporto NetApp, al team di supporto interno dell'organizzazione o a un partner di supporto. Per impostazione predefinita, l'invio di pacchetti AutoSupport a NetApp è attivato quando StorageGRID viene configurato per la prima volta.

La funzione AutoSupport può essere disattivata. Tuttavia, NetApp consiglia di abilitare l'IT perché AutoSupport aiuta a velocizzare l'identificazione e la risoluzione dei problemi in caso di problemi nel sistema StorageGRID.

AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. Data la natura sensibile dei pacchetti AutoSupport, NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio di pacchetti AutoSupport a NetApp.

Condivisione delle risorse tra origini (CORS)

È possibile configurare la condivisione delle risorse cross-origin (CORS) per un bucket S3 se si desidera che quel bucket e gli oggetti in quel bucket siano accessibili alle applicazioni web in altri domini. In generale, non abilitare il CORS a meno che non sia necessario. Se è richiesto un CORS, limitarlo alle origini attendibili.

Consultare la procedura per "Configurazione del CORS (Cross-Origin Resource sharing)".

Dispositivi di sicurezza esterni

Una soluzione di protezione avanzata completa deve affrontare i meccanismi di sicurezza esterni a StorageGRID. L'utilizzo di ulteriori dispositivi di infrastruttura per il filtraggio e la limitazione dell'accesso a StorageGRID è un metodo efficace per stabilire e mantenere una posizione di sicurezza rigorosa. Questi dispositivi di sicurezza esterni includono firewall, sistemi di prevenzione delle intrusioni (IPS) e altri dispositivi di sicurezza.

Per il traffico client non attendibile, si consiglia un bilanciamento del carico di terze parti. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.

Mitigazione ransomware

Proteggi i tuoi dati a oggetti dagli attacchi ransomware seguendo i consigli riportati nella "Difesa ransomware con StorageGRID".

Configurare StorageGRID per FabricPool

Configure StorageGRID for FabricPool: Panoramica

Se si utilizza il software NetApp ONTAP, è possibile utilizzare NetApp FabricPool per tierare i dati inattivi su un sistema di storage a oggetti NetApp StorageGRID.

Seguire queste istruzioni per:

- Scopri le considerazioni e le Best practice per la configurazione di StorageGRID per un carico di lavoro FabricPool.
- Scopri come configurare un sistema di storage a oggetti StorageGRID per l'utilizzo con FabricPool.

- Scopri come fornire i valori richiesti a ONTAP quando Aggiungi StorageGRID come Tier cloud FabricPool.

Guida rapida alla configurazione di StorageGRID per FabricPool

Pianificare la configurazione

- Decidere quale criterio di tiering dei volumi FabricPool utilizzare per eseguire il tiering dei dati ONTAP inattivi in StorageGRID.
- Pianificare e installare un sistema StorageGRID per soddisfare le esigenze di capacità e performance dello storage.
- Acquisire familiarità con il software di sistema StorageGRID, incluso "Grid Manager" e a. "Manager tenant".
- Esaminare le Best practice di FabricPool per "Gruppi HA", "bilanciamento del carico", "ILM", e. "di più".
- Consulta queste risorse aggiuntive, che forniscono dettagli sull'utilizzo e la configurazione di ONTAP e FabricPool:

  "TR-4598: Best practice FabricPool in ONTAP"

  "ONTAP 9: Panoramica sulla gestione dei Tier FabricPool con Gestione di sistema"

Eseguire attività preliminari

Ottenere il "Informazioni necessarie per collegare StorageGRID come Tier cloud", tra cui:

- Indirizzi IP
- Nomi di dominio
- Certificato SSL

Facoltativamente, configurare "federazione delle identità" e. "single sign-on".

Configurare le impostazioni StorageGRID

Utilizzare StorageGRID per ottenere i valori necessari a ONTAP per la connessione alla rete.

Utilizzando il "Installazione guidata di FabricPool" è il metodo consigliato e più rapido per configurare tutti gli elementi, ma è anche possibile configurare ogni entità manualmente, se necessario.

Configurare ONTAP e DNS

USA ONTAP per "aggiungi un tier cloud" Che utilizza i valori StorageGRID. Quindi, "Configurare le voci DNS" Per associare gli indirizzi IP ai nomi di dominio che si intende utilizzare.

Monitorare e gestire

Quando il sistema è in funzione, eseguire le attività in corso in ONTAP e StorageGRID per gestire e monitorare il tiering dei dati FabricPool nel tempo.

Che cos'è FabricPool?

FabricPool è una soluzione di storage ibrido ONTAP che utilizza un aggregato flash dalle performance elevate come Tier delle performance e un archivio di oggetti come Tier del cloud. L'utilizzo di aggregati abilitati per FabricPool consente di ridurre i costi dello storage senza compromettere performance, efficienza o protezione.

FabricPool associa un Tier cloud (un archivio di oggetti esterno, come StorageGRID) a un Tier locale (un aggregato di storage ONTAP) per creare una raccolta composita di dischi. I volumi all'interno di FabricPool possono quindi sfruttare il tiering mantenendo i dati attivi (hot) sullo storage ad alte performance (il Tier locale) e inattivando (cold) i tiering nell'archivio di oggetti esterno (il Tier cloud).

Non sono necessarie modifiche architetturali e puoi continuare a gestire i dati e l'ambiente applicativo dal sistema di storage centrale ONTAP.

Che cos'è StorageGRID?

NetApp StorageGRID è un'architettura di storage che gestisce i dati come oggetti, rispetto ad altre architetture di storage come lo storage a blocchi o file. Gli oggetti vengono conservati all'interno di un singolo contenitore (ad esempio un bucket) e non vengono nidificati come file all'interno di una directory all'interno di altre directory. Sebbene lo storage a oggetti offra generalmente performance inferiori rispetto allo storage a blocchi o a file, è notevolmente più scalabile. I bucket StorageGRID possono contenere petabyte di dati e miliardi di oggetti.

Perché utilizzare StorageGRID come Tier cloud FabricPool?

FabricPool può eseguire il tiering dei dati ONTAP a diversi provider di storage a oggetti, tra cui StorageGRID. A differenza dei cloud pubblici che potrebbero impostare un numero massimo di IOPS (Input/Output Operations per Second) supportati a livello di bucket o container, le performance di StorageGRID sono scalabili in base al numero di nodi in un sistema. L'utilizzo di StorageGRID come livello cloud FabricPool ti consente di conservare i tuoi dati nel tuo cloud privato per ottenere le massime performance e il controllo completo sui tuoi dati.

Inoltre, non è necessaria una licenza FabricPool quando si utilizza StorageGRID come livello cloud.

Informazioni necessarie per collegare StorageGRID come Tier cloud

Prima di poter collegare StorageGRID come livello cloud per FabricPool, è necessario eseguire i passaggi di configurazione in StorageGRID e ottenere determinati valori da utilizzare in ONTAP.

Di quali valori ho bisogno?

La seguente tabella mostra i valori da configurare in StorageGRID e il modo in cui tali valori vengono utilizzati da ONTAP e dal server DNS.

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Indirizzi IP virtuali (VIP)	StorageGRID > Gruppo ha	Voce DNS
Porta	StorageGRID > endpoint del bilanciamento del carico	Gestore di sistema ONTAP > Aggiungi livello cloud

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Certificato SSL	StorageGRID > endpoint del bilanciamento del carico	Gestore di sistema ONTAP > Aggiungi livello cloud
Nome server (FQDN)	StorageGRID > endpoint del bilanciamento del carico	Voce DNS
ID chiave di accesso e chiave di accesso segreta	StorageGRID > tenant e bucket	Gestore di sistema ONTAP > Aggiungi livello cloud
Nome bucket/container	StorageGRID > tenant e bucket	Gestore di sistema ONTAP > Aggiungi livello cloud

Come si ottengono questi valori?

In base alle proprie esigenze, è possibile effettuare una delle seguenti operazioni per ottenere le informazioni necessarie:

- Utilizzare "Installazione guidata di FabricPool". L'installazione guidata di FabricPool consente di configurare rapidamente i valori richiesti in StorageGRID e di creare un file da utilizzare per configurare Gestione di sistema di ONTAP. La procedura guidata guida l'utente attraverso i passaggi richiesti e aiuta a verificare che le impostazioni siano conformi alle Best practice di StorageGRID e FabricPool.
- Configurare ogni elemento manualmente. Quindi, immettere i valori in Gestore di sistema di ONTAP o nell'interfaccia utente di ONTAP. Attenersi alla seguente procedura:
  a. "Configurare un gruppo ad alta disponibilità (ha) per FabricPool".
  b. "Creare un endpoint di bilanciamento del carico per FabricPool".
  c. "Creare un account tenant per FabricPool".
  d. Accedere all'account tenant, quindi "creare il bucket e le chiavi di accesso per l'utente root".
  e. Creare una regola ILM per i dati FabricPool e aggiungerla ai criteri ILM attivi. Vedere "Configurare ILM per i dati FabricPool".
  f. Facoltativamente, "Creare una policy di classificazione del traffico per FabricPool".

Utilizzare l'installazione guidata di FabricPool

Utilizzare l'installazione guidata di FabricPool: Considerazioni e requisiti

È possibile utilizzare la configurazione guidata di FabricPool per configurare StorageGRID come sistema di storage a oggetti per un livello cloud FabricPool. Una volta completata l'installazione guidata, è possibile immettere i dettagli richiesti in Gestione sistema di ONTAP.

Quando utilizzare l'installazione guidata di FabricPool

L'installazione guidata di FabricPool guida l'utente in ogni fase della configurazione di StorageGRID per l'utilizzo con FabricPool e configura automaticamente determinate entità, come ad esempio ILM e i criteri di classificazione del traffico. Durante il completamento della procedura guidata, è possibile scaricare un file da utilizzare per immettere i valori in Gestione sistema di ONTAP. Utilizzare la procedura guidata per configurare il

sistema più rapidamente e per assicurarsi che le impostazioni siano conformi alle Best practice StorageGRID e FabricPool.

Se si dispone dell'autorizzazione di accesso root, è possibile completare l'installazione guidata di FabricPool quando si inizia a utilizzare Gestione griglia di StorageGRID oppure accedere e completare la procedura guidata in qualsiasi momento. A seconda dei requisiti, è possibile configurare manualmente alcuni o tutti gli elementi richiesti e quindi utilizzare la procedura guidata per assemblare i valori richiesti da ONTAP in un singolo file.

Utilizzare la procedura guidata di installazione di FabricPool, a meno che non si sappiano requisiti speciali o l'implementazione richieda una personalizzazione significativa.

Prima di utilizzare la procedura guidata

Confermare di aver completato questi passaggi dei prerequisiti.

Esaminare le Best practice

- Si dispone di una comprensione generale di "Informazioni necessarie per collegare StorageGRID come Tier cloud".
- Hai esaminato le Best practice di FabricPool per:
  - "Gruppi ad alta disponibilità (ha)"
  - "Bilanciamento del carico"
  - "Regole e policy ILM"

Ottenere gli indirizzi IP e configurare le interfacce VLAN

Se si configura un gruppo ha, si sa a quali nodi ONTAP si connetterà e a quale rete StorageGRID verrà utilizzata. Si conoscono anche i valori da inserire per la subnet CIDR, l'indirizzo IP del gateway e gli indirizzi IP virtuali (VIP).

Se si intende utilizzare una LAN virtuale per separare il traffico FabricPool, l'interfaccia VLAN è già stata configurata. Vedere "Configurare le interfacce VLAN".

Configurare la federazione di identità e SSO

Se si prevede di utilizzare la federazione di identità o il Single Sign-on (SSO) per il sistema StorageGRID, queste funzionalità sono state attivate. Si sa anche quale gruppo federato deve disporre dell'accesso root per l'account tenant che verrà utilizzato da ONTAP. Vedere "USA la federazione delle identità" e. "Configurare il single sign-on".

Ottenere e configurare i nomi di dominio

- Si conosce il nome di dominio completo (FQDN) da utilizzare per StorageGRID. Le voci DNS (Domain Name Server) associano questo FQDN agli indirizzi IP virtuali (VIP) del gruppo ha creato utilizzando la procedura guidata. Vedere "Configurare il server DNS".
- Se si prevede di utilizzare le richieste in stile host virtuale S3 "Nomi di dominio degli endpoint S3 configurati". Per impostazione predefinita, ONTAP utilizza URL di tipo path, ma si consiglia di utilizzare richieste virtuali di tipo hosted.

Esaminare i requisiti del bilanciamento del carico e del certificato di sicurezza

Se si intende utilizzare il bilanciamento del carico StorageGRID, è stato esaminato il generale "considerazioni per il bilanciamento del carico". Si dispone dei certificati da caricare o dei valori necessari per generare un certificato.

Se si intende utilizzare un endpoint esterno (di terze parti) per il bilanciamento del carico, si dispone del nome di dominio completo (FQDN), della porta e del certificato per il bilanciamento del carico.

Confermare la configurazione del pool di storage ILM

Se inizialmente è stato installato StorageGRID 11,6 o versione precedente, è stato configurato il pool di archiviazione che verrà utilizzato. In generale, è necessario creare un pool di storage per ogni sito StorageGRID che verrà utilizzato per memorizzare i dati ONTAP.

> Questo prerequisito non si applica se StorageGRID 11,7 o 11,8 è stato installato inizialmente. Quando si installa inizialmente una di queste versioni, vengono creati automaticamente pool di storage per ogni sito.

Relazione tra ONTAP e il livello cloud StorageGRID

La procedura guidata FabricPool ti guida nel processo di creazione di un singolo Tier cloud StorageGRID che include un tenant StorageGRID, un set di chiavi di accesso e un bucket StorageGRID. Puoi associare questo livello cloud StorageGRID a uno o più livelli locali ONTAP.

L'aggiunta di un singolo Tier cloud a più Tier locali in un cluster è la Best practice generale. Tuttavia, a seconda dei requisiti, è possibile utilizzare più di un bucket o anche più tenant StorageGRID per i Tier locali in un singolo cluster. L'utilizzo di diversi bucket e tenant consente di isolare l'accesso ai dati e ai dati tra i Tier locali di ONTAP, ma è piuttosto più complesso da configurare e gestire.

NetApp sconsiglia di collegare un singolo Tier cloud ai Tier locali in più cluster.

> Per le Best practice per l'utilizzo di StorageGRID con NetApp MetroCluster™ e FabricPool Mirror, vedere "TR-4598: Best practice FabricPool in ONTAP".

Opzionale: Utilizzare un bucket diverso per ciascun Tier locale

Per utilizzare più di un bucket per i Tier locali in un cluster ONTAP, aggiungere più di un Tier cloud StorageGRID in ONTAP. Ogni livello cloud condivide lo stesso gruppo ha, endpoint di bilanciamento del carico, tenant e chiavi di accesso, ma utilizza un container diverso (bucket StorageGRID). Attenersi alla seguente procedura generale:

1. Da Gestione griglia di StorageGRID, completare la configurazione guidata di FabricPool per il primo livello cloud.
2. Da Gestore di sistema di ONTAP, Aggiungi un livello cloud e utilizza il file scaricato da StorageGRID per fornire i valori richiesti.
3. Da StorageGRID tenant manager, accedere al tenant creato dalla procedura guidata e creare un secondo bucket.
4. Completare nuovamente la procedura guidata FabricPool. Selezionare il gruppo ha esistente, l'endpoint del bilanciamento del carico e il tenant. Quindi, selezionare il nuovo bucket creato manualmente. Creare una nuova regola ILM per il nuovo bucket e attivare un criterio ILM per includere tale regola.
5. Da ONTAP, Aggiungi un secondo Tier cloud ma fornisci il nuovo nome del bucket.

Facoltativo: Utilizzare un tenant e un bucket diversi per ciascun Tier locale

Per utilizzare più di un tenant e diversi set di chiavi di accesso per i Tier locali in un cluster ONTAP, aggiungere più di un Tier cloud StorageGRID in ONTAP. Ogni livello cloud condivide lo stesso gruppo ha, endpoint di bilanciamento del carico, ma utilizza un tenant, chiavi di accesso e container (bucket StorageGRID) diversi. Attenersi alla seguente procedura generale:

1. Da Gestione griglia di StorageGRID, completare la configurazione guidata di FabricPool per il primo livello cloud.
2. Da Gestore di sistema di ONTAP, Aggiungi un livello cloud e utilizza il file scaricato da StorageGRID per fornire i valori richiesti.
3. Completare nuovamente la procedura guidata FabricPool. Selezionare il gruppo ha esistente e l'endpoint del bilanciamento del carico. Crea un nuovo tenant e bucket. Creare una nuova regola ILM per il nuovo bucket e attivare un criterio ILM per includere tale regola.
4. Da ONTAP, Aggiungi un secondo livello cloud ma fornisci la nuova chiave di accesso, la chiave segreta e il nome del bucket.

Accedere e completare l'installazione guidata di FabricPool

È possibile utilizzare la configurazione guidata di FabricPool per configurare StorageGRID come sistema di storage a oggetti per un livello cloud FabricPool.

Prima di iniziare

- Hai esaminato il "considerazioni e requisiti" Per l'utilizzo dell'installazione guidata di FabricPool.

> Se si desidera configurare StorageGRID per l'utilizzo con qualsiasi altra applicazione client S3, visitare il sito Web "Utilizzare l'installazione guidata S3".

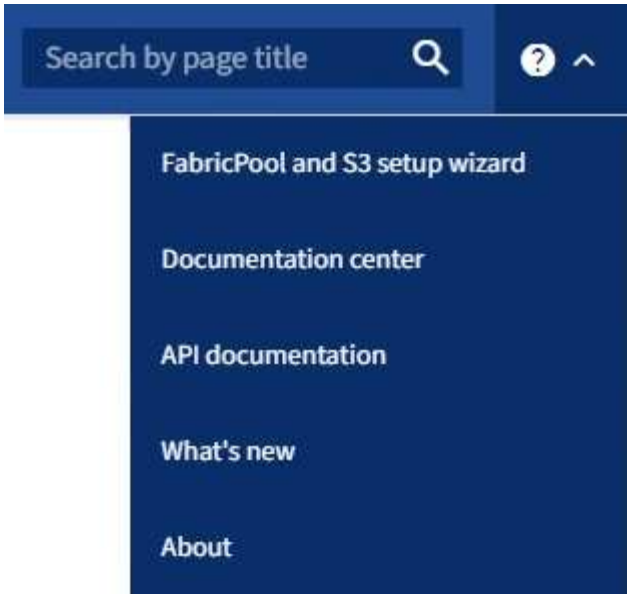
- Hai il "Autorizzazione di accesso root".

Accedere alla procedura guidata

È possibile completare l'installazione guidata di FabricPool quando si inizia a utilizzare Gestione griglia di StorageGRID oppure accedere e completare l'installazione guidata in qualsiasi momento.

Fasi

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Se nella dashboard viene visualizzato il banner **FabricPool and S3 setup wizard**, selezionare il link nel banner. Se il banner non viene più visualizzato, selezionare l'icona della guida dalla barra di intestazione in Gestione griglia e selezionare **Installazione guidata FabricPool and S3**.



3. Nella sezione FabricPool della pagina di installazione guidata di FabricPool e S3, selezionare **Configura ora**.

   Fase 1 di 9: Viene visualizzato il messaggio Configure ha group (Configura gruppo ha).

Fase 1 di 9: Configurazione del gruppo ha

Un gruppo ad alta disponibilità (ha) è un insieme di nodi che contengono ciascuno il servizio bilanciamento del carico StorageGRID. Un gruppo ha può contenere nodi gateway, nodi di amministrazione o entrambi.

È possibile utilizzare un gruppo ha per mantenere disponibili le connessioni dati FabricPool. Un gruppo ha utilizza indirizzi IP virtuali (VIP) per fornire un accesso altamente disponibile al servizio Load Balancer. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool

Per ulteriori informazioni su questa attività, vedere "Gestire i gruppi ad alta disponibilità" e. "Best practice per i gruppi ad alta disponibilità".

Fasi

1. Se si prevede di utilizzare un bilanciamento del carico esterno, non è necessario creare un gruppo ha. Selezionare **Ignora questo passaggio** e passare a. Fase 2 di 9: Configurare l'endpoint del bilanciamento del carico.
2. Per utilizzare il bilanciamento del carico StorageGRID, creare un nuovo gruppo ha o utilizzare un gruppo ha esistente.

Creare un gruppo ha

a. Per creare un nuovo gruppo ha, selezionare **Crea gruppo ha**.

b. Per la fase **inserire i dettagli**, completare i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome di visualizzazione univoco per questo gruppo ha.
Descrizione (opzionale)	La descrizione di questo gruppo ha.

c. Per il passo **Add interfaces**, selezionare le interfacce di nodo che si desidera utilizzare in questo gruppo ha.

   Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.

   È possibile selezionare uno o più nodi, ma è possibile selezionare una sola interfaccia per ciascun nodo.

d. Per la fase **prioritize interfaces**, determinare l'interfaccia primaria e le interfacce di backup per questo gruppo ha.

   Trascinare le righe per modificare i valori nella colonna **Ordine di priorità**.

   La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.

   Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi IP virtuali (VIP) si spostano nella 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. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

e. Per il passo **inserire gli indirizzi IP**, completare i seguenti campi.

Campo	Descrizione
Subnet CIDR	L'indirizzo della subnet VIP nella notazione CIDR& 8212;un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere bit host impostati. Ad esempio, `192.16.0.0/22`.
Indirizzo IP del gateway (opzionale)	Opzionale. Se gli indirizzi IP ONTAP utilizzati per accedere a StorageGRID non si trovano sulla stessa sottorete degli indirizzi VIP StorageGRID, immettere l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve trovarsi all'interno della subnet VIP.

Campo	Descrizione
Virtual IP address (Indirizzo IP virtuale)	Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP e tutti saranno attivi contemporaneamente sull'interfaccia attiva. Almeno un indirizzo deve essere IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

f. Selezionare **Crea gruppo ha**, quindi selezionare **fine** per tornare all'installazione guidata di FabricPool.

g. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Utilizzare il gruppo ha esistente

a. Per utilizzare un gruppo ha esistente, selezionare il nome del gruppo ha dall'elenco a discesa **Select an ha group** (Seleziona un gruppo ha).

b. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Fase 2 di 9: Configurare l'endpoint del bilanciamento del carico

StorageGRID utilizza un bilanciamento del carico per gestire il carico di lavoro dalle applicazioni client, come FabricPool. Il bilanciamento del carico massimizza la velocità e la capacità di connessione tra più nodi di storage.

È possibile utilizzare il servizio bilanciamento del carico StorageGRID, disponibile su tutti i nodi gateway e di amministrazione, oppure connettersi a un bilanciamento del carico esterno (di terze parti). Si consiglia di utilizzare il bilanciamento del carico StorageGRID.

Per ulteriori informazioni su questa attività, consultare la sezione generale "considerazioni per il bilanciamento del carico" e a. "Best practice per il bilanciamento del carico per FabricPool".

Fasi

1. Selezionare o creare un endpoint di bilanciamento del carico StorageGRID o utilizzare un bilanciamento del carico esterno.

Creare l'endpoint

a. Selezionare **Crea endpoint**.

b. Per il passo **inserire i dettagli dell'endpoint**, completare i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433 per il primo endpoint creato, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché queste porte sono riservate sui nodi Admin. **Nota:** le porte utilizzate da altri servizi di rete non sono consentite. Vedere "Riferimento porta di rete".
Tipo di client	Deve essere **S3**.
Protocollo di rete	Selezionare **HTTPS**. **Nota**: La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

c. Per il passo **Select binding mode**, specificare la modalità di binding. La modalità di associazione controlla l'accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (impostazione predefinita)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione **Global** (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.

Modalità	Descrizione
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

d. Per il passaggio **accesso tenant**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket. **Allow all tenant** è quasi sempre l'opzione appropriata per l'endpoint di bilanciamento del carico utilizzato per FabricPool. Selezionare questa opzione se si utilizza l'installazione guidata di FabricPool per un nuovo sistema StorageGRID e non sono stati ancora creati account tenant.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

e. Per il passo **Allega certificato**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Carica certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato dalla CA, una chiave privata del certificato e un bundle CA opzionale.
Generare un certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciamento del carico" per informazioni dettagliate su cosa inserire.
Utilizza il certificato StorageGRID S3 e Swift	Questa opzione è disponibile solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID. Vedere "Configurare i certificati API S3 e Swift" per ulteriori informazioni.

f. Selezionare **fine** per tornare all'installazione guidata di FabricPool.

g. Selezionare **continua** per passare al punto tenant e bucket.

Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Utilizzare l'endpoint del bilanciamento del carico esistente

a. Selezionare il nome di un endpoint esistente dall'elenco a discesa **Select a load balancer endpoint**.

b. Selezionare **continua** per passare al punto tenant e bucket.

Utilizzare un bilanciamento del carico esterno

a. Completare i seguenti campi per il bilanciamento del carico esterno.

Campo	Descrizione
FQDN	Il nome di dominio completo (FQDN) del bilanciamento del carico esterno.
Porta	Il numero di porta che FabricPool utilizzerà per connettersi al bilanciamento del carico esterno.
Certificato	Copiare il certificato del server per il bilanciamento del carico esterno e incollarlo in questo campo.

b. Selezionare **continua** per passare al punto tenant e bucket.

Fase 3 di 9: Tenant e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per memorizzare e recuperare oggetti in StorageGRID. Ogni tenant dispone di utenti, chiavi di accesso, bucket, oggetti e un set specifico di funzionalità. È necessario creare un tenant StorageGRID prima di poter creare il bucket che FabricPool utilizzerà.

Un bucket è un container utilizzato per memorizzare gli oggetti e i metadati degli oggetti di un tenant. Anche se alcuni tenant potrebbero avere molti bucket, la procedura guidata consente di creare o selezionare solo un tenant e un bucket alla volta. Puoi utilizzare il tenant Manager in un secondo momento per aggiungere altri bucket necessari.

È possibile creare un nuovo tenant e bucket per l'utilizzo di FabricPool oppure selezionare un tenant e un bucket esistenti. Se si crea un nuovo tenant, il sistema crea automaticamente l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root del tenant.

Per ulteriori informazioni su questa attività, vedere "Creare un account tenant per FabricPool" e. "Creare un bucket S3 e ottenere una chiave di accesso".

Fasi

Creare un nuovo tenant e bucket o selezionare un tenant esistente.

Nuovo tenant e bucket

1. Per creare un nuovo tenant e bucket, immettere un **Nome tenant**. Ad esempio, `FabricPool tenant`.
2. Definire l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del sistema StorageGRID "federazione delle identità", "SSO (Single Sign-on)", o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

3. Per **Nome bucket**, immettere il nome del bucket che verrà utilizzato da FabricPool per memorizzare i dati ONTAP. Ad esempio, `fabricpool-bucket`.

   Non è possibile modificare il nome del bucket dopo averlo creato.

4. Selezionare **Region** per questo bucket.

   Utilizzare la regione predefinita (`us-east-1`) A meno che non si preveda di utilizzare ILM in futuro per filtrare gli oggetti in base all'area del bucket.

5. Selezionare **Create and continue** (Crea e continua) per creare il tenant e il bucket e passare alla fase di download dei dati

Selezionare tenant e bucket

L'account tenant esistente deve disporre di almeno un bucket che non ha attivato il controllo delle versioni. Non puoi selezionare un account tenant esistente se non esiste un bucket per quel tenant.

1. Selezionare il tenant esistente dall'elenco a discesa **Nome tenant**.
2. Selezionare il bucket esistente dall'elenco a discesa **Nome bucket**.

   FabricPool non supporta il controllo delle versioni degli oggetti, pertanto i bucket con la versione attivata non vengono visualizzati.

   Non selezionare un bucket con blocco oggetti S3 abilitato per l'utilizzo con FabricPool.

3. Selezionare **continua** per passare alla fase di download dei dati.

Fase 4 di 9: Download delle impostazioni ONTAP

Durante questa fase, è possibile scaricare un file da utilizzare per immettere i valori in Gestione di sistema di ONTAP.

Fasi

1. In alternativa, selezionare l'icona di copia ( ) Per copiare sia l'ID della chiave di accesso che la chiave di accesso segreta negli Appunti.

   Questi valori sono inclusi nel file di download, ma è possibile salvarli separatamente.

2. Selezionare **Scarica impostazioni ONTAP** per scaricare un file di testo contenente i valori immessi finora.

   Il `ONTAP_FabricPool_settings_bucketname.txt` Il file include le informazioni necessarie per configurare StorageGRID come sistema di storage a oggetti per un livello cloud FabricPool, tra cui:

   - Dettagli sulla connessione del bilanciamento del carico, inclusi nome del server (FQDN), porta e certificato
   - Nome bucket
   - ID della chiave di accesso e chiave di accesso segreta per l'utente root dell'account tenant

3. Salvare le chiavi copiate e il file scaricato in una posizione sicura.

   > Non chiudere questa pagina fino a quando non sono stati copiati entrambi i tasti di accesso, scaricati le impostazioni ONTAP o entrambi. I tasti non saranno disponibili dopo la chiusura di questa pagina. Assicurarsi di salvare queste informazioni in una posizione sicura perché possono essere utilizzate per ottenere dati dal sistema StorageGRID.

4. Selezionare la casella di controllo per confermare di aver scaricato o copiato l'ID della chiave di accesso e la chiave di accesso segreta.
5. Selezionare **continua** per passare alla fase del pool di storage ILM.

Fase 5 di 9: Selezionare un pool di storage

Un pool di storage è un gruppo di nodi di storage. Quando si seleziona un pool di storage, si determinano i nodi che StorageGRID utilizzerà per memorizzare i dati a più livelli da ONTAP.

Per ulteriori informazioni su questo passaggio, vedere "Creare un pool di storage".

Fasi

1. Dall'elenco a discesa **Sito**, selezionare il sito StorageGRID che si desidera utilizzare per i dati a più livelli di ONTAP.
2. Dall'elenco a discesa **Storage pool**, selezionare il pool di storage per il sito.

   Il pool di storage di un sito include tutti i nodi di storage di quel sito.

3. Selezionare **continua** per passare al passo della regola ILM.

Fase 6 di 9: Esaminare la regola ILM per FabricPool

Le regole ILM (Information Lifecycle Management) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel sistema StorageGRID.

L'installazione guidata di FabricPool crea automaticamente la regola ILM consigliata per l'utilizzo di FabricPool. Questa regola si applica solo al bucket specificato. Utilizza la codifica di cancellazione 2+1 in un singolo sito per memorizzare i dati a più livelli da ONTAP.

Per ulteriori informazioni su questo passaggio, vedere "Creare una regola ILM" e. "Best practice per l'utilizzo di ILM con i dati FabricPool".

Fasi

1. Esaminare i dettagli della regola.

Campo	Descrizione
Nome della regola	Generato automaticamente e non modificabile
Descrizione	Generato automaticamente e non modificabile
Filtro	Il nome del bucket Questa regola si applica solo agli oggetti salvati nel bucket specificato.
Tempo di riferimento	Tempo di acquisizione L'istruzione di posizionamento inizia quando gli oggetti vengono inizialmente salvati nel bucket.
Istruzioni per il posizionamento	USA erasure coding 2+1

2. Ordinare il diagramma di conservazione per **periodo di tempo** e **pool di storage** per confermare le istruzioni di posizionamento.
   - Il **periodo di tempo** per la regola è **giorno 0 - per sempre**. **Giorno 0** indica che la regola viene applicata quando i dati vengono sottoposti a tiering da ONTAP. **Per sempre** significa che ILM di StorageGRID non eliminerà i dati a più livelli da ONTAP.
   - Il **Storage pool** per la regola è il pool di storage selezionato. **EC 2+1** indica che i dati verranno memorizzati utilizzando la codifica di cancellazione 2+1. Ogni oggetto verrà salvato come due frammenti di dati e un frammento di parità. I tre frammenti per ciascun oggetto verranno salvati in diversi nodi di storage in un singolo sito.
3. Selezionare **Create and continue** (Crea e continua) per creare questa regola e passare al passaggio del criterio ILM.

Fase 7 di 9: Esaminare e attivare il criterio ILM

Una volta creata la regola ILM per l'utilizzo di FabricPool, la procedura guidata di installazione di FabricPool crea un criterio ILM. È necessario simulare e rivedere attentamente questo criterio prima di attivarlo.

Per ulteriori informazioni su questo passaggio, vedere "Creare un criterio ILM" e. "Best practice per l'utilizzo di ILM con i dati FabricPool".

Quando si attiva un nuovo criterio ILM, StorageGRID utilizza tale criterio per gestire il posizionamento, la durata e la protezione dei dati di tutti gli oggetti nella griglia, inclusi gli oggetti esistenti e quelli appena acquisiti. In alcuni casi, l'attivazione di un nuovo criterio può causare lo spostamento degli oggetti esistenti in nuove posizioni.

Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool. Impostare il periodo di conservazione su **forever** per garantire che gli oggetti FabricPool non vengano cancellati da ILM StorageGRID.

Fasi

1. Facoltativamente, aggiornare il nome * Policy* generato dal sistema. Per impostazione predefinita, il sistema aggiunge "+ FabricPool" al nome del criterio attivo o inattivo, ma è possibile fornire il proprio nome.
2. Esaminare l'elenco di regole nel criterio inattivo.
   - Se la griglia non dispone di un criterio ILM inattivo, la procedura guidata crea un criterio inattivo clonando il criterio attivo e aggiungendo la nuova regola all'inizio.
   - Se la griglia dispone già di un criterio ILM inattivo e tale criterio utilizza le stesse regole e lo stesso ordine del criterio ILM attivo, la procedura guidata aggiunge la nuova regola all'inizio del criterio inattivo.
   - Se il criterio inattivo contiene regole diverse o un ordine diverso da quello attivo, la procedura guidata crea un nuovo criterio inattivo clonando il criterio attivo e aggiungendo la nuova regola all'inizio.
3. Controllare l'ordine delle regole nel nuovo criterio inattivo.

   Poiché la regola FabricPool è la prima regola, tutti gli oggetti nel bucket FabricPool vengono posizionati prima della valutazione delle altre regole del criterio. Gli oggetti in qualsiasi altro bucket vengono posizionati in base alle regole successive del criterio.

4. Consulta il diagramma di conservazione per scoprire come conservare i diversi oggetti.
   a. Selezionare **Espandi tutto** per visualizzare un diagramma di conservazione per ciascuna regola nel criterio inattivo.
   b. Selezionare **periodo di tempo** e **pool di storage** per rivedere il diagramma di conservazione. Confermare che le regole applicabili al bucket FabricPool o al tenant conservino gli oggetti **per sempre**.
5. Dopo aver esaminato il criterio inattivo, selezionare **attiva e continua** per attivare il criterio e passare alla fase di classificazione del traffico.

Gli errori in una policy ILM possono causare una perdita di dati irreparabile. Esaminare attentamente la policy prima di attivarla.

Fase 8 di 9: Creazione di criteri di classificazione del traffico

Come opzione, la configurazione guidata di FabricPool può creare una policy di classificazione del traffico che è possibile utilizzare per monitorare il carico di lavoro di FabricPool. La policy creata dal sistema utilizza una regola di corrispondenza per identificare tutto il traffico di rete correlato al bucket creato. Questo criterio monitora solo il traffico e non limita il traffico per FabricPool o altri client.

Per ulteriori informazioni su questo passaggio, vedere "Creare una policy di classificazione del traffico per FabricPool".

Fasi

1. Esaminare la policy.
2. Se si desidera creare questa policy di classificazione del traffico, selezionare **Crea e continua**.

   Non appena FabricPool inizia a tiering dei dati su StorageGRID, puoi accedere alla pagina delle policy di classificazione del traffico per visualizzare le metriche del traffico di rete per questa policy. In seguito, è possibile aggiungere regole per limitare altri carichi di lavoro e garantire che il carico di lavoro FabricPool abbia la maggior parte della larghezza di banda.

3. In caso contrario, selezionare **Ignora questo passaggio**.

Fase 9 di 9: Riepilogo

Il riepilogo fornisce dettagli sugli elementi configurati, tra cui il nome del bilanciamento del carico, del tenant e del bucket, la policy di classificazione del traffico e la policy ILM attiva,

Fasi

1. Esaminare il riepilogo.
2. Selezionare **fine**.

Passi successivi

Dopo aver completato la procedura guidata FabricPool, eseguire questi passaggi aggiuntivi.

Fasi

1. Passare a. "Configurare Gestore di sistema di ONTAP" Per inserire i valori salvati e completare il lato ONTAP della connessione. È necessario aggiungere StorageGRID come livello cloud, collegare il livello cloud a un livello locale per creare un FabricPool e impostare le policy di tiering dei volumi.
2. Passare a. "Configurare il server DNS" E assicurarsi che il DNS includa un record per associare il nome del server StorageGRID (nome di dominio completo) a ciascun indirizzo IP StorageGRID che si intende utilizzare.
3. Passare a. "Altre Best practice per StorageGRID e FabricPool" Per apprendere le Best practice per i registri di controllo di StorageGRID e altre opzioni di configurazione globali.

Configurare StorageGRID manualmente

Creare un gruppo ad alta disponibilità (ha) per FabricPool

Quando si configura StorageGRID per l'utilizzo con FabricPool, è possibile creare facoltativamente uno o più gruppi ad alta disponibilità (ha).
Un gruppo ha è un insieme di nodi che contengono ciascuno il servizio bilanciamento del carico StorageGRID. Un gruppo ha può contenere nodi gateway, nodi di amministrazione o entrambi.

È possibile utilizzare un gruppo ha per mantenere disponibili le connessioni dati FabricPool. Un gruppo ha utilizza indirizzi IP virtuali (VIP) per fornire un accesso altamente disponibile al servizio Load Balancer. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool.

Per ulteriori informazioni su questa attività, vedere "Gestire i gruppi ad alta disponibilità". Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- Hai esaminato il "best practice per i gruppi ad alta disponibilità".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Se si intende utilizzare una VLAN, è stata creata l'interfaccia VLAN. Vedere "Configurare le interfacce VLAN".

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.
2. Selezionare **Crea**.
3. Per la fase **inserire i dettagli**, completare i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome di visualizzazione univoco per questo gruppo ha.
Descrizione (opzionale)	La descrizione di questo gruppo ha.

4. Per il passo **Add interfaces**, selezionare le interfacce di nodo che si desidera utilizzare in questo gruppo ha.

   Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.

   È possibile selezionare uno o più nodi, ma è possibile selezionare una sola interfaccia per ciascun nodo.

5. Per la fase **prioritize interfaces**, determinare l'interfaccia primaria e le interfacce di backup per questo gruppo ha.

   Trascinare le righe per modificare i valori nella colonna **Ordine di priorità**.

   La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.

   Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi IP virtuali (VIP) si spostano nella 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. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

6. Per il passo **inserire gli indirizzi IP**, completare i seguenti campi.

Campo	Descrizione
Subnet CIDR	L'indirizzo della subnet VIP nella notazione CIDR& 8212;un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere bit host impostati. Ad esempio, `192.16.0.0/22`.

Campo	Descrizione
Indirizzo IP del gateway (opzionale)	Opzionale. Se gli indirizzi IP ONTAP utilizzati per accedere a StorageGRID non si trovano sulla stessa sottorete degli indirizzi VIP StorageGRID, immettere l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve trovarsi all'interno della subnet VIP.
Virtual IP address (Indirizzo IP virtuale)	Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP. Almeno un indirizzo deve essere IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

7. Selezionare **Create ha group** (Crea gruppo ha), quindi selezionare **Finish** (fine).

Creare un endpoint di bilanciamento del carico per FabricPool

StorageGRID utilizza un bilanciamento del carico per gestire il carico di lavoro dalle applicazioni client, come FabricPool. Il bilanciamento del carico massimizza la velocità e la capacità di connessione tra più nodi di storage.

Quando si configura StorageGRID per l'utilizzo con FabricPool, è necessario configurare un endpoint di bilanciamento del carico e caricare o generare un certificato endpoint di bilanciamento del carico, utilizzato per proteggere la connessione tra ONTAP e StorageGRID.

Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Hai esaminato il generale "considerazioni per il bilanciamento del carico" così come il "Best practice per il bilanciamento del carico per FabricPool".

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
2. Selezionare **Crea**.
3. Per il passo **inserire i dettagli dell'endpoint**, completare i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.

Campo	Descrizione
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433 per il primo endpoint creato, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione. **Nota:** le porte utilizzate da altri servizi di rete non sono consentite. Vedere "Riferimento porta di rete". Fornirai questo numero a ONTAP quando Aggiungi StorageGRID come Tier cloud FabricPool.
Tipo di client	Selezionare **S3**.
Protocollo di rete	Selezionare **HTTPS**. **Nota**: La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

4. Per il passo **Select binding mode**, specificare la modalità di binding. La modalità di associazione controlla l'accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (impostazione predefinita)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione **Global** (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

5. Per il passaggio **accesso tenant**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket. **Allow all tenant** è quasi sempre l'opzione appropriata per l'endpoint di bilanciamento del carico utilizzato per FabricPool. Selezionare questa opzione se non sono ancora stati creati account tenant.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

6. Per il passo **Allega certificato**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Carica certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato dalla CA, una chiave privata del certificato e un bundle CA opzionale.
Generare un certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciamento del carico" per informazioni dettagliate su cosa inserire.
Utilizza il certificato StorageGRID S3 e Swift	Questa opzione è disponibile solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID. Vedere "Configurare i certificati API S3 e Swift" per ulteriori informazioni.

7. Selezionare **Crea**.

> Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Creare un account tenant per FabricPool

È necessario creare un account tenant in Grid Manager per l'utilizzo con FabricPool.

Gli account tenant consentono alle applicazioni client di memorizzare e recuperare oggetti su StorageGRID. Ogni account tenant dispone di un proprio ID account, gruppi e utenti autorizzati, bucket e oggetti.

Per ulteriori informazioni su questa attività, vedere "Creare un account tenant". Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **TENANT**.
2. Selezionare **Crea**.
3. Per la procedura di inserimento dei dettagli, immettere le seguenti informazioni.

Campo	Descrizione
Nome	Un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Una volta creato, l'account tenant riceve un ID account numerico univoco.
Descrizione (opzionale)	Una descrizione che aiuta a identificare il tenant.
Tipo di client	Deve essere **S3** per FabricPool.
Quota di storage (opzionale)	Lasciare vuoto questo campo per FabricPool.

4. Per il passo Select permissions:
   a. Non selezionare **Allow platform Services** (Consenti servizi piattaforma).

      I tenant FabricPool non devono in genere utilizzare servizi di piattaforma, come la replica di CloudMirror.

   b. Facoltativamente, selezionare **Usa origine identità propria**.
   c. Non selezionare **Allow S3 Select** (Consenti selezione S3).

      I tenant FabricPool in genere non devono utilizzare S3 Select.

   d. Facoltativamente, selezionare **Usa connessione federazione griglia** per consentire al tenant di utilizzare un "connessione a federazione di griglie" per il clone dell'account e la replica cross-grid. Quindi, selezionare la connessione a federazione di griglie da utilizzare.
5. Per la fase di definizione dell'accesso root, specificare quale utente disporrà dell'autorizzazione di accesso root iniziale per l'account tenant, a seconda che il sistema StorageGRID utilizzi o meno "federazione delle identità", "SSO (Single Sign-on)", o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.

Opzione	Eseguire questa operazione
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

6. Selezionare **Crea tenant**.

Creare un bucket S3 e ottenere le chiavi di accesso

Prima di utilizzare StorageGRID con un carico di lavoro FabricPool, è necessario creare un bucket S3 per i dati FabricPool. È inoltre necessario ottenere una chiave di accesso e una chiave di accesso segreta per l'account tenant che si utilizzerà per FabricPool.

Per ulteriori informazioni su questa attività, vedere "Creare un bucket S3" e. "Creare le proprie chiavi di accesso S3". Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- È stato creato un account tenant per l'utilizzo di FabricPool.
- Si dispone dell'accesso root all'account tenant.

Fasi

1. Accedi al tenant manager.

   È possibile effettuare una delle seguenti operazioni:

   - Dalla pagina account tenant in Grid Manager, selezionare il collegamento **Accedi** per il tenant e immettere le credenziali.
   - Immettere l'URL dell'account tenant in un browser Web e le credenziali.

2. Creare un bucket S3 per i dati FabricPool.

   È necessario creare un bucket unico per ogni cluster ONTAP che si intende utilizzare.

   a. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
   b. Selezionare **Crea bucket**.
   c. Immettere il nome del bucket StorageGRID che si desidera utilizzare con FabricPool. Ad esempio, `fabricpool-bucket`.

      Non è possibile modificare il nome del bucket dopo averlo creato.

   d. Selezionare la regione per questo bucket.

      Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione.

   e. Selezionare **continua**.
   f. Selezionare **Crea bucket**.

Non selezionare **attiva versione oggetto** per il bucket FabricPool. Allo stesso modo, non modificare un bucket FabricPool per utilizzare **available** o una coerenza non predefinita. La coerenza bucket consigliata per i bucket FabricPool è **Read-after-new-write**, che è la coerenza predefinita per un nuovo bucket.

3. Creare una chiave di accesso e una chiave di accesso segreta.

   a. Selezionare **STORAGE (S3)** > **My access key**.

   b. Selezionare **Crea chiave**.

   c. Selezionare **Crea chiave di accesso**.

   d. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

      Questi valori verranno immessi in ONTAP quando si configura StorageGRID come livello cloud FabricPool.

Se in futuro si generano una nuova chiave di accesso e una chiave di accesso segreta in StorageGRID, inserire le nuove chiavi in ONTAP prima di eliminare i vecchi valori da StorageGRID. In caso contrario, ONTAP potrebbe perdere temporaneamente l'accesso a StorageGRID.

Configurare ILM per i dati FabricPool

Puoi utilizzare questo semplice esempio di policy come punto di partenza per le tue regole e policy ILM.

In questo esempio si presuppone che si stiano progettando le regole ILM e una policy ILM per un sistema StorageGRID con quattro nodi di storage in un singolo data center a Denver, Colorado. I dati FabricPool in questo esempio utilizzano un bucket denominato `fabricpool-bucket`.

Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita. Per ulteriori informazioni, vedere "Gestire gli oggetti con ILM".

Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool. Impostare il periodo di conservazione su **forever** per garantire che gli oggetti FabricPool non vengano cancellati da ILM StorageGRID.

Prima di iniziare

- Hai esaminato il "Best practice per l'utilizzo di ILM con i dati FabricPool".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso a ILM o Root".
- Se è stato eseguito l'upgrade a StorageGRID 11,8 da una versione precedente di StorageGRID, è stato configurato il pool di storage che verrà utilizzato. In generale, è necessario creare un pool di storage per ogni sito StorageGRID da utilizzare per archiviare i dati.

Questo prerequisito non si applica se StorageGRID 11,7 o 11,8 è stato installato inizialmente. Quando si installa inizialmente una di queste versioni, vengono creati automaticamente pool di storage per ogni sito.

Fasi

1. Creare una regola ILM che si applica solo ai dati in `fabricpool-bucket`. Questa regola di esempio consente di creare copie codificate per la cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	2 + 1 erasure coding per i dati FabricPool
Nome bucket	`fabricpool-bucket` È anche possibile filtrare l'account tenant FabricPool.
Filtri avanzati	Dimensione dell'oggetto superiore a 0.2 MB. **Nota:** FabricPool scrive solo oggetti da 4 MB, ma è necessario aggiungere un filtro per le dimensioni degli oggetti perché questa regola utilizza la codifica di cancellazione.
Tempo di riferimento	Tempo di acquisizione
Periodo di tempo e collocamenti	Dal giorno 0 memorizzare per sempre Memorizzare gli oggetti cancellando il codice utilizzando lo schema 2+1 EC a Denver e conservarli in StorageGRID per sempre. Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool.
Comportamento di acquisizione	Bilanciato

2. Creare una regola ILM predefinita che crei due copie replicate di qualsiasi oggetto non corrispondente alla prima regola. Non selezionare un filtro di base (account tenant o nome bucket) o filtri avanzati.

Definizione della regola	Valore di esempio
Nome della regola	Due copie replicate
Nome bucket	*nessuno*
Filtri avanzati	*nessuno*
Tempo di riferimento	Tempo di acquisizione

Definizione della regola	Valore di esempio
Periodo di tempo e collocamenti	Dal giorno 0 memorizzare per sempre Memorizzare gli oggetti replicando 2 copie a Denver.
Comportamento di acquisizione	Bilanciato

3. Creare un criterio ILM e selezionare le due regole. Poiché la regola di replica non utilizza alcun filtro, può essere l'ultima regola predefinita per il criterio.
4. Acquisire oggetti di test nella griglia.
5. Simulare il criterio con gli oggetti di test per verificare il comportamento.
6. Attivare il criterio.

Quando questo criterio è attivato, StorageGRID inserisce i dati degli oggetti come segue:

- I dati a più livelli di FabricPool in `fabricpool-bucket` verrà sottoposto a erasure coding utilizzando lo schema di erasure coding 2+1. Due frammenti di dati e un frammento di parità verranno posizionati su tre diversi nodi di storage.
- Tutti gli oggetti in tutti gli altri bucket verranno replicati. Verranno create due copie e collocate su due diversi nodi di storage.
- Le copie verranno conservate in StorageGRID per sempre. ILM di StorageGRID non elimina questi oggetti.

Creare una policy di classificazione del traffico per FabricPool

È possibile, in via opzionale, progettare una policy di classificazione del traffico StorageGRID per ottimizzare la qualità del servizio per il carico di lavoro FabricPool.

Per ulteriori informazioni su questa attività, vedere "Gestire le policy di classificazione del traffico". Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

Le Best practice per la creazione di una policy di classificazione del traffico per FabricPool dipendono dal carico di lavoro, come segue:

- Se si prevede di suddividere i dati del carico di lavoro primario FabricPool in StorageGRID, assicurarsi che il carico di lavoro FabricPool abbia la maggior parte della larghezza di banda. È possibile creare una policy di classificazione del traffico per limitare tutti gli altri carichi di lavoro.

  > In generale, le operazioni di lettura FabricPool sono più importanti per le priorità rispetto alle operazioni di scrittura.

  Ad esempio, se altri client S3 utilizzano questo sistema StorageGRID, è necessario creare un criterio di classificazione del traffico. È possibile limitare il traffico di rete per gli altri bucket, tenant, subnet IP o

endpoint del bilanciamento del carico.

*In genere, non è necessario imporre limiti di qualità del servizio su qualsiasi carico di lavoro FabricPool; è necessario limitare solo gli altri carichi di lavoro.

- I limiti imposti agli altri carichi di lavoro devono tenere conto del comportamento di tali carichi di lavoro. I limiti imposti variano anche in base al dimensionamento e alle funzionalità del tuo grid e alla quantità di utilizzo prevista.

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.
2. Selezionare **Crea**.
3. Inserire un nome e una descrizione (opzionale) per la policy e selezionare **continua**.
4. Per il passo Add Matching rules (Aggiungi regole di corrispondenza), aggiungere almeno una regola.
   a. Selezionare **Aggiungi regola**
   b. Per tipo, selezionare **endpoint del bilanciamento del carico** e selezionare l'endpoint del bilanciamento del carico creato per FabricPool.

      È inoltre possibile selezionare l'account o il bucket del tenant FabricPool.

   c. Se si desidera che questo criterio di traffico limiti il traffico per gli altri endpoint, selezionare **corrispondenza inversa**.
5. Facoltativamente, aggiungere uno o più limiti per controllare il traffico di rete corrispondente alla regola.

   StorageGRID raccoglie le metriche anche se non si aggiungono limiti, in modo da poter comprendere le tendenze del traffico.

   a. Selezionare **Aggiungi un limite**.
   b. Selezionare il tipo di traffico che si desidera limitare e il limite da applicare.
6. Selezionare **continua**.
7. Leggere e rivedere la policy di classificazione del traffico. Utilizzare il pulsante **precedente** per tornare indietro e apportare le modifiche necessarie. Quando si è soddisfatti della policy, selezionare **Salva e continua**.

Dopo il completamento

"Visualizzare le metriche del traffico di rete" per verificare che i criteri stiano applicando i limiti di traffico previsti.

Configurare Gestore di sistema di ONTAP

Dopo aver ottenuto le informazioni StorageGRID richieste, puoi accedere a ONTAP per aggiungere StorageGRID come livello cloud.

Prima di iniziare

- Una volta completata l'installazione guidata di FabricPool, si dispone di `ONTAP_FabricPool_settings_bucketname.txt` file scaricato.
- Se StorageGRID è stato configurato manualmente, si dispone del nome di dominio completo (FQDN) utilizzato per StorageGRID o dell'indirizzo IP virtuale (VIP) per il gruppo StorageGRID ha, del numero di

porta per l'endpoint del bilanciamento del carico, del certificato del bilanciamento del carico, L'ID della chiave di accesso e la chiave segreta per l'utente root dell'account tenant e il nome del bucket ONTAP utilizzato in tale tenant.

Accedere a Gestore di sistema di ONTAP

Queste istruzioni descrivono come utilizzare Gestione di sistema di ONTAP per aggiungere StorageGRID come livello cloud. È possibile completare la stessa configurazione utilizzando l'interfaccia utente di ONTAP. Per istruzioni, visitare il sito Web all'indirizzo "ONTAP 9: Gestione dei livelli FabricPool con l'interfaccia CLI".

Fasi

1. Accedere a Gestore di sistema per il cluster ONTAP che si desidera raggruppare in StorageGRID.
2. Accedere come amministratore del cluster.
3. Accedere a **STORAGE** > **Tier** > **Add Cloud Tier**.
4. Selezionare **StorageGRID** dall'elenco dei provider di archivi di oggetti.

Inserire i valori StorageGRID

Vedere "ONTAP 9: Panoramica sulla gestione dei Tier FabricPool con Gestione di sistema" per ulteriori informazioni.

Fasi

1. Completare il modulo Add Cloud Tier utilizzando `ONTAP_FabricPool_settings_`*`bucketname`*`.txt` o i valori ottenuti manualmente.

Campo	Descrizione
Nome	Immettere un nome univoco per questo livello cloud. È possibile accettare il valore predefinito.
Stile URL	Se "Nomi di dominio degli endpoint S3 configurati", Selezionare **Virtual Hosted-style URL**. **URL stile percorso** è l'impostazione predefinita per ONTAP, ma per StorageGRID si consiglia di utilizzare richieste virtuali in stile host. È necessario utilizzare **URL stile percorso** se si fornisce un indirizzo IP invece di un nome di dominio per il campo **Nome server (FQDN)**.
Nome server (FQDN)	Immettere il nome di dominio completo (FQDN) utilizzato per StorageGRID o l'indirizzo IP virtuale (VIP) per il gruppo StorageGRID ha. Ad esempio, `s3.storagegrid.`*`company`*`.com`. Tenere presente quanto segue: • L'indirizzo IP o il nome di dominio specificato deve corrispondere al certificato caricato o generato per l'endpoint del bilanciamento del carico di StorageGRID. • Se si fornisce un nome di dominio, il record DNS deve essere associato a ciascun indirizzo IP utilizzato per la connessione a StorageGRID. Vedere "Configurare il server DNS".

Campo	Descrizione
SSL	Enabled (attivato) (impostazione predefinita).
Certificato dell'archivio di oggetti	Incollare il PEM del certificato utilizzato per l'endpoint del bilanciamento del carico di StorageGRID, tra cui: `-----BEGIN CERTIFICATE-----` e. `-----END CERTIFICATE-----`. **Nota:** se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.
Porta	Inserire la porta utilizzata dall'endpoint del bilanciamento del carico StorageGRID. ONTAP utilizzerà questa porta quando si connette a StorageGRID. Ad esempio, 10433.
Chiave di accesso e chiave segreta	Immettere l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root dell'account tenant StorageGRID. **Suggerimento**: Se in futuro si generano una nuova chiave di accesso e una chiave di accesso segreta in StorageGRID, inserire le nuove chiavi in ONTAP prima di eliminare i vecchi valori da StorageGRID. In caso contrario, ONTAP potrebbe perdere temporaneamente l'accesso a StorageGRID.
Nome del container	Immettere il nome del bucket StorageGRID creato per l'utilizzo con questo Tier ONTAP.

2. Completare la configurazione finale di FabricPool in ONTAP.
   a. Collegare uno o più aggregati al livello cloud.
   b. Facoltativamente, creare una policy di tiering dei volumi.

Configurare il server DNS

Dopo aver configurato i gruppi ad alta disponibilità, gli endpoint del bilanciamento del carico e i nomi di dominio degli endpoint S3, è necessario assicurarsi che il DNS includa le voci necessarie per StorageGRID. È necessario includere una voce DNS per ciascun nome nel certificato di protezione e per ogni indirizzo IP che si potrebbe utilizzare.

Vedere "Considerazioni per il bilanciamento del carico".

Voci DNS per il nome del server StorageGRID

Aggiungere voci DNS per associare il nome del server StorageGRID (nome di dominio completo) a ciascun indirizzo IP StorageGRID che si intende utilizzare.
Gli indirizzi IP immessi nel DNS dipendono dall'utilizzo di un gruppo ha di nodi per il bilanciamento del carico:

- Se è stato configurato un gruppo ha, ONTAP si connetterà agli indirizzi IP virtuali di tale gruppo ha.
- Se non si utilizza un gruppo ha, ONTAP può connettersi al servizio bilanciamento del carico StorageGRID

utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore.

- Se il nome del server viene risolto in più indirizzi IP, ONTAP stabilisce le connessioni client con tutti gli indirizzi IP (fino a un massimo di 16 indirizzi IP). Gli indirizzi IP vengono raccolti con un metodo round-robin quando vengono stabilite le connessioni.

Voci DNS per richieste virtuali in stile host

Se è stato definito "Nomi di dominio degli endpoint S3" Inoltre, verranno utilizzate le richieste virtuali in stile host, verranno aggiunte voci DNS per tutti i nomi di dominio degli endpoint S3 richiesti, inclusi i nomi con caratteri jolly.

Best practice StorageGRID per FabricPool

Best practice per i gruppi ad alta disponibilità (ha)

Prima di associare StorageGRID come livello cloud FabricPool, scopri i gruppi ad alta disponibilità (ha) di StorageGRID e consulta le Best practice per l'utilizzo dei gruppi ad alta disponibilità con FabricPool.

Che cos'è un gruppo ha?

Un gruppo ad alta disponibilità (ha) è un insieme di interfacce da più nodi gateway StorageGRID, nodi amministrativi o entrambi. Un gruppo ha aiuta a mantenere disponibili le connessioni dati dei client. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool.

Ogni gruppo ha fornisce un accesso altamente disponibile ai servizi condivisi sui nodi associati. Ad esempio, un gruppo ha costituito da interfacce solo su nodi gateway o su entrambi i nodi Admin e Gateway fornisce un accesso altamente disponibile al servizio Load Balancer condiviso.

Per ulteriori informazioni sui gruppi ad alta disponibilità, vedere "Gestire i gruppi ad alta disponibilità (ha)".

Utilizzo di gruppi ha

Le Best practice per la creazione di un gruppo StorageGRID ha per FabricPool dipendono dal carico di lavoro.

- Se si prevede di utilizzare FabricPool con i dati del carico di lavoro primario, è necessario creare un gruppo ha che includa almeno due nodi di bilanciamento del carico per evitare l'interruzione del recupero dei dati.
- Se si prevede di utilizzare la policy di tiering del volume solo snapshot di FabricPool o Tier di performance locali non primari (ad esempio, ubicazioni per il disaster recovery o destinazioni NetApp SnapMirror®), è possibile configurare un gruppo ha con un solo nodo.

Queste istruzioni descrivono la configurazione di un gruppo ha per Active-Backup ha (un nodo è attivo e un nodo è il backup). Tuttavia, potrebbe essere preferibile utilizzare DNS Round Robin o Active-Active ha. Per ulteriori informazioni sui vantaggi di queste altre configurazioni ha, vedere "Opzioni di configurazione per i gruppi ha".

Best practice per il bilanciamento del carico per FabricPool

Prima di associare StorageGRID come livello cloud FabricPool, esaminare le Best practice per l'utilizzo dei bilanciatori di carico con FabricPool.

Per informazioni generali sul bilanciamento del carico StorageGRID e sul certificato di bilanciamento del

carico, vedere "Considerazioni per il bilanciamento del carico".

Best practice per l'accesso del tenant all'endpoint del bilanciamento del carico utilizzato per FabricPool

È possibile controllare quali tenant possono utilizzare un endpoint specifico di bilanciamento del carico per accedere ai bucket. È possibile consentire tutti i tenant, consentire alcuni tenant o bloccare alcuni tenant. Quando si crea un endpoint di bilanciamento del carico per l'utilizzo di FabricPool, selezionare **Allow all tenant** (Consenti tutti i tenant). ONTAP crittografa i dati inseriti nei bucket StorageGRID, pertanto questo livello di sicurezza aggiuntivo non offre una sicurezza aggiuntiva minima.

Best practice per il certificato di sicurezza

Quando si crea un endpoint di bilanciamento del carico StorageGRID per l'utilizzo di FabricPool, si fornisce il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

Nella maggior parte dei casi, la connessione tra ONTAP e StorageGRID deve utilizzare la crittografia TLS (Transport Layer Security). L'utilizzo di FabricPool senza crittografia TLS è supportato ma non consigliato. Quando si seleziona il protocollo di rete per l'endpoint del bilanciamento del carico StorageGRID, selezionare **HTTPS**. Quindi, fornire il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

Per ulteriori informazioni sul certificato server per un endpoint di bilanciamento del carico:

- "Gestire i certificati di sicurezza"
- "Considerazioni per il bilanciamento del carico"
- "Linee guida per la protezione avanzata dei certificati server"

Aggiungi certificato a ONTAP

Quando si aggiunge StorageGRID come livello cloud FabricPool, è necessario installare lo stesso certificato nel cluster ONTAP, inclusi i certificati root e gli eventuali certificati CA subordinati.

Gestire la scadenza del certificato

> ⚠ Se il certificato utilizzato per proteggere la connessione tra ONTAP e StorageGRID scade, FabricPool smetterà temporaneamente di funzionare e ONTAP perderà temporaneamente l'accesso ai dati a livello di StorageGRID.

Per evitare problemi di scadenza del certificato, attenersi alle seguenti Best practice:

- Monitorare attentamente gli avvisi che avvisano di avvicinarsi alle date di scadenza del certificato, come ad esempio **scadenza del certificato endpoint del bilanciamento del carico** e **scadenza del certificato server globale per gli avvisi S3 e Swift API**.
- Mantenere sempre sincronizzate le versioni StorageGRID e ONTAP del certificato. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint di bilanciamento del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato da ONTAP per il livello cloud.
- Utilizzare un certificato CA con firma pubblica. Se si utilizza un certificato firmato da una CA, è possibile utilizzare l'API Grid Management per automatizzare la rotazione del certificato. Ciò consente di sostituire i certificati in scadenza senza interruzioni.
- Se è stato generato un certificato StorageGRID autofirmato e il certificato sta per scadere, è necessario sostituirlo manualmente in StorageGRID e in ONTAP prima della scadenza del certificato esistente. Se un certificato autofirmato è già scaduto, disattivare la convalida del certificato in ONTAP per evitare la perdita di accesso.

Vedere "Knowledge base di NetApp: Come configurare un nuovo certificato server autofirmato StorageGRID su un'implementazione ONTAP FabricPool esistente" per istruzioni.

Best practice per l'utilizzo di ILM con i dati FabricPool

Se si utilizza FabricPool per eseguire il tiering dei dati in StorageGRID, è necessario comprendere i requisiti per l'utilizzo di ILM (Information Lifecycle Management) di StorageGRID con i dati FabricPool.

> FabricPool non conosce le regole o le policy ILM di StorageGRID. La perdita di dati può verificarsi se il criterio ILM di StorageGRID non è configurato correttamente. Per informazioni dettagliate, vedere "Creare una regola ILM: Panoramica" e. "Creare una policy ILM: Panoramica".

Linee guida per l'utilizzo di ILM con FabricPool

Quando si utilizza l'installazione guidata di FabricPool, la procedura guidata crea automaticamente una nuova regola ILM per ogni bucket S3 creato e aggiunge tale regola a un criterio inattivo. Viene richiesto di attivare il criterio. La regola creata automaticamente segue le Best practice consigliate: Utilizza la codifica di cancellazione 2+1 in un singolo sito.

Se si sta configurando StorageGRID manualmente invece di utilizzare l'installazione guidata di FabricPool, consultare queste linee guida per assicurarsi che le regole ILM e i criteri ILM siano adatti ai dati FabricPool e ai requisiti di business. Potrebbe essere necessario creare nuove regole e aggiornare i criteri ILM attivi per soddisfare queste linee guida.

- Puoi utilizzare qualsiasi combinazione di regole di replica e erasure coding per proteggere i dati del livello cloud.

  La Best practice consigliata consiste nell'utilizzare la codifica di cancellazione 2+1 all'interno di un sito per una protezione dei dati conveniente. L'erasure coding utilizza più CPU, ma offre una capacità di storage significativamente inferiore rispetto alla replica. Gli schemi 4+1 e 6+1 utilizzano una capacità inferiore rispetto allo schema 2+1. Tuttavia, gli schemi 4+1 e 6+1 sono meno flessibili se è necessario aggiungere nodi di storage durante l'espansione della griglia. Per ulteriori informazioni, vedere "Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione".

- Ogni regola applicata ai dati FabricPool deve utilizzare la codifica di cancellazione oppure creare almeno due copie replicate.

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

- Se necessario "Rimuovere i dati FabricPool da StorageGRID", Utilizzare ONTAP per recuperare tutti i dati per il volume FabricPool e promuoverlo al livello di performance.

  > Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool. Impostare il periodo di conservazione in ogni regola ILM su **forever** per garantire che gli oggetti FabricPool non vengano cancellati da ILM StorageGRID.

- Non creare regole che spostino i dati del Tier cloud FabricPool dal bucket a un'altra posizione. Non è possibile utilizzare un pool di storage cloud per spostare i dati FabricPool in un altro archivio di oggetti. Allo stesso modo, non è possibile archiviare i dati FabricPool su nastro utilizzando un nodo di archiviazione.

> 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.

- A partire da ONTAP 9.8, è possibile creare tag a oggetti per semplificare la classificazione e l'ordinamento dei dati a più livelli. Ad esempio, è possibile impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Quindi, quando si creano le regole ILM in StorageGRID, è possibile utilizzare il filtro avanzato tag oggetto per selezionare e inserire questi dati.

Altre Best practice per StorageGRID e FabricPool

Quando si configura un sistema StorageGRID per l'utilizzo con FabricPool, potrebbe essere necessario modificare altre opzioni di StorageGRID. Prima di modificare un'impostazione globale, valutare in che modo la modifica influirà sulle altre applicazioni S3.

Destinazioni di log e messaggi di audit

I carichi di lavoro FabricPool spesso prevedono un elevato tasso di operazioni di lettura, che può generare un elevato volume di messaggi di audit.

- Se non si richiede un record delle operazioni di lettura del client per FabricPool o qualsiasi altra applicazione S3, andare a **CONFIGURAZIONE** > **monitoraggio** > **verifica e server syslog**. Modificare l'impostazione **letture client** su **errore** per ridurre il numero di messaggi di controllo registrati nel registro di controllo. Vedere "Configurare i messaggi di audit e le destinazioni dei log" per ulteriori informazioni.
- Se si dispone di un grande grid, si utilizzano più tipi di applicazioni S3 o si desidera conservare tutti i dati di audit, configurare un server syslog esterno e salvare le informazioni di audit in remoto. L'utilizzo di un server esterno riduce al minimo l'impatto delle performance della registrazione dei messaggi di audit senza ridurre la completezza dei dati di audit. Vedere "Considerazioni sul server syslog esterno" per ulteriori informazioni.

Crittografia degli oggetti

Durante la configurazione di StorageGRID, è possibile attivare il "opzione globale per la crittografia degli oggetti memorizzati" Se è richiesta la crittografia dei dati per altri client StorageGRID. I dati a più livelli da FabricPool a StorageGRID sono già crittografati, pertanto l'attivazione dell'impostazione StorageGRID non è necessaria. Le chiavi di crittografia lato client sono di proprietà di ONTAP.

Compressione degli oggetti

Durante la configurazione di StorageGRID, non attivare "opzione globale per comprimere gli oggetti memorizzati". I dati a più livelli da FabricPool a StorageGRID sono già compressi. L'utilizzo dell'opzione StorageGRID non riduce ulteriormente le dimensioni di un oggetto.

Consistenza della benna

Per i bucket FabricPool, la coerenza del bucket consigliata è **Read-after-new-write**, che è la coerenza predefinita per un nuovo bucket. Non modificare i bucket FabricPool per utilizzare **available** o **strong-site**.

Tiering FabricPool

Se un nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verificare che il volume non disponga di un criterio di tiering FabricPool attivato. Ad esempio, se un nodo StorageGRID è in esecuzione su un host VMware, assicurarsi che il volume che esegue il backup del datastore per il nodo StorageGRID non abbia un criterio di tiering FabricPool attivato. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

> Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

Rimuovere i dati FabricPool da StorageGRID

Se è necessario rimuovere i dati FabricPool attualmente memorizzati in StorageGRID, è necessario utilizzare ONTAP per recuperare tutti i dati del volume FabricPool e promuoverli al livello di performance.

Prima di iniziare

- Sono state esaminate le istruzioni e le considerazioni in "Promuovi i dati al Tier di performance".
- Si utilizza ONTAP 9.8 o versione successiva.
- Si sta utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti StorageGRID per l'account tenant FabricPool che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root".

A proposito di questa attività

Queste istruzioni spiegano come trasferire i dati da StorageGRID a FabricPool. Eseguire questa procedura utilizzando ONTAP e Gestore tenant StorageGRID.

Fasi

1. Da ONTAP, eseguire il `volume modify` comando.

   Impostare `tiering-policy` a. `none` per interrompere il nuovo tiering e l'impostazione `cloud-retrieval-policy` a. `promote` Per restituire tutti i dati che erano stati precedentemente Tiered a StorageGRID.

   Vedere "Promuovi tutti i dati da un volume FabricPool al Tier di performance".

2. Attendere il completamento dell'operazione.

   È possibile utilizzare `volume object-store` con il `tiering` opzione a. "verifica lo stato della promozione del tier di performance".

3. Una volta completata l'operazione di promozione, accedere al manager tenant StorageGRID per ottenere l'account tenant FabricPool.
4. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
5. Verificare che il bucket FabricPool sia vuoto.
6. Se il bucket è vuoto, "eliminare il bucket".

Al termine

Quando si elimina il bucket, il tiering da FabricPool a StorageGRID non può più continuare. Tuttavia, poiché il Tier locale è ancora collegato al Tier cloud di StorageGRID, Gestore di sistema di ONTAP restituirà messaggi di errore che indicano che il bucket non è accessibile.

Per evitare questi messaggi di errore, effettuare una delle seguenti operazioni:

- Utilizza il mirror FabricPool per collegare un altro livello cloud all'aggregato.
- Spostare i dati dall'aggregato FabricPool a un aggregato non FabricPool, quindi eliminare l'aggregato inutilizzato.

Vedere "Documentazione ONTAP per FabricPool" per istruzioni.

Utilizzare tenant e client StorageGRID

Utilizzare un account tenant

USA un account tenant: Panoramica

Un account tenant consente di utilizzare l'API REST di S3 (Simple Storage Service) o l'API REST di Swift per memorizzare e recuperare oggetti in un sistema StorageGRID.

Che cos'è un account tenant?

Ogni account tenant dispone di gruppi federati o locali, utenti, bucket S3 o container Swift e oggetti.

Gli account tenant possono essere utilizzati per separare gli oggetti memorizzati da diverse entità. Ad esempio, è possibile utilizzare più account tenant per uno dei seguenti casi di utilizzo:

- **Caso d'utilizzo aziendale:** se il sistema StorageGRID viene utilizzato all'interno di un'azienda, lo storage a oggetti del grid potrebbe essere separato dai diversi reparti dell'organizzazione. Ad esempio, potrebbero essere presenti account tenant per il reparto Marketing, il reparto Assistenza clienti, il reparto risorse umane e così via.

  > Se si utilizza il protocollo client S3, è anche possibile utilizzare i bucket S3 e le policy bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario creare account tenant separati. Vedere le istruzioni per l'implementazione "Bucket S3 e policy bucket" per ulteriori informazioni.

- **Caso d'utilizzo del provider di servizi:** se il sistema StorageGRID viene utilizzato da un provider di servizi, lo storage a oggetti della griglia potrebbe essere separato dalle diverse entità che affittano lo storage. Ad esempio, potrebbero essere presenti account tenant per la società A, la società B, la società C e così via.

Come creare un account tenant

Gli account tenant vengono creati da "Amministratore della griglia di StorageGRID che utilizza il gestore della griglia". Quando si crea un account tenant, l'amministratore della griglia specifica quanto segue:

- Informazioni di base, tra cui il nome del tenant, il tipo di client (S3 o Swift) e la quota di storage opzionale.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine di identità, utilizzare S3 Select o utilizzare una connessione a federazione di griglie.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione di identità o SSO (Single Sign-on).

Inoltre, gli amministratori della griglia possono attivare l'impostazione blocco oggetti S3 per il sistema StorageGRID se gli account tenant S3 devono soddisfare i requisiti normativi. Quando S3 Object Lock è attivato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

Configurare i tenant S3

Dopo un "Viene creato l'account tenant S3", È possibile accedere a Tenant Manager per eseguire attività come le seguenti:

- Configurare la federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia)
- Gestire gruppi e utenti
- Utilizza la federazione di grid per il clone dell'account e la replica cross-grid
- Gestire le chiavi di accesso S3
- Creare e gestire i bucket S3
- Utilizzare i servizi della piattaforma S3
- USA S3 Select
- Monitorare l'utilizzo dello storage

Anche se è possibile creare e gestire bucket S3 con Tenant Manager, è necessario utilizzare un "Client S3" oppure "S3 Console" acquisizione e gestione degli oggetti.

Configurare i tenant di Swift

Dopo un "Viene creato un account tenant Swift", È possibile accedere a Tenant Manager per eseguire attività come le seguenti:

- Configurare la federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia)
- Gestire gruppi e utenti
- Monitorare l'utilizzo dello storage

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

Come effettuare l'accesso e disconnettersi

Accedi a Tenant Manager

Per accedere a Tenant Manager, immettere l'URL del tenant nella barra degli indirizzi di a. "browser web supportato".

Prima di iniziare

- Si dispone delle credenziali di accesso.
- Si dispone di un URL per accedere a Tenant Manager, fornito dall'amministratore della griglia. L'URL sarà simile a uno dei seguenti esempi:

```
https://FQDN_or_Admin_Node_IP/

https://FQDN_or_Admin_Node_IP:port/

https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

L'URL include sempre un nome di dominio completo (FQDN), l'indirizzo IP di un nodo amministrativo o l'indirizzo IP virtuale di un gruppo ha di nodi amministrativi. Potrebbe anche includere un numero di porta,

l'ID dell'account tenant a 20 cifre o entrambi.

- Se l'URL non include l'ID account a 20 cifre del tenant, si dispone di questo ID account.
- Si sta utilizzando un "browser web supportato".
- I cookie sono attivati nel browser Web.
- L'utente appartiene a un gruppo di utenti che dispone di "autorizzazioni di accesso specifiche".

Fasi

1. Avviare un "browser web supportato".
2. Nella barra degli indirizzi del browser, immettere l'URL per accedere a Tenant Manager.
3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser.
4. Accedi al tenant manager.

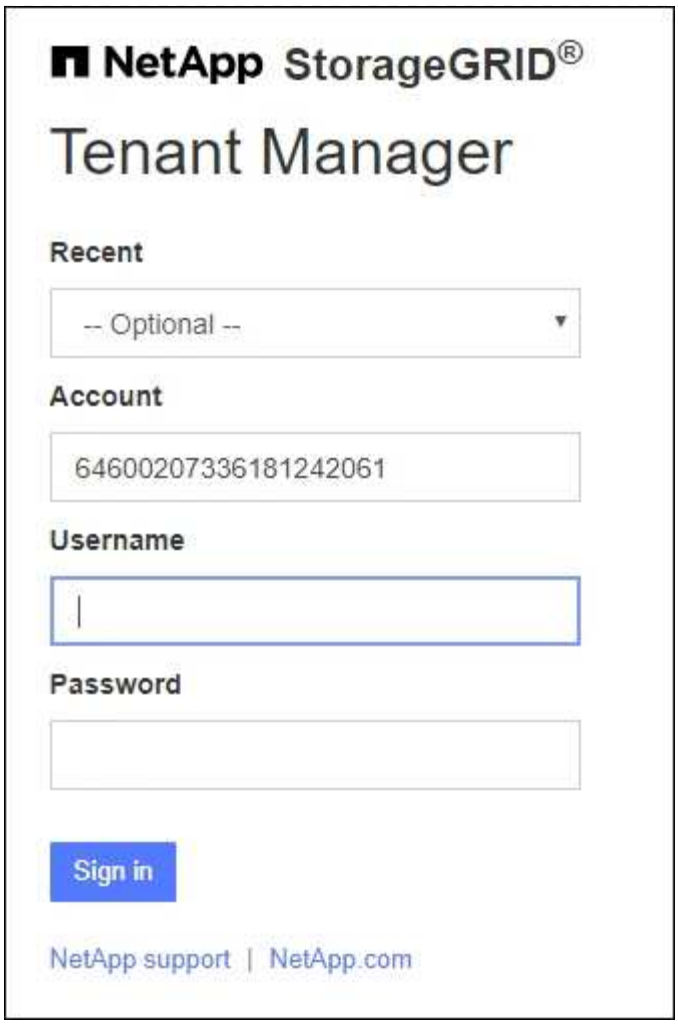
   La schermata di accesso che viene visualizzata dipende dall'URL immesso e dalla configurazione di SSO (Single Sign-on) per StorageGRID.

Non si utilizza SSO

Se StorageGRID non utilizza SSO, viene visualizzata una delle seguenti schermate:

- Pagina di accesso a Grid Manager. Selezionare il collegamento **accesso tenant**.

- La pagina di accesso del tenant manager. Il campo **account** potrebbe essere già completato, come mostrato di seguito.



i. Se l'ID account a 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account tenant, se visualizzato nell'elenco degli account recenti, oppure inserire l'ID account.

ii. Immettere il nome utente e la password.

iii. Selezionare **Accedi**.

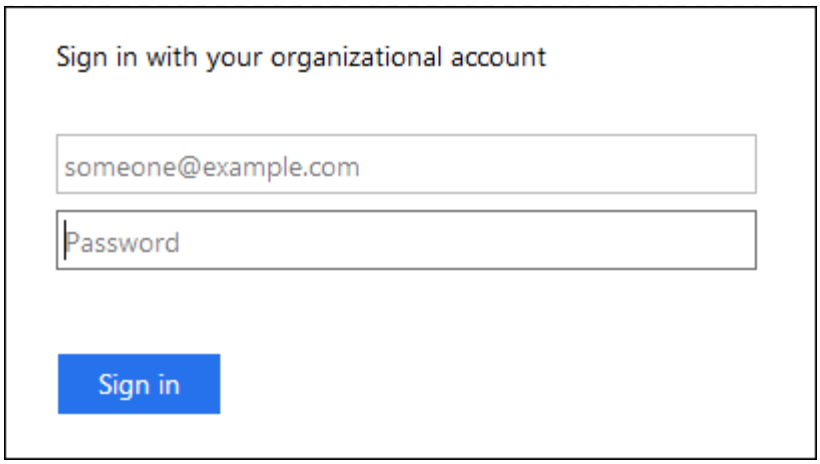
Viene visualizzata la dashboard di Tenant Manager.

iv. Se hai ricevuto una password iniziale da un altro utente, seleziona ***Username*** > **Change password** per proteggere il tuo account.

Utilizzo di SSO

Se StorageGRID utilizza SSO, viene visualizzata una delle seguenti schermate:

◦ Pagina SSO della tua organizzazione. Ad esempio:



Immettere le credenziali SSO standard e selezionare **Accedi**.

- La pagina di accesso SSO di Tenant Manager.

i. Se l'ID account a 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account tenant, se visualizzato nell'elenco degli account recenti, oppure inserire l'ID account.

ii. Selezionare **Accedi**.

iii. Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

Viene visualizzata la dashboard di Tenant Manager.

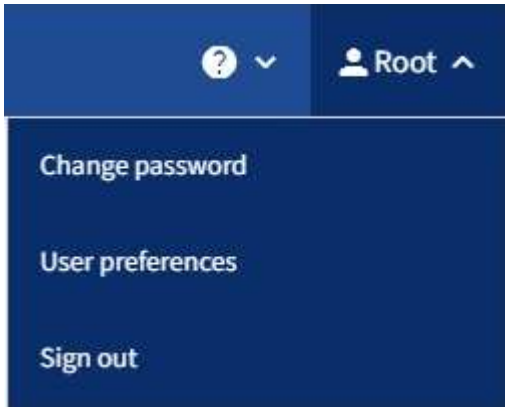
Disconnettersi da Tenant Manager

Una volta terminato il lavoro con il tenant manager, devi disconnetterti per garantire che

gli utenti non autorizzati non possano accedere al sistema StorageGRID. La chiusura del browser potrebbe non disconnettersi dal sistema, in base alle impostazioni dei cookie del browser.

Fasi

1. Individuare il menu a discesa Username (Nome utente) nell'angolo in alto a destra dell'interfaccia utente.



2. Selezionare il nome utente, quindi selezionare **Disconnetti**.

   - Se SSO non è in uso:

     Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso del tenant manager.

     Se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.

   - Se SSO è attivato:

     Si è disconnessi da tutti i nodi di amministrazione ai quali si stava accedendo. Viene visualizzata la pagina di accesso a StorageGRID. Il nome dell'account tenant a cui hai appena effettuato l'accesso viene elencato come predefinito nell'elenco a discesa **account recenti** e viene visualizzato l'ID account* del tenant.

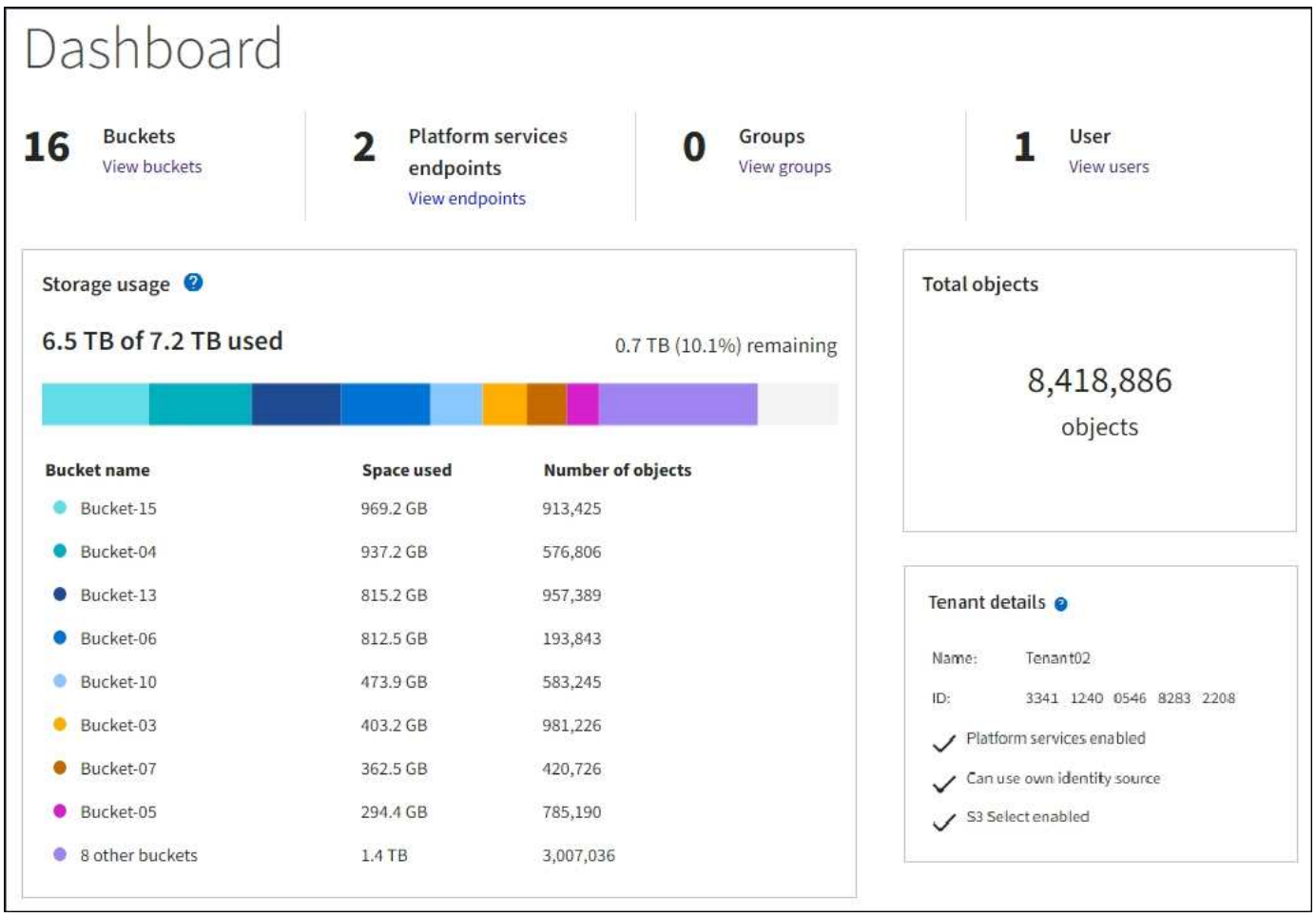
     Se SSO è attivato e si è anche connessi a Grid Manager, è necessario disconnettersi da Grid Manager per disconnettersi da SSO.

Comprendere la dashboard di Tenant Manager

La dashboard di Tenant Manager offre una panoramica della configurazione di un account tenant e della quantità di spazio utilizzata dagli oggetti nei bucket (S3) o nei container (Swift) del tenant. Se il tenant dispone di una quota, la dashboard mostra la quantità di quota utilizzata e la quantità rimanente. In caso di errori relativi all'account tenant, gli errori vengono visualizzati nella dashboard.

I valori di spazio utilizzato sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi.

Una volta caricati gli oggetti, la dashboard è simile al seguente esempio:



Riepilogo account tenant

La parte superiore della dashboard contiene le seguenti informazioni:

- Il numero di bucket o container configurati, gruppi e utenti
- Il numero di endpoint dei servizi della piattaforma, se configurati

È possibile selezionare i collegamenti per visualizzare i dettagli.

Il lato destro della dashboard contiene le seguenti informazioni:

- Il numero totale di oggetti per il tenant.

  Per un account S3, se non sono stati acquisiti oggetti e si dispone di "Autorizzazione di accesso root", vengono visualizzate le linee guida per iniziare invece del numero totale di oggetti.

- Dettagli del tenant, inclusi il nome e l'ID dell'account tenant e se il tenant può utilizzarlo "servizi della piattaforma", "la propria origine di identità", "federazione di grid", o. "S3 Seleziona" (vengono elencate solo le autorizzazioni attivate).

Utilizzo dello storage e delle quote

Il pannello Storage Use (utilizzo storage) contiene le seguenti informazioni:

- La quantità di dati oggetto per il tenant.

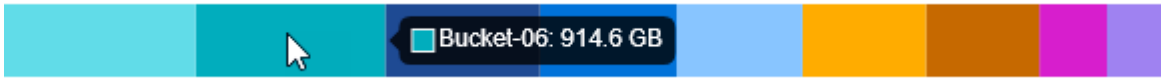
> Questo valore indica la quantità totale di dati dell'oggetto caricati e non rappresenta lo spazio utilizzato per memorizzare le copie di tali oggetti e dei relativi metadati.

- Se viene impostata una quota, la quantità totale di spazio disponibile per i dati dell'oggetto e la quantità e la percentuale di spazio rimanente. La quota limita la quantità di dati oggetto che è possibile acquisire.

> L'utilizzo delle quote si basa su stime interne e in alcuni casi potrebbe essere superato. Ad esempio, StorageGRID controlla la quota quando un tenant avvia il caricamento degli oggetti e rifiuta le nuove ricerche se il tenant ha superato la quota. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente quando determina se la quota è stata superata. Se gli oggetti vengono eliminati, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti fino a quando l'utilizzo della quota non viene ricalcolato. I calcoli relativi all'utilizzo delle quote possono richiedere 10 minuti o più.

- Un grafico a barre che rappresenta le dimensioni relative dei bucket o dei container più grandi.

  È possibile posizionare il cursore su uno dei segmenti del grafico per visualizzare lo spazio totale consumato da quel bucket o container.



- Per corrispondere al grafico a barre, un elenco dei bucket o container più grandi, inclusa la quantità totale di dati oggetto e il numero di oggetti per ciascun bucket o container.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

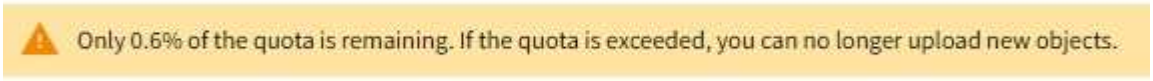
  Se il tenant ha più di nove bucket o container, tutti gli altri bucket o container vengono combinati in una singola voce in fondo all'elenco.

Per modificare le unità per i valori di storage visualizzati in Tenant Manager, selezionare il menu a discesa User (utente) in alto a destra in Tenant Manager, quindi selezionare **User preferences** (Preferenze utente).

Avvisi sull'utilizzo delle quote

Se gli avvisi sull'utilizzo delle quote sono stati attivati in Grid Manager, vengono visualizzati in Tenant Manager quando la quota è bassa o superata, come segue:

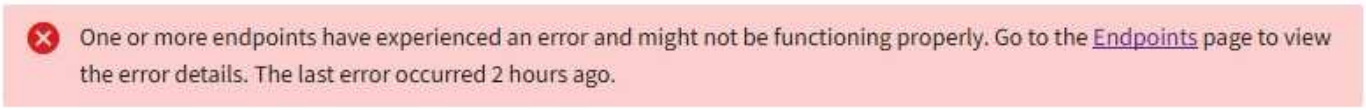
Se è stato utilizzato il 90% o più della quota di un tenant, viene attivato l'avviso **quota di utilizzo elevata del tenant**. Eseguire le azioni consigliate per l'avviso.



Se si supera la quota, non è possibile caricare nuovi oggetti.

Errori degli endpoint

Se hai utilizzato Grid Manager per configurare uno o più endpoint da utilizzare con i servizi della piattaforma, la dashboard di Tenant Manager visualizza un avviso se si sono verificati errori degli endpoint negli ultimi sette giorni.



Per visualizzare i dettagli su "errori degli endpoint dei servizi della piattaforma", Selezionare **Endpoint** per visualizzare la pagina Endpoint.

API di gestione del tenant

Comprendere l'API di gestione dei tenant

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Tenant Management invece dell'interfaccia utente di Tenant Manager. Ad esempio, è possibile utilizzare l'API per automatizzare le operazioni o creare più entità, ad esempio gli utenti, più rapidamente.

L'API di gestione dei tenant:

- Utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che consente a sviluppatori e non sviluppatori di interagire con l'API. L'interfaccia utente di Swagger fornisce dettagli completi e documentazione per ogni operazione API.
- Utilizzi "versione per supportare aggiornamenti senza interruzioni".

Per accedere alla documentazione Swagger per l'API di gestione tenant:

1. Accedi al tenant manager.
2. Nella parte superiore di Tenant Manager, selezionare l'icona della guida e selezionare **documentazione API**.

Operazioni API

L'API di gestione tenant organizza le operazioni API disponibili nelle seguenti sezioni:

- **Account**: Operazioni sull'account tenant corrente, incluso il recupero delle informazioni sull'utilizzo dello storage.
- **Auth**: Operazioni per l'autenticazione della sessione utente.

  L'API di gestione tenant supporta lo schema di autenticazione del token del bearer. Per l'accesso del tenant, immettere un nome utente, una password e un ID account nel corpo JSON della richiesta di autenticazione (ovvero `POST /api/v3/authorize`). Se l'utente viene autenticato correttamente, viene restituito un token di sicurezza. Questo token deve essere fornito nell'intestazione delle richieste API successive ("autorizzazione: Token portante").

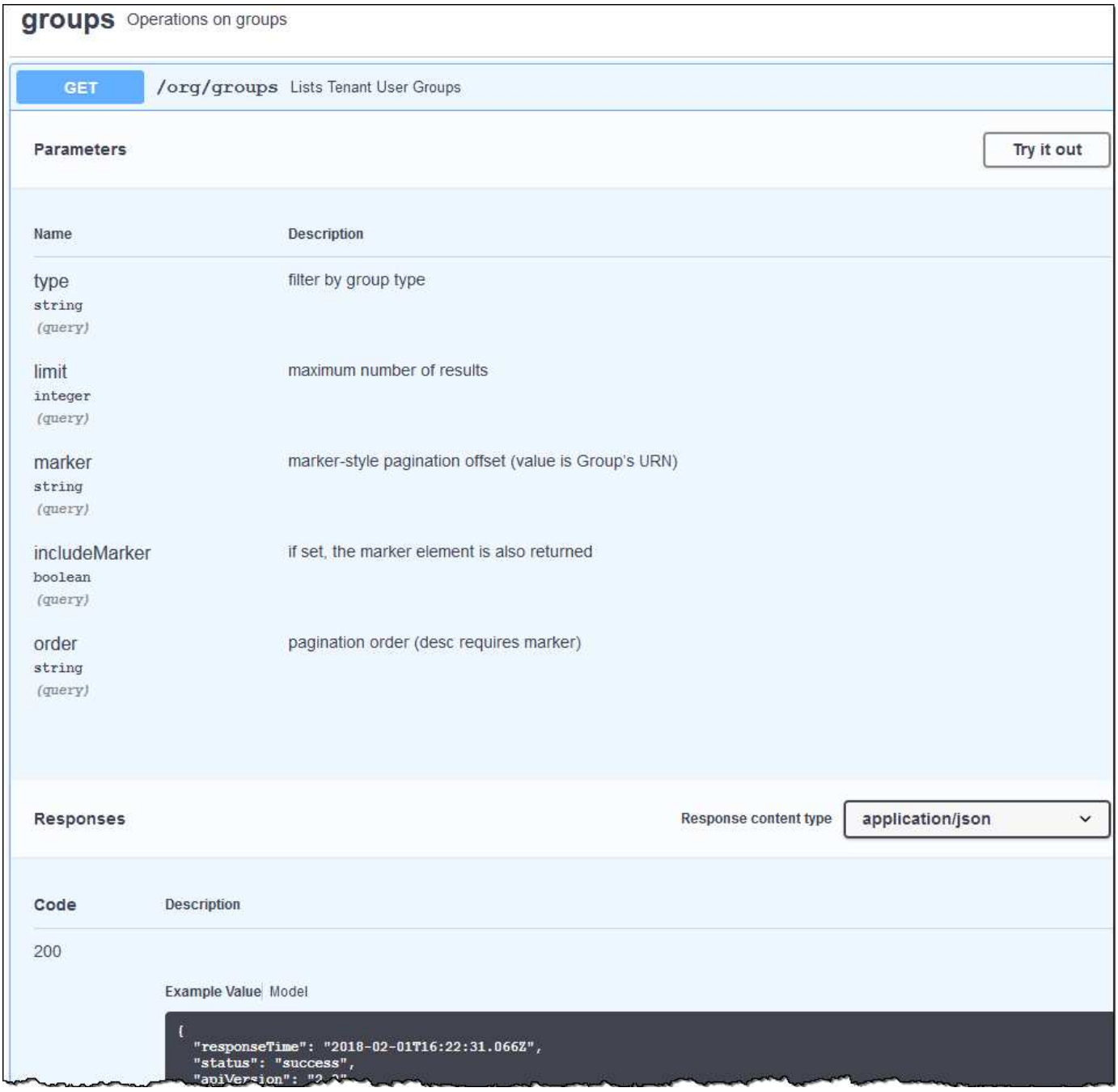
  Per informazioni su come migliorare la protezione dell'autenticazione, vedere "Protezione contro la falsificazione di richieste cross-site".

  > Se per il sistema StorageGRID è attivato il Single Sign-on (SSO), è necessario eseguire diversi passaggi per l'autenticazione. Vedere "Istruzioni per l'utilizzo dell'API Grid Management".

- **Config**: Operazioni relative alla release del prodotto e alle versioni dell'API di gestione tenant. È possibile elencare la versione di release del prodotto e le principali versioni dell'API supportate da tale release.
- **Container**: Operazioni su bucket S3 o container Swift.
- **Disattivato-funzioni**: Operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **Endpoint**: Operazioni per gestire un endpoint. Gli endpoint consentono a un bucket S3 di utilizzare un servizio esterno per la replica, le notifiche o l'integrazione della ricerca di StorageGRID CloudMirror.
- **Grid-Federation-Connections**: Operazioni su connessioni di federazione di grid e replica cross-grid.
- **Groups**: Operazioni per gestire gruppi tenant locali e recuperare gruppi tenant federati da un'origine di identità esterna.
- **Identity-source**: Operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **ilm**: Operazioni sulle impostazioni ILM (Information Lifecycle Management).
- **Regioni**: Operazioni per determinare quali regioni sono state configurate per il sistema StorageGRID.
- **s3**: Operazioni per gestire le chiavi di accesso S3 per gli utenti del tenant.
- **s3-Object-lock**: Operazioni sulle impostazioni globali S3 Object Lock, utilizzate per supportare la conformità alle normative.
- **Utenti**: Operazioni per visualizzare e gestire gli utenti del tenant.

Dettagli dell'operazione

Quando si espandono le operazioni API, è possibile visualizzare l'azione HTTP, l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le possibili risposte.



Emettere richieste API

Tutte le operazioni API eseguite utilizzando la pagina web API Docs sono operazioni live. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Fasi

1. Selezionare l'azione HTTP per visualizzare i dettagli della richiesta.
2. Determinare se la richiesta richiede parametri aggiuntivi, ad esempio un ID utente o un gruppo. Quindi, ottenere questi valori. Potrebbe essere necessario emettere prima una richiesta API diversa per ottenere le informazioni necessarie.
3. Determinare se è necessario modificare il corpo della richiesta di esempio. In tal caso, è possibile selezionare **modello** per conoscere i requisiti di ciascun campo.

4. Selezionare **Provalo**.
5. Fornire i parametri richiesti o modificare il corpo della richiesta secondo necessità.
6. Selezionare **Esegui**.
7. Esaminare il codice di risposta per determinare se la richiesta ha avuto esito positivo.

Versione dell'API di gestione tenant

L'API di gestione tenant utilizza il controllo delle versioni per supportare aggiornamenti senza interruzioni.

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

```
https://hostname_or_ip_address/api/v4/authorize
```

La versione principale dell'API viene modificata quando vengono apportate modifiche che sono *non compatibili* con le versioni precedenti. La versione secondaria dell'API viene modificata quando vengono apportate modifiche che sono *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o di nuove proprietà.

Nell'esempio seguente viene illustrato il modo in cui la versione dell'API viene modificata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Versione precedente	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene attivata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova release di funzionalità di StorageGRID, si continua ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.

> È possibile configurare le versioni supportate. Vedere la sezione **config** della documentazione Swagger API per "API di Grid Management" per ulteriori informazioni. È necessario disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API per utilizzare la versione più recente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Deprecated: True"
- Il corpo di risposta JSON include "deprecato": Vero
- Viene aggiunto un avviso obsoleto a nms.log. Ad esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinare quali versioni API sono supportate nella release corrente

Utilizzare `GET /versions` Richiesta API per restituire un elenco delle versioni principali dell'API supportate. Questa richiesta si trova nella sezione **config** della documentazione dell'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione dell'API utilizzando un parametro path (`/api/v4`) o un'intestazione (`Api-Version: 4`). Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protezione contro la contraffazione delle richieste (CSRF)

Puoi contribuire a proteggere dagli attacchi di cross-site request forgery (CSRF) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se attivarla al momento dell'accesso.

Un utente malintenzionato in grado di inviare una richiesta a un sito diverso (ad esempio con UN HTTP Form POST) può causare l'esecuzione di determinate richieste utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggere dagli attacchi CSRF utilizzando token CSRF. Se attivato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro POST-body specifico.

Per attivare la funzione, impostare `csrfToken` parametro a. `true` durante l'autenticazione. L'impostazione predefinita è `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando è vero, un `GridCsrfToken` Il cookie viene impostato con un valore casuale per l'accesso a Grid Manager e a. `AccountCsrfToken` Il cookie viene impostato con un valore casuale per l'accesso a Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere una delle seguenti opzioni:

- Il `X-Csrf-Token` Header, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo con codifica a modulo: A. `csrfToken` parametro del corpo della richiesta codificato dal modulo.

Per configurare la protezione CSRF, utilizzare "API di Grid Management" oppure "API di gestione del tenant".

> Le richieste che dispongono di un set di cookie token CSRF applicheranno anche l'intestazione "Content-Type: Application/json" per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzare connessioni di federazione di griglie

Clonare utenti e gruppi tenant

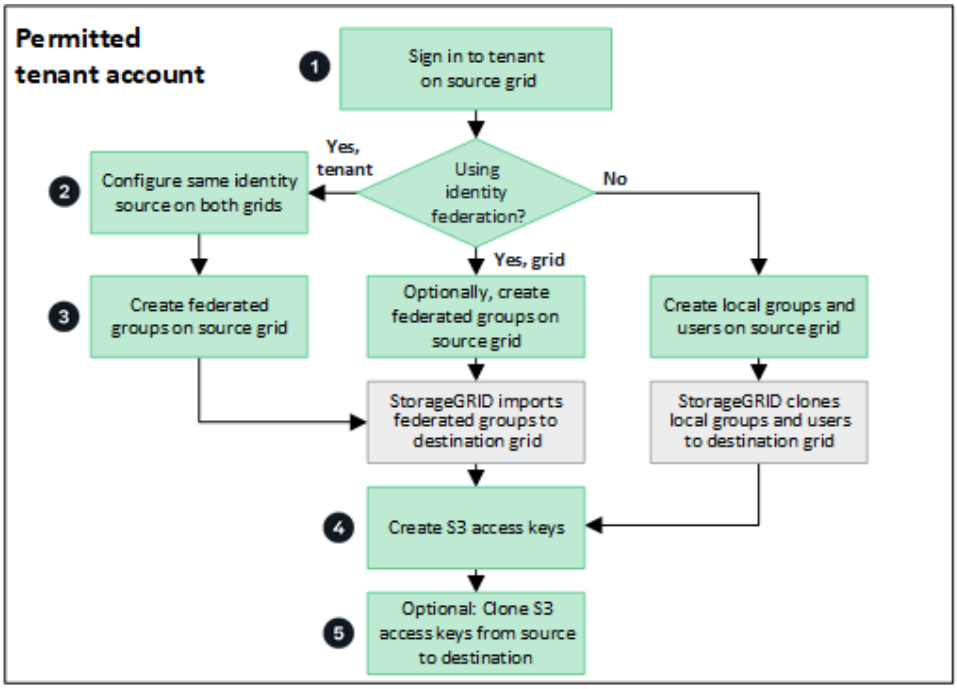
Se un tenant è stato creato o modificato per utilizzare una connessione federazione grid, tale tenant viene replicato da un sistema StorageGRID (il tenant di origine) a un altro sistema StorageGRID (il tenant di replica). Dopo la replica del tenant, tutti i gruppi e gli utenti aggiunti al tenant di origine vengono clonati sul tenant di replica.

Il sistema StorageGRID in cui il tenant viene originariamente creato è la *griglia di origine* del tenant. Il sistema StorageGRID in cui viene replicato il tenant è la *griglia di destinazione* del tenant. Entrambi gli account tenant hanno lo stesso ID account, nome, descrizione, quota di storage e autorizzazioni assegnate, tuttavia, il tenant di destinazione non dispone inizialmente di una password utente root. Per ulteriori informazioni, vedere "Cos'è il clone dell'account" e. "Gestire i tenant autorizzati".

Per è richiesta la clonazione delle informazioni dell'account tenant "replica cross-grid" di oggetti bucket. Avere gli stessi gruppi di tenant e gli stessi utenti su entrambe le griglie garantisce l'accesso ai bucket e agli oggetti corrispondenti su entrambe le griglie.

Workflow del tenant per il clone dell'account

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, consultare il diagramma del flusso di lavoro per visualizzare i passaggi che verranno eseguiti per clonare gruppi, utenti e chiavi di accesso S3.



Questi sono i passaggi principali del flusso di lavoro:

1 Accedi al tenant

Accedere all'account tenant sulla griglia di origine (la griglia in cui è stato creato il tenant).

2 Facoltativamente, configurare la federazione delle identità

Se l'account tenant dispone dell'autorizzazione **Usa origine identità propria** per utilizzare utenti e gruppi federati, configurare la stessa origine identità (con le stesse impostazioni) per gli account tenant di origine e di destinazione. I gruppi federati e gli utenti non possono essere clonati a meno che entrambe le griglie non utilizzino la stessa origine di identità. Per istruzioni, vedere "USA la federazione delle identità".

3 Creare gruppi e utenti

Quando si creano gruppi e utenti, iniziare sempre dalla griglia di origine del tenant. Quando si aggiunge un nuovo gruppo, StorageGRID lo clona automaticamente nella griglia di destinazione.

- Se la federazione di identità è configurata per l'intero sistema StorageGRID o per l'account tenant, "creare nuovi gruppi tenant" importando gruppi federati dall'origine dell'identità.
- Se non si utilizza la federazione delle identità, "creare nuovi gruppi locali" e poi "creare utenti locali".

4 Creare chiavi di accesso S3

È possibile "creare le proprie chiavi di accesso" o a. "creare le chiavi di accesso di un altro utente" sulla griglia di origine o di destinazione per accedere ai bucket di tale griglia.

5 Facoltativamente, clonare le chiavi di accesso S3

Se è necessario accedere ai bucket con le stesse chiavi di accesso su entrambe le griglie, creare le chiavi di accesso nella griglia di origine e utilizzare l'API di Tenant Manager per clonarle manualmente nella griglia di destinazione. Per istruzioni, vedere "Clonare le chiavi di accesso S3 utilizzando l'API".

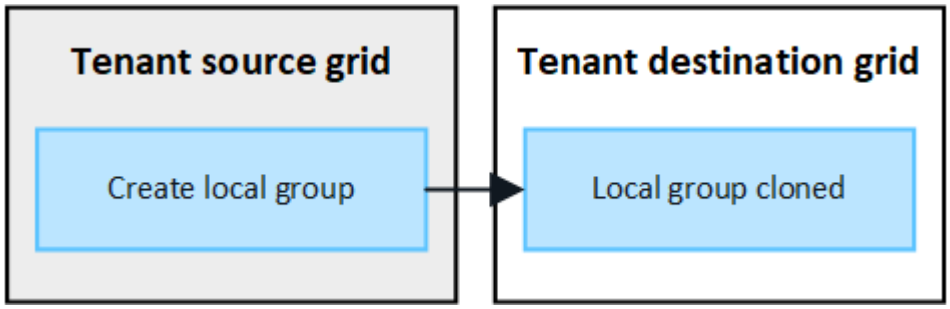
Come vengono clonati gruppi, utenti e chiavi di accesso S3?

Esaminare questa sezione per comprendere come vengono clonati gruppi, utenti e chiavi di accesso S3 tra la griglia di origine del tenant e la griglia di destinazione del tenant.

I gruppi locali creati sulla griglia di origine vengono clonati

Dopo aver creato e replicato un account tenant nella griglia di destinazione, StorageGRID clona automaticamente i gruppi locali aggiunti alla griglia di origine del tenant nella griglia di destinazione del tenant.

Sia il gruppo originale che il clone dispongono della stessa modalità di accesso, delle stesse autorizzazioni di gruppo e dei criteri di gruppo S3. Per istruzioni, vedere "Creare gruppi per il tenant S3".

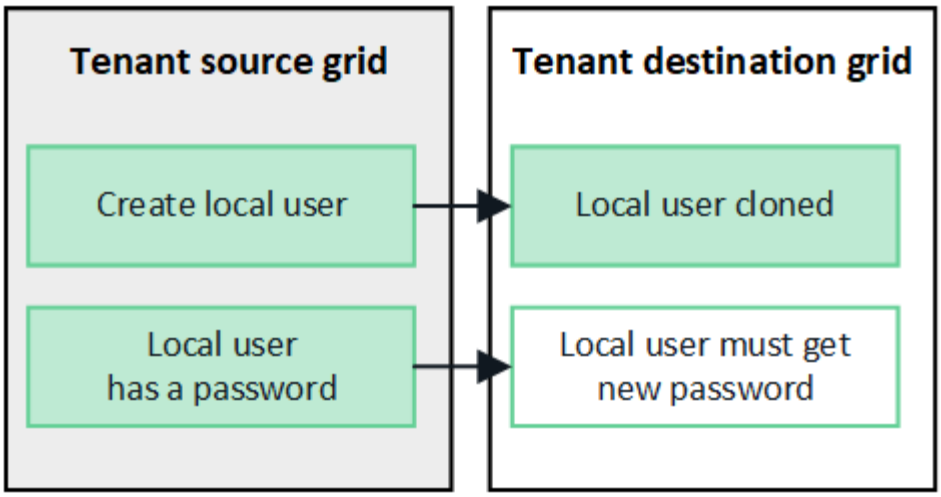


> Tutti gli utenti selezionati quando si crea un gruppo locale nella griglia di origine non vengono inclusi quando il gruppo viene clonato nella griglia di destinazione. Per questo motivo, non selezionare gli utenti quando si crea il gruppo. Al momento della creazione degli utenti, selezionare il gruppo.

Gli utenti locali creati sulla griglia di origine vengono clonati

Quando si crea un nuovo utente locale nella griglia di origine, StorageGRID clona automaticamente tale utente nella griglia di destinazione. Sia l'utente originale che il clone hanno lo stesso nome completo, nome utente e impostazione **Nega accesso**. Entrambi gli utenti appartengono anche agli stessi gruppi. Per istruzioni, vedere "Gestire gli utenti locali".

Per motivi di sicurezza, le password degli utenti locali non vengono clonate nella griglia di destinazione. Se un utente locale deve accedere a Tenant Manager nella griglia di destinazione, l'utente root dell'account tenant deve aggiungere una password per tale utente nella griglia di destinazione. Per istruzioni, vedere "Gestire gli utenti locali".

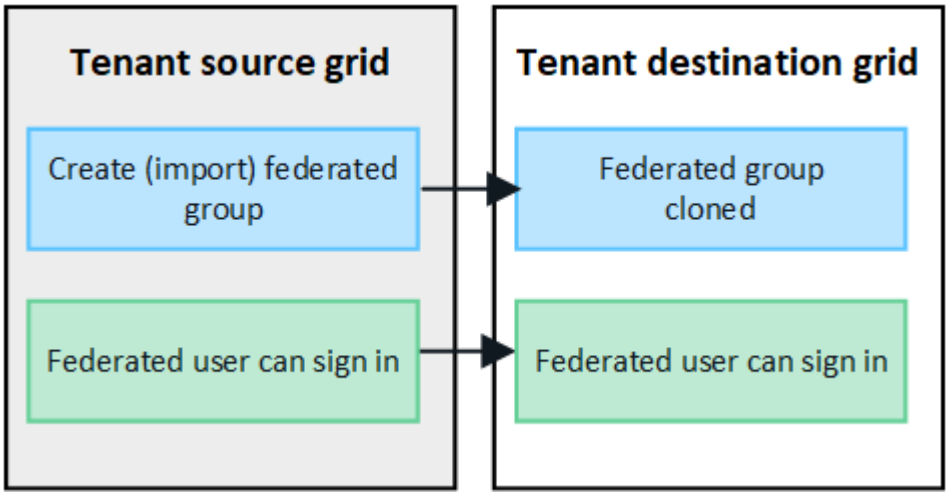


I gruppi federati creati sulla griglia di origine vengono clonati

Presupponendo i requisiti per l'utilizzo del clone dell'account con "single sign-on" e. "federazione delle identità" i gruppi federati creati (importati) per il tenant nella griglia di origine vengono clonati automaticamente nel tenant nella griglia di destinazione.

Entrambi i gruppi dispongono della stessa modalità di accesso, delle stesse autorizzazioni di gruppo e dei criteri di gruppo S3.

Una volta creati i gruppi federati per il tenant di origine e clonati nel tenant di destinazione, gli utenti federati possono accedere al tenant su entrambi i grid.

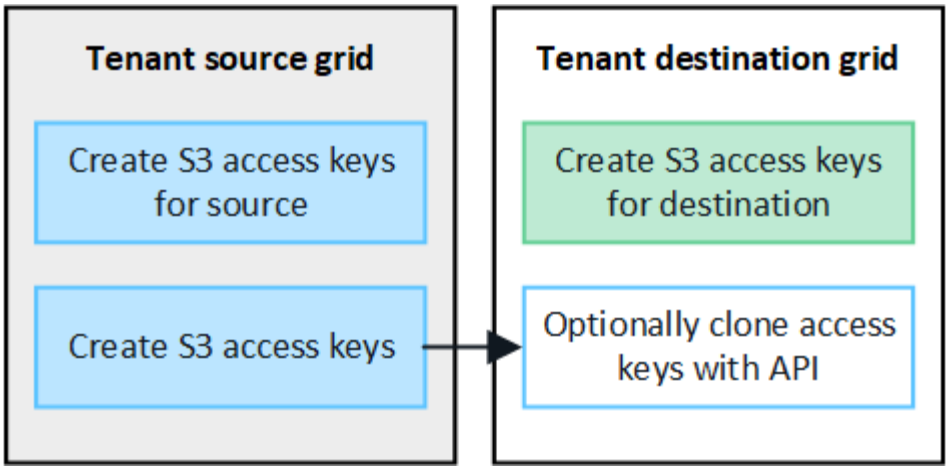


Le chiavi di accesso S3 possono essere clonate manualmente

StorageGRID non clonerà automaticamente le chiavi di accesso S3 perché la sicurezza è migliorata grazie alla presenza di chiavi diverse su ogni griglia.

Per gestire le chiavi di accesso sulle due griglie, è possibile eseguire una delle seguenti operazioni:

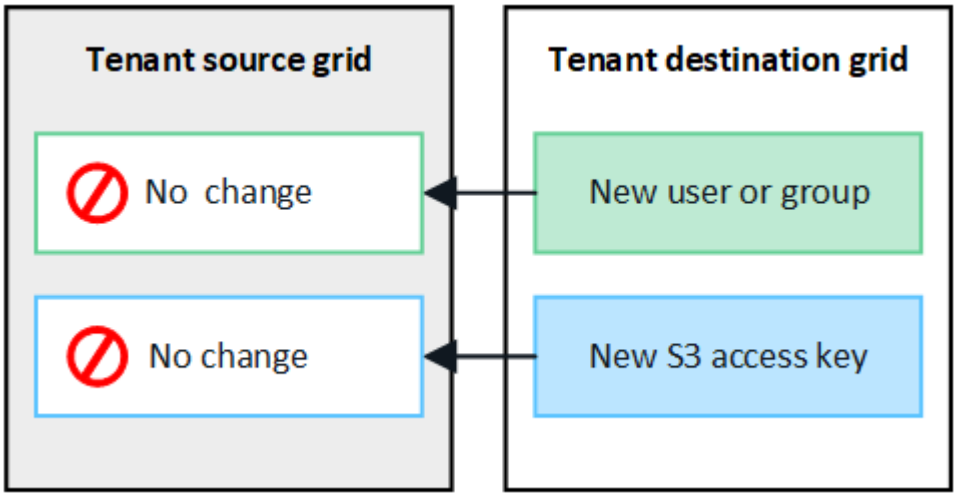
- Se non è necessario utilizzare gli stessi tasti per ogni griglia, è possibile "creare le proprie chiavi di accesso" oppure "creare le chiavi di accesso di un altro utente" su ogni griglia.
- Se è necessario utilizzare le stesse chiavi su entrambe le griglie, è possibile creare chiavi nella griglia di origine e utilizzare l'API di Tenant Manager per manualmente "clonare le chiavi" alla griglia di destinazione.



Quando si clonano le chiavi di accesso S3 per un utente federato, sia l'utente che le chiavi di accesso S3 vengono clonate nel tenant di destinazione.

I gruppi e gli utenti aggiunti alla griglia di destinazione non vengono clonati

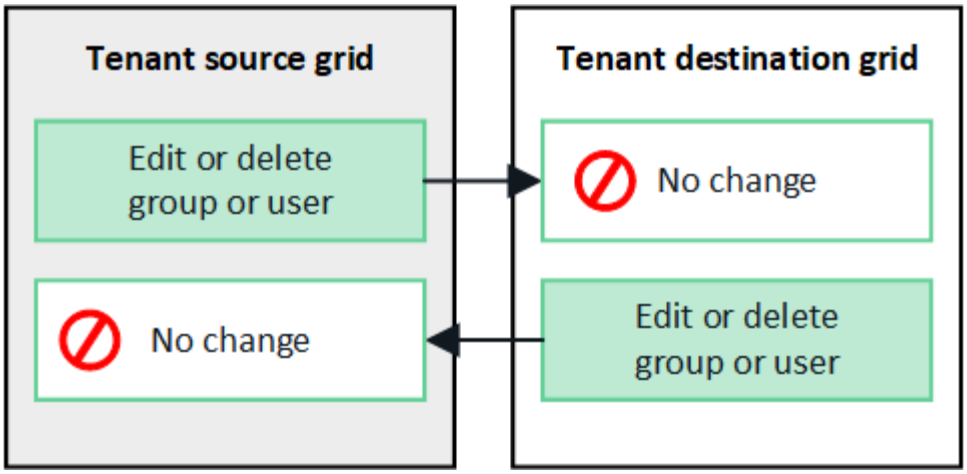
La clonazione avviene solo dalla griglia di origine del tenant alla griglia di destinazione del tenant. Se si creano o importano gruppi e utenti nella griglia di destinazione del tenant, StorageGRID non clonerà questi elementi nella griglia di origine del tenant.



I gruppi, gli utenti e le chiavi di accesso modificati o cancellati non vengono clonati

La clonazione avviene solo quando si creano nuovi gruppi e utenti.

Se si modificano o eliminano gruppi, utenti o chiavi di accesso in una griglia, le modifiche non verranno clonate nell'altra griglia.



Clonare le chiavi di accesso S3 utilizzando l'API

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile utilizzare l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione.

Prima di iniziare

- L'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**.
- La connessione a federazione di griglie ha uno stato **Connection** di **Connected**.
- Hai effettuato l'accesso al tenant Manager sulla griglia di origine del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestisci le tue credenziali S3 o l'autorizzazione di accesso root".
- Se si clonano le chiavi di accesso per un utente locale, l'utente esiste già su entrambe le griglie.

> Quando si clonano le chiavi di accesso S3 per un utente federato, sia l'utente che le chiavi di accesso S3 vengono aggiunte al tenant di destinazione.

Clonare le proprie chiavi di accesso

È possibile clonare le proprie chiavi di accesso se è necessario accedere agli stessi bucket su entrambe le griglie.

Fasi

1. Utilizzando il tenant Manager sulla griglia di origine, "creare le proprie chiavi di accesso" e scaricare `.csv` file.
2. Nella parte superiore di Tenant Manager, selezionare l'icona della guida e selezionare **documentazione API**.
3. Nella sezione **s3**, selezionare il seguente endpoint:

   ```
   POST /org/users/current-user/replicate-s3-access-key
   ```

4. Selezionare **Provalo**.
5. Nella casella di testo **body**, sostituire le voci di esempio per **accessKey** e **secretAccessKey** con i valori del file **.csv** scaricato.

   Assicurarsi di conservare le virgolette doppie intorno a ciascuna stringa.

6. Se la chiave scade, sostituire la voce di esempio **Expires** con la data e l'ora di scadenza come stringa nel formato data-time ISO 8601 (ad esempio, `2024-02-28T22:46:33-08:00`). Se la chiave non scade, inserire **Null** come valore per la voce **Expires** (oppure rimuovere la riga **Expires** e la virgola precedente).
7. Selezionare **Esegui**.
8. Verificare che il codice di risposta del server sia **204**, a indicare che la chiave è stata clonata correttamente nella griglia di destinazione.

Clonare le chiavi di accesso di un altro utente

È possibile clonare le chiavi di accesso di un altro utente se è necessario accedere agli stessi bucket su entrambe le griglie.

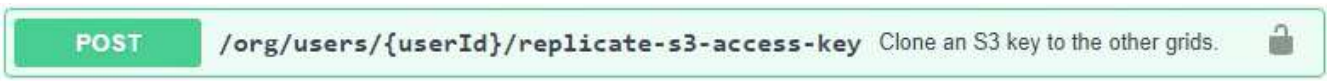
Fasi

1. Utilizzando il tenant Manager sulla griglia di origine, "Creare le chiavi di accesso S3 dell'altro utente" e scaricare `.csv` file.
2. Nella parte superiore di Tenant Manager, selezionare l'icona della guida e selezionare **documentazione API**.
3. Ottenere l'ID utente. Questo valore è necessario per clonare le chiavi di accesso degli altri utenti.
   a. Nella sezione **users**, selezionare il seguente endpoint:

      `GET /org/users`

   b. Selezionare **Provalo**.
   c. Specificare i parametri da utilizzare per la ricerca degli utenti.
   d. Selezionare **Esegui**.
   e. Individuare l'utente di cui si desidera clonare le chiavi e copiare il numero nel campo **id**.
4. Nella sezione **s3**, selezionare il seguente endpoint:

   `POST /org/users/{userId}/replicate-s3-access-key`



5. Selezionare **Provalo**.

6. Nella casella di testo **ID utente**, incollare l'ID utente copiato.
7. Nella casella di testo **body**, sostituire le voci di esempio **example access key** e **secret access key** con i valori del file **.csv** dell'utente.

   Assicurarsi di conservare le virgolette doppie intorno alla stringa.

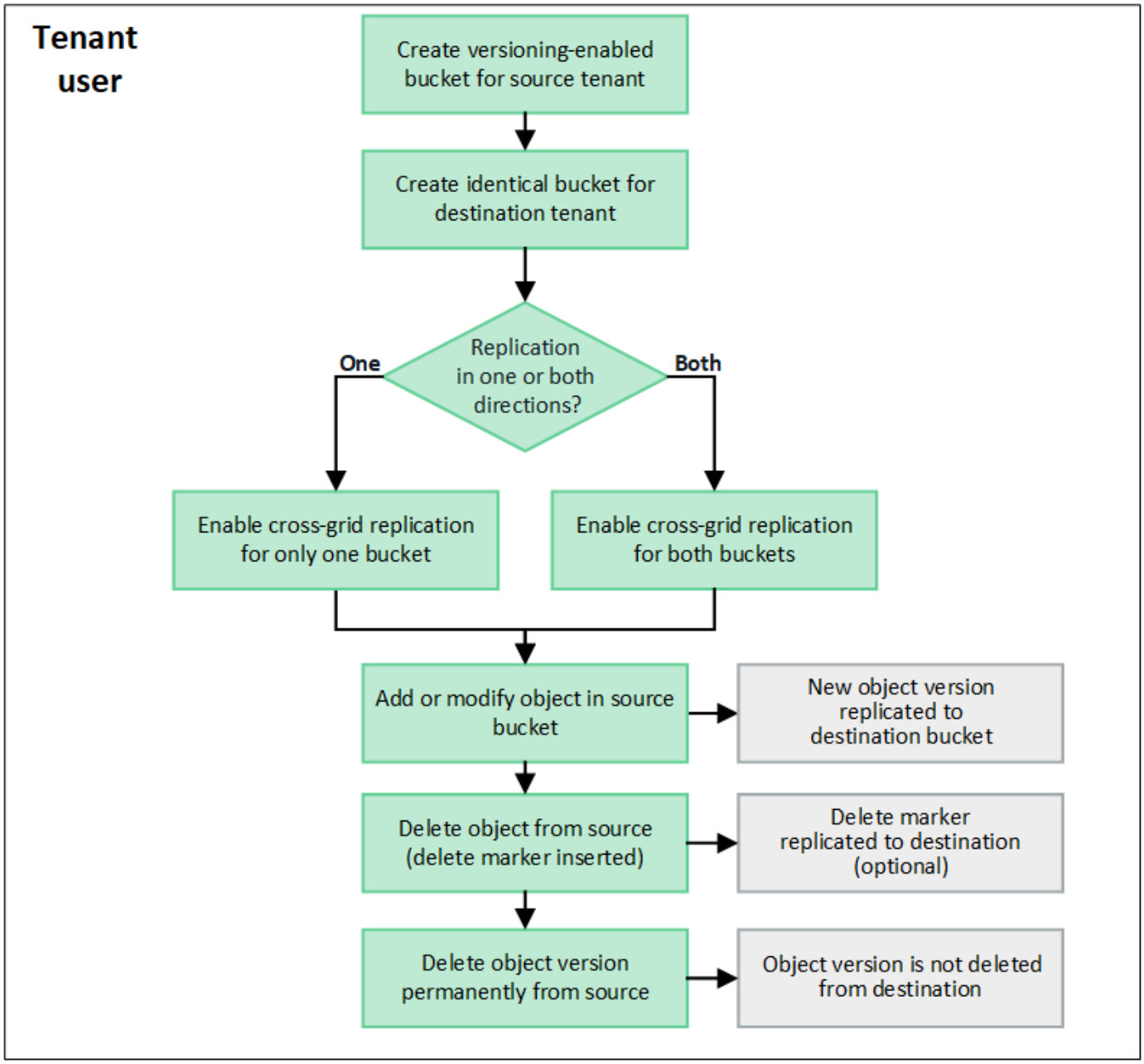
8. Se la chiave scade, sostituire la voce di esempio **Expires** con la data e l'ora di scadenza come stringa nel formato data-time ISO 8601 (ad esempio, `2023-02-28T22:46:33-08:00`). Se la chiave non scade, inserire **Null** come valore per la voce **Expires** (oppure rimuovere la riga **Expires** e la virgola precedente).
9. Selezionare **Esegui**.
10. Verificare che il codice di risposta del server sia **204**, a indicare che la chiave è stata clonata correttamente nella griglia di destinazione.

Gestire la replica cross-grid

Se all'account tenant è stata assegnata l'autorizzazione **Usa connessione federazione griglia** al momento della creazione, è possibile utilizzare la replica cross-grid per replicare automaticamente gli oggetti tra i bucket nella griglia di origine del tenant e i bucket nella griglia di destinazione del tenant. La replica cross-grid può avvenire in una o entrambe le direzioni.

Workflow per la replica cross-grid

Il diagramma del flusso di lavoro riassume i passaggi da eseguire per configurare la replica cross-grid tra bucket su due grid. Di seguito sono descritte in dettaglio le fasi descritte.



Configurare la replica cross-grid

Prima di poter utilizzare la replica cross-grid, è necessario accedere agli account tenant corrispondenti su ogni grid e creare bucket identici. Quindi, è possibile attivare la replica cross-grid su uno o entrambi i bucket.

Prima di iniziare

- Hai esaminato i requisiti per la replica cross-grid. Vedere "Che cos'è la replica cross-grid".
- Si sta utilizzando un "browser web supportato".
- L'account tenant dispone dell'autorizzazione **use grid Federation Connection** e su entrambe le griglie sono presenti account tenant identici. Vedere "Gestire i tenant consentiti per la connessione a federazione di grid".
- L'utente tenant che si sta effettuando l'accesso esiste già su entrambe le griglie e appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".
- Se si accede alla griglia di destinazione del tenant come utente locale, l'utente root dell'account tenant ha

impostato una password per l'account utente su tale griglia.

Creare due bucket identici

Come primo passo, accedi ai corrispondenti account tenant su ogni griglia e crea bucket identici.

Fasi

1. A partire da una delle due griglie della connessione a federazione di griglie, creare un nuovo bucket:
   a. Accedere all'account tenant utilizzando le credenziali di un utente tenant presente in entrambe le griglie.

      Se non si riesce ad accedere alla griglia di destinazione del tenant come utente locale, verificare che l'utente root dell'account tenant abbia impostato una password per l'account utente.

   b. Seguire le istruzioni da a. "Creare un bucket S3".
   c. Nella scheda **Manage object settings** (Gestisci impostazioni oggetto), selezionare **Enable object versioning** (attiva versione oggetto).
   d. Se il blocco oggetti S3 è attivato per il sistema StorageGRID, non attivare il blocco oggetti S3 per il bucket.
   e. Selezionare **Crea bucket**.
   f. Selezionare **fine**.
2. Ripetere questi passaggi per creare un bucket identico per lo stesso account tenant sull'altra griglia nella connessione della federazione di griglie.

   Secondo necessità, ogni benna può utilizzare una regione diversa.

Abilitare la replica cross-grid

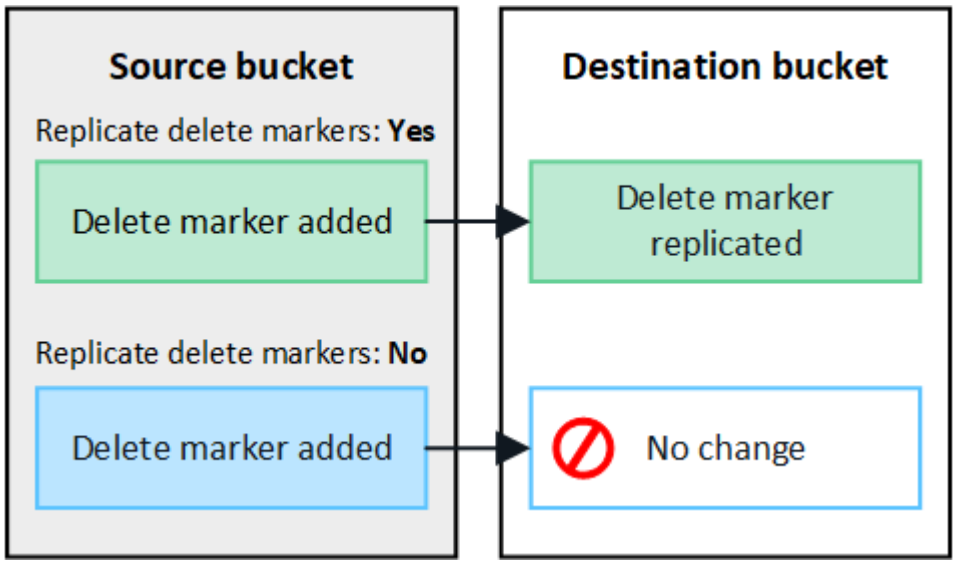
È necessario eseguire questi passaggi prima di aggiungere oggetti a uno dei bucket.

Fasi

1. A partire da una griglia di cui si desidera replicare gli oggetti, attivare "replica cross-grid in un'unica direzione":
   a. Accedi all'account tenant per il bucket.
   b. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
   c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
   d. Selezionare la scheda **Cross-grid Replication**.
   e. Selezionare **Enable** (attiva) ed esaminare l'elenco dei requisiti.
   f. Se tutti i requisiti sono stati soddisfatti, selezionare la connessione a federazione di griglia che si desidera utilizzare.
   g. Facoltativamente, modificare l'impostazione di **Replicate delete markers** per determinare cosa accade nella griglia di destinazione se un client S3 invia una richiesta di eliminazione alla griglia di origine che non include un ID di versione:
      - **Sì** (impostazione predefinita): Un marcatore di eliminazione viene aggiunto al bucket di origine e

replicato nel bucket di destinazione.

- **No**: Un marcatore di eliminazione viene aggiunto al bucket di origine ma non viene replicato nel bucket di destinazione.



> Se la richiesta di eliminazione include un ID di versione, la versione dell'oggetto viene rimossa in modo permanente dal bucket di origine. StorageGRID non replica le richieste di eliminazione che includono un ID di versione, pertanto la stessa versione dell'oggetto non viene eliminata dalla destinazione.

Vedere "Che cos'è la replica cross-grid" per ulteriori informazioni.

a. In alternativa, modificare l'impostazione della categoria di controllo **Cross-Grid Replication** per gestire il volume dei messaggi di controllo:
   - **Errore** (impostazione predefinita): Solo le richieste di replica cross-grid non riuscite sono incluse nell'output di controllo.
   - **Normale**: Sono incluse tutte le richieste di replica cross-grid, il che aumenta significativamente il volume dell'output di controllo.

b. Rivedere le selezioni. Non è possibile modificare queste impostazioni a meno che entrambi i bucket non siano vuoti.

c. Selezionare **Enable (attiva) e test**.

   Dopo alcuni istanti, viene visualizzato un messaggio di successo. Gli oggetti aggiunti a questo bucket verranno replicati automaticamente nell'altra griglia. **La replica cross-grid** viene visualizzata come funzione abilitata nella pagina dei dettagli del bucket.

2. In alternativa, passare al bucket corrispondente sull'altra griglia e. "abilitare la replica cross-grid in entrambe le direzioni".

Test di replica tra griglie

Se la replica cross-grid è attivata per un bucket, potrebbe essere necessario verificare che la connessione e la replica cross-grid funzionino correttamente e che i bucket di origine e di destinazione soddisfino ancora tutti i requisiti (ad esempio, il controllo delle versioni è ancora attivato).

Prima di iniziare

- Si sta utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".

Fasi

1. Accedi all'account tenant per il bucket.
2. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
3. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
4. Selezionare la scheda **Cross-grid Replication**.
5. Selezionare **Test di connessione**.

   Se la connessione è in buone condizioni, viene visualizzato un banner di successo. In caso contrario, viene visualizzato un messaggio di errore che l'utente e l'amministratore della griglia possono utilizzare per risolvere il problema. Per ulteriori informazioni, vedere "Risolvere i problemi relativi agli errori di federazione della griglia".

6. Se la replica cross-grid è configurata per avvenire in entrambe le direzioni, passare al bucket corrispondente sull'altra griglia e selezionare **Test Connection** per verificare che la replica cross-grid funzioni nell'altra direzione.

Disattiva la replica cross-grid

Se non si desidera più copiare gli oggetti nell'altra griglia, è possibile interrompere in modo permanente la replica tra griglie.

Prima di disattivare la replica cross-grid, tenere presente quanto segue:

- La disattivazione della replica cross-grid non rimuove gli oggetti che sono già stati copiati tra le griglie. Ad esempio, oggetti in `my-bucket` Sulla griglia 1 che sono state copiate in `my-bucket` Sulla griglia 2 non vengono rimossi se si disattiva la replica cross-grid per quel bucket. Se si desidera eliminare questi oggetti, è necessario rimuoverli manualmente.
- Se la replica cross-grid è stata attivata per ciascuno dei bucket (ovvero, se la replica si verifica in entrambe le direzioni), è possibile disattivare la replica cross-grid per uno o entrambi i bucket. Ad esempio, è possibile disattivare la replica degli oggetti da `my-bucket` Sulla griglia 1 a. `my-bucket` Sulla griglia 2, continuando a replicare gli oggetti da `my-bucket` Sulla griglia 2 a. `my-bucket` Sulla griglia 1.
- È necessario disattivare la replica cross-grid prima di poter rimuovere l'autorizzazione di un tenant per utilizzare la connessione di federazione grid. Vedere "Gestire i tenant autorizzati".
- Se si disattiva la replica cross-grid per un bucket che contiene oggetti, non sarà possibile riabilitare la replica cross-grid a meno che non si eliminino tutti gli oggetti dai bucket di origine e di destinazione.

  Non è possibile riabilitare la replica a meno che entrambi i bucket non siano vuoti.

Prima di iniziare

- Si sta utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".

Fasi

1. Partendo dalla griglia di cui non si desidera più replicare gli oggetti, interrompere la replica cross-grid per il bucket:

a. Accedi all'account tenant per il bucket.
b. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
d. Selezionare la scheda **Cross-grid Replication**.
e. Selezionare **Disable Replication** (Disattiva replica).
f. Se si è certi di voler disattivare la replica cross-grid per questo bucket, digitare **Sì** nella casella di testo e selezionare **Disattiva**.

   Dopo alcuni istanti, viene visualizzato un messaggio di successo. I nuovi oggetti aggiunti a questo bucket non possono più essere replicati automaticamente nell'altra griglia. **La replica cross-grid** non viene più visualizzata come funzione abilitata nella pagina bucket.

2. Se la replica cross-grid è stata configurata per avvenire in entrambe le direzioni, passare al bucket corrispondente sull'altra griglia e interrompere la replica cross-grid nell'altra direzione.

Visualizza connessioni di federazione di griglie

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile visualizzare le connessioni consentite.

Prima di iniziare

- L'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**.
- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".

Fasi

1. Selezionare **STORAGE (S3)** > **Grid Federation Connections**.

   Viene visualizzata la pagina Grid Federation Connection (connessione federazione griglia) che include una tabella che riepiloga le seguenti informazioni:

Colonna	Descrizione
Nome della connessione	Le connessioni della federazione di griglie che il tenant dispone dell'autorizzazione per l'utilizzo.
Bucket con replica cross-grid	Per ogni connessione a federazione di grid, i bucket tenant con replica cross-grid attivata. Gli oggetti aggiunti a questi bucket verranno replicati nell'altra griglia della connessione.
Ultimo errore	Per ogni connessione a federazione di griglie, si verifica l'errore più recente, se presente, quando i dati venivano replicati nell'altra griglia. Vedere Eliminare l'ultimo errore.

2. Facoltativamente, selezionare un nome di bucket in "visualizza i dettagli del bucket".

Cancella l'ultimo errore

Nella colonna **ultimo errore** potrebbe essere visualizzato un errore per uno dei seguenti motivi:

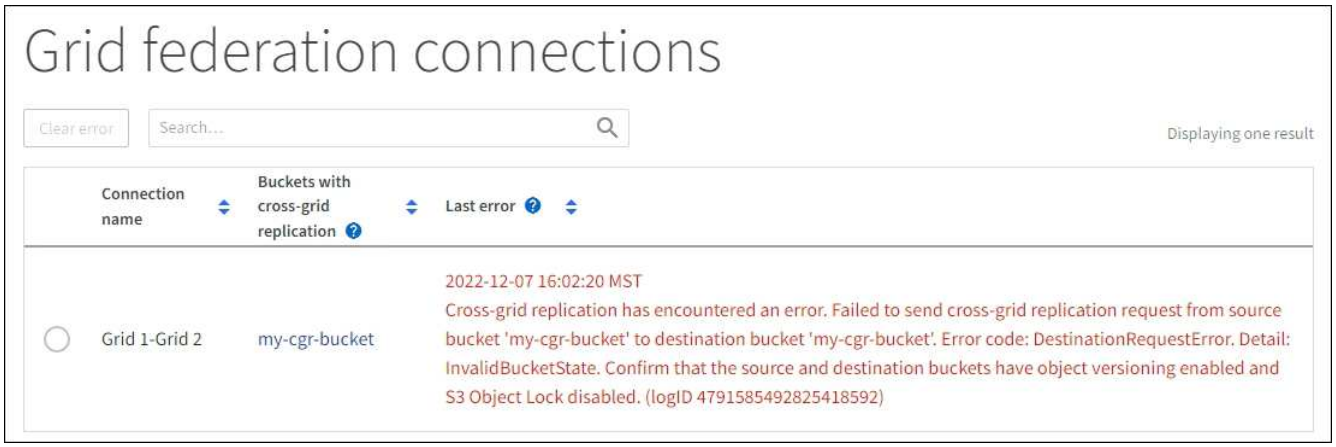
- Versione dell'oggetto di origine non trovata.
- Bucket di origine non trovato.
- Il bucket di destinazione è stato cancellato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il bucket di destinazione ha la versione sospesa.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più disponibile.

> In questa colonna viene visualizzato solo l'ultimo errore di replica tra griglie; gli errori precedenti che potrebbero essere stati rilevati non verranno visualizzati.

Fasi

1. Se nella colonna **ultimo errore** viene visualizzato un messaggio, visualizzare il testo del messaggio.

   Ad esempio, questo errore indica che il bucket di destinazione per la replica cross-grid era in uno stato non valido, probabilmente perché il controllo delle versioni era stato sospeso o S3 Object Lock era attivato.



2. Eseguire le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso nel bucket di destinazione per la replica cross-grid, riabilitare il controllo delle versioni per quel bucket.
3. Selezionare la connessione dalla tabella.
4. Selezionare **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.

   > Per assicurarsi che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo l'indicazione dell'ora nel messaggio prima di acquisire un nuovo oggetto.

7. Per determinare se non è stato possibile replicare oggetti a causa dell'errore del bucket, vedere "Identificare e riprovare le operazioni di replica non riuscite".

Gestire gruppi e utenti

USA la federazione delle identità

L'utilizzo della federazione delle identità rende più rapida la configurazione di gruppi e utenti tenant e consente agli utenti tenant di accedere all'account tenant utilizzando credenziali familiari.

Configurare la federazione delle identità per Tenant Manager

È possibile configurare la federazione delle identità per il tenant Manager se si desidera che i gruppi e gli utenti tenant vengano gestiti in un altro sistema, ad esempio Active Directory, Azure Active Directory (Azure ad), OpenLDAP o Oracle Directory Server.

Prima di iniziare

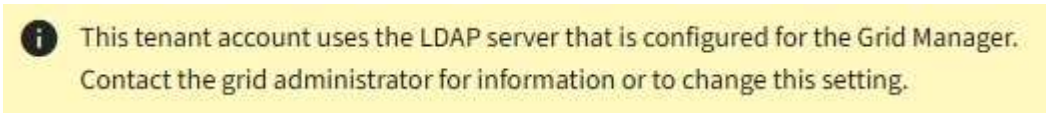
- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".
- Si utilizza Active Directory, Azure ad, OpenLDAP o Oracle Directory Server come provider di identità.

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

- Se si intende utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere Linee guida per la configurazione del server OpenLDAP.
- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità deve utilizzare TLS 1.2 o 1.3. Vedere "Crittografia supportata per le connessioni TLS in uscita".

A proposito di questa attività

La possibilità di configurare un servizio di federazione delle identità per il tenant dipende dalla configurazione dell'account tenant. Il tenant potrebbe condividere il servizio di federazione delle identità configurato per Grid Manager. Se viene visualizzato questo messaggio quando si accede alla pagina Identity Federation, non è possibile configurare un'origine di identità federata separata per questo tenant.

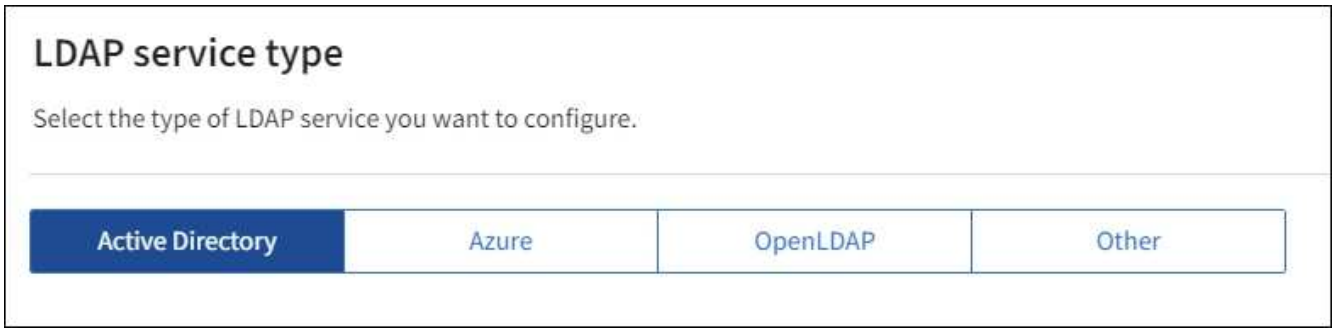


Inserire la configurazione

Quando si configura Identify Federation, vengono forniti i valori necessari a StorageGRID per connettersi a un servizio LDAP.

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Identity Federation**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).
3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.



Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP. In caso contrario, passare alla fase successiva.
   - **User Unique Name** (Nome univoco utente): Il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a. `sAMAccountName` Per Active Directory e. `uid` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
   - **UUID utente**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a. `objectGUID` Per Active Directory e. `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Ogni valore dell'utente per l'attributo specificato deve essere un numero esadecimale a 32 cifre in formato a 16 byte o stringa, dove i trattini vengono ignorati.
   - **Group Unique Name** (Nome univoco gruppo): Il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a. `sAMAccountName` Per Active Directory e. `cn` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
   - **UUID gruppo**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a. `objectGUID` Per Active Directory e. `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale a 32 cifre nel formato a 16 byte o stringa, dove i trattini vengono ignorati.
5. Per tutti i tipi di servizio LDAP, inserire le informazioni richieste relative al server LDAP e alla connessione di rete nella sezione Configura server LDAP.
   - **Nome host**: Il nome di dominio completo (FQDN) o l'indirizzo IP del server LDAP.
   - **Port** (porta): Porta utilizzata per la connessione al server LDAP.

     La porta predefinita per STARTTLS è 389 e la porta predefinita per LDAPS è 636. Tuttavia, è possibile utilizzare qualsiasi porta purché il firewall sia configurato correttamente.

   - **Username**: Percorso completo del nome distinto (DN) per l'utente che si connette al server LDAP.

     Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome principale dell'utente.

     L'utente specificato deve disporre dell'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

     - `sAMAccountName` oppure `uid`
     - `objectGUID`, `entryUUID`, o. `nsuniqueid`

- `cn`
- `memberOf` oppure `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, e. `userPrincipalName`
- **Azure**: `accountEnabled` e. `userPrincipalName`

◦ **Password**: La password associata al nome utente.

> Se si modifica la password in futuro, è necessario aggiornarla in questa pagina.

◦ **DN base gruppo**: Il percorso completo del nome distinto (DN) per una sottostruttura LDAP che si desidera cercare gruppi. Nell'esempio di Active Directory (riportato di seguito), tutti i gruppi il cui nome distinto è relativo al DN di base (DC=storagegrid,DC=example,DC=com) possono essere utilizzati come gruppi federati.

> I valori **Group unique name** devono essere univoci all'interno del **Group base DN** a cui appartengono.

◦ **User base DN**: Percorso completo del nome distinto (DN) di una sottostruttura LDAP che si desidera cercare gli utenti.

> I valori **Nome univoco utente** devono essere univoci all'interno del **DN base utente** a cui appartengono.

◦ **Bind username format** (opzionale): Il modello di nome utente predefinito che StorageGRID deve utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il formato **bind username** perché può consentire agli utenti di accedere se StorageGRID non è in grado di collegarsi con l'account del servizio.

Immettere uno di questi modelli:

- **Modello UserPrincipalName (Active Directory e Azure)**: `[USERNAME]@*example*.com`
- **Modello di nome di accesso di livello inferiore (Active Directory e Azure)**: `*example*\[USERNAME]`
- **Modello nome distinto**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Includi **[NOME UTENTE]** esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), selezionare un'impostazione di protezione.
   ◦ **Usa STARTTLS**: Utilizza STARTTLS per proteggere le comunicazioni con il server LDAP. Si tratta dell'opzione consigliata per Active Directory, OpenLDAP o altro, ma questa opzione non è supportata per Azure.
   ◦ **Usa LDAPS**: L'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. Selezionare questa opzione per Azure.
   ◦ **Non utilizzare TLS**: Il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Azure.

L'utilizzo dell'opzione **non utilizzare TLS** non è supportato se il server Active Directory applica la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

7. Se si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.
   - **Usa certificato CA del sistema operativo**: Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
   - **Usa certificato CA personalizzato**: Utilizza un certificato di protezione personalizzato.

     Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

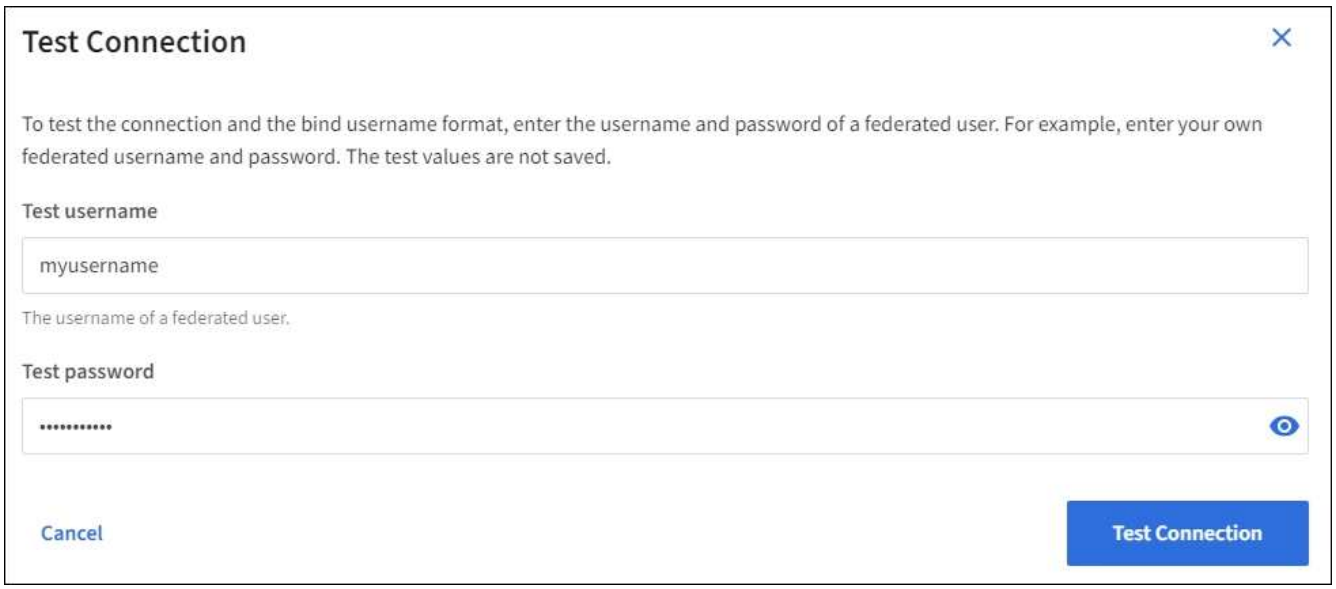
Verificare la connessione e salvare la configurazione

Dopo aver inserito tutti i valori, è necessario verificare la connessione prima di salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente BIND, se fornito.

Fasi

1. Selezionare **Test di connessione**.
2. Se non è stato fornito un formato nome utente BIND:
   - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.
   - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". Selezionare **Chiudi**. Quindi, risolvere eventuali problemi e verificare nuovamente la connessione.
3. Se è stato fornito un formato BIND Username, inserire il nome utente e la password di un utente federato valido.

   Ad esempio, inserire il proprio nome utente e la propria password. Non includere caratteri speciali nel nome utente, ad esempio @ o /.



   - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.

- Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente BIND o il nome utente e la password di prova non sono validi. Risolvere eventuali problemi e verificare nuovamente la connessione.

Forzare la sincronizzazione con l'origine dell'identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dall'origine dell'identità. È possibile forzare l'avvio della sincronizzazione se si desidera attivare o limitare le autorizzazioni utente il più rapidamente possibile.

Fasi

1. Vai alla pagina Identity Federation.
2. Selezionare **Sync server** nella parte superiore della pagina.

   Il processo di sincronizzazione potrebbe richiedere del tempo a seconda dell'ambiente in uso.

   L'avviso **errore di sincronizzazione federazione identità** viene attivato se si verifica un problema durante la sincronizzazione di utenti e gruppi federati dall'origine dell'identità.

Disattiva la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione di identità per gruppi e utenti. Quando la federazione delle identità è disattivata, non vi è alcuna comunicazione tra StorageGRID e l'origine delle identità. Tuttavia, tutte le impostazioni configurate vengono conservate, consentendo di riabilitare facilmente la federazione delle identità in futuro.

A proposito di questa attività

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non viene eseguita e non vengono generati avvisi o allarmi per gli account che non sono stati sincronizzati.
- La casella di controllo **Enable Identity Federation** (attiva federazione identità) è disattivata se Single Sign-on (SSO) è impostato su **Enabled** o **Sandbox Mode**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabled** prima di poter disattivare la federazione delle identità. Vedere "Disattiva single sign-on".

Fasi

1. Vai alla pagina Identity Federation.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).

Linee guida per la configurazione del server OpenLDAP

Se si desidera utilizzare un server OpenLDAP per la federazione delle identità, è necessario configurare impostazioni specifiche sul server OpenLDAP.

Per le fonti di identità che non sono Active Directory o Azure, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare eventuali chiavi S3 per l'utente o rimuovere l'utente da tutti i gruppi.

MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo in
"Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4".

Indicizzazione

È necessario configurare i seguenti attributi OpenLDAP con le parole chiave di indice specificate:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Inoltre, assicurarsi che i campi indicati nella guida per Nome utente siano indicizzati per ottenere prestazioni ottimali.

Consultare le informazioni relative alla manutenzione dell'appartenenza al gruppo inverso nella sezione "Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4".

Gestire i gruppi di tenant

Creare gruppi per un tenant S3

È possibile gestire le autorizzazioni per i gruppi di utenti S3 importando gruppi federati o creando gruppi locali.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".
- Se si intende importare un gruppo federated, è possibile "federazione di identità configurata"e il gruppo federated esiste già nell'origine identità configurata.
- Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, hai esaminato il flusso di lavoro e le considerazioni per "clonazione di utenti e gruppi tenant"e hai effettuato l'accesso alla griglia di origine del tenant.

Accedere alla procedura guidata Crea gruppo

Come prima fase, accedere alla procedura guidata Crea gruppo.

Fasi

1. Selezionare **GESTIONE ACCESSI** > **gruppi**.
2. Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, verificare che venga visualizzato un banner blu che indica che i nuovi gruppi creati in questa griglia verranno clonati nello stesso tenant nell'altra griglia della connessione. Se questo banner non viene visualizzato, potresti aver effettuato l'accesso alla griglia di destinazione del tenant.

3. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federated.

Fasi

1. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda **Federated group** (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

   Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti appartenenti a gruppi locali non potranno accedere a Gestione tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni di gruppo.

2. Inserire il nome del gruppo.
   - **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.

     Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, si verificherà un errore di clonazione se lo stesso **nome univoco** esiste già per il tenant nella griglia di destinazione.

   - **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.
3. Selezionare **continua**.

Gestire le autorizzazioni di gruppo

Le autorizzazioni di gruppo controllano le attività che gli utenti possono eseguire nelle API di gestione tenant e tenant Manager.

Fasi

1. Per la modalità **Access**, selezionare una delle seguenti opzioni:
   - **Read-write** (valore predefinito): Gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.

- **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API di gestione tenant Manager o tenant. Gli utenti locali di sola lettura possono modificare le proprie password.

> Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

2. Selezionare una o più autorizzazioni per questo gruppo.

   Vedere "Permessi di gestione del tenant".

3. Selezionare **continua**.

Impostare i criteri di gruppo S3

I criteri di gruppo determinano le autorizzazioni di accesso S3 che gli utenti avranno.

Fasi

1. Selezionare il criterio che si desidera utilizzare per questo gruppo.

Policy di gruppo	Descrizione
Nessun accesso S3	Predefinito. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non sia concesso con una policy bucket. Se si seleziona questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
Accesso in sola lettura	Gli utenti di questo gruppo hanno accesso in sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile modificare questa stringa.
Accesso completo	Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo ad accesso completo. Impossibile modificare questa stringa.
Riduzione del ransomware	Questo criterio di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti. Gli utenti di tenant Manager che dispongono dell'autorizzazione **Gestisci tutti i bucket** possono eseguire l'override di questa policy di gruppo. Limitare l'autorizzazione Manage All bucket (Gestisci tutti i bucket) agli utenti attendibili e utilizzare l'autenticazione multifattore (MFA), se disponibile.

Policy di gruppo	Descrizione
Personalizzato	Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

2. Se si seleziona **Custom**, inserire il criterio di gruppo. Ogni policy di gruppo ha un limite di dimensione di 5,120 byte. Immettere una stringa valida formattata con JSON.

   Per informazioni dettagliate sui criteri di gruppo, inclusa la sintassi del linguaggio e gli esempi, vedere "Criteri di gruppo di esempio".

3. Se si sta creando un gruppo locale, selezionare **continua**. Se si sta creando un gruppo federated, selezionare **Crea gruppo** e **fine**.

Aggiunta di utenti (solo gruppi locali)

È possibile salvare il gruppo senza aggiungere utenti oppure aggiungere utenti locali già esistenti.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, gli utenti selezionati quando si crea un gruppo locale nella griglia di origine non vengono inclusi quando il gruppo viene clonato nella griglia di destinazione. Per questo motivo, non selezionare gli utenti quando si crea il gruppo. Al momento della creazione degli utenti, selezionare il gruppo.

Fasi

1. Facoltativamente, selezionare uno o più utenti locali per questo gruppo.
2. Selezionare **Crea gruppo** e **fine**.

   Il gruppo creato viene visualizzato nell'elenco dei gruppi.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ci si trova nella griglia di origine del tenant, il nuovo gruppo viene clonato nella griglia di destinazione del tenant. **Success** viene visualizzato come **Cloning status** nella sezione Overview della pagina dei dettagli del gruppo.

Creare gruppi per un tenant Swift

È possibile gestire le autorizzazioni di accesso per un account tenant Swift importando gruppi federati o creando gruppi locali. Almeno un gruppo deve disporre dell'autorizzazione Swift Administrator, necessaria per gestire i container e gli oggetti per un account tenant Swift.

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

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".
- Se si intende importare un gruppo federated, è possibile "federazione di identità configurata"e il gruppo federated esiste già nell'origine identità configurata.

Accedere alla procedura guidata Crea gruppo

Fasi

Come prima fase, accedere alla procedura guidata Crea gruppo.

1. Selezionare **GESTIONE ACCESSI** > **gruppi**.
2. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federated.

Fasi

1. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda **Federated group** (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

   Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti appartenenti a gruppi locali non potranno accedere a Gestione tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni di gruppo.

2. Inserire il nome del gruppo.
   - **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.
   - **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.
3. Selezionare **continua**.

Gestire le autorizzazioni di gruppo

Le autorizzazioni di gruppo controllano le attività che gli utenti possono eseguire nelle API di gestione tenant e tenant Manager.

Fasi

1. Per la modalità **Access**, selezionare una delle seguenti opzioni:
   - **Read-write** (valore predefinito): Gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
   - **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API di gestione tenant Manager o tenant. Gli utenti locali di sola lettura possono modificare le proprie password.

     Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

2. Selezionare la casella di controllo **Root access** se gli utenti del gruppo devono accedere all'API di gestione tenant o tenant Manager.
3. Selezionare **continua**.

Impostare i criteri di gruppo di Swift

Gli utenti Swift hanno bisogno dell'autorizzazione di amministratore per autenticarsi nell'API SWIFT REST per creare container e acquisire oggetti.

1. Selezionare la casella di controllo **Swift Administrator** se gli utenti del gruppo devono utilizzare l'API SWIFT REST per gestire container e oggetti.
2. Se si sta creando un gruppo locale, selezionare **continua**. Se si sta creando un gruppo federated, selezionare **Crea gruppo** e **fine**.

Aggiunta di utenti (solo gruppi locali)

È possibile salvare il gruppo senza aggiungere utenti oppure aggiungere utenti locali già esistenti.

Fasi

1. Facoltativamente, selezionare uno o più utenti locali per questo gruppo.

   Se non sono ancora stati creati utenti locali, è possibile aggiungere questo gruppo all'utente nella pagina utenti. Vedere "Gestire gli utenti locali".

2. Selezionare **Crea gruppo** e **fine**.

   Il gruppo creato viene visualizzato nell'elenco dei gruppi.

Permessi di gestione del tenant

Prima di creare un gruppo tenant, prendere in considerazione le autorizzazioni che si desidera assegnare a tale gruppo. Le autorizzazioni di gestione del tenant determinano le attività che gli utenti possono eseguire utilizzando il tenant Manager o l'API di gestione del tenant. Un utente può appartenere a uno o più gruppi. Le autorizzazioni sono cumulative se un utente appartiene a più gruppi.

Per accedere a tenant Manager o utilizzare l'API di gestione tenant, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono accedere possono eseguire le seguenti operazioni:

- Visualizza la dashboard
- Modificare la propria password (per gli utenti locali)

Per tutte le autorizzazioni, l'impostazione della modalità di accesso del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni o se possono visualizzare solo le relative impostazioni e funzionalità.

> Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

È possibile assegnare a un gruppo le seguenti autorizzazioni. Tenere presente che i tenant S3 e Swift dispongono di permessi di gruppo diversi.

Permesso	Descrizione	Dettagli
Accesso root	Fornisce l'accesso completo al tenant Manager e all'API di gestione del tenant.	Gli utenti Swift devono disporre dell'autorizzazione di accesso root per accedere all'account tenant.
Amministratore	Solo tenant Swift. Fornisce l'accesso completo ai container e agli oggetti Swift per questo account tenant	Gli utenti Swift devono disporre dell'autorizzazione di amministratore Swift per eseguire qualsiasi operazione con l'API REST Swift.
Gestisci le tue credenziali S3	Consente agli utenti di creare e rimuovere le proprie chiavi di accesso S3.	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu **STORAGE (S3)** > **My S3 access keys**.
Visualizza tutti i bucket	**S3 locatari**: Consente agli utenti di visualizzare tutte le configurazioni di bucket e bucket. **Tenant Swift**: Consente agli utenti Swift di visualizzare tutte le configurazioni di container e container utilizzando l'API di gestione dei tenant.	Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu **bucket**. Questa autorizzazione viene sostituita dall'autorizzazione Gestisci tutti i bucket. Non influisce sui criteri di gruppo o bucket S3 utilizzati dai client S3 o dalla console S3. È possibile assegnare questa autorizzazione solo ai gruppi Swift dall'API di gestione dei tenant. Non puoi assegnare questa autorizzazione ai gruppi Swift utilizzando il tenant Manager.
Gestire tutti i bucket	**S3 tenant**: Consente agli utenti di utilizzare Tenant Manager e l'API di gestione tenant per creare ed eliminare bucket S3 e gestire le impostazioni per tutti i bucket S3 nell'account tenant, indipendentemente dai criteri di bucket S3 o di gruppo. **Tenant Swift**: Consente agli utenti Swift di controllare la coerenza dei container Swift utilizzando l'API di gestione dei tenant.	Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu **bucket**. Questa autorizzazione sostituisce l'autorizzazione Visualizza tutti i bucket. Non influisce sui criteri di gruppo o bucket S3 utilizzati dai client S3 o dalla console S3. È possibile assegnare questa autorizzazione solo ai gruppi Swift dall'API di gestione dei tenant. Non puoi assegnare questa autorizzazione ai gruppi Swift utilizzando il tenant Manager.

Permesso	Descrizione	Dettagli
Gestire gli endpoint	Consente agli utenti di utilizzare il gestore tenant o l'API di gestione tenant per creare o modificare gli endpoint del servizio della piattaforma, che vengono utilizzati come destinazione per i servizi della piattaforma StorageGRID.	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu **Platform Services Endpoint**.
Utilizzare la scheda Console S3	Se combinato con l'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket, consente agli utenti di visualizzare e gestire gli oggetti dalla scheda Console S3 nella pagina dei dettagli di un bucket.	

Gestire i gruppi

Gestire i gruppi di tenant in base alle esigenze per visualizzare, modificare o duplicare un gruppo e altro ancora.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".

Visualizzare o modificare il gruppo

È possibile visualizzare e modificare le informazioni di base e i dettagli di ciascun gruppo.

Fasi

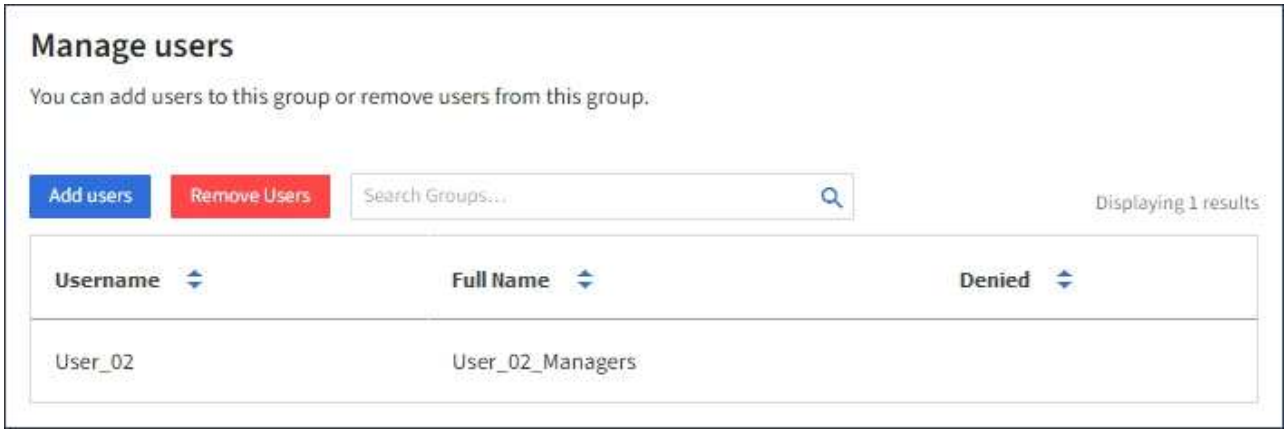
1. Selezionare **GESTIONE ACCESSI** > **gruppi**.
2. Consultare le informazioni fornite nella pagina gruppi, che elenca le informazioni di base per tutti i gruppi locali e federati per questo account tenant.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si stanno visualizzando i gruppi nella griglia di origine del tenant:

   - Un messaggio banner indica che se si modifica o si rimuove un gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
   - Se necessario, un messaggio di intestazione indica se i gruppi non sono stati clonati nel tenant sulla griglia di destinazione. È possibile riprovare a creare un clone di gruppo questo non è riuscito.
3. Se si desidera modificare il nome del gruppo:
   a. Selezionare la casella di controllo del gruppo.
   b. Selezionare **azioni** > **Modifica nome gruppo**.
   c. Inserire il nuovo nome.
   d. Selezionare **Salva modifiche.**
4. Se si desidera visualizzare ulteriori dettagli o apportare modifiche aggiuntive, effettuare una delle seguenti operazioni:

- Selezionare il nome del gruppo.
- Selezionare la casella di controllo relativa al gruppo e selezionare **azioni** > **Visualizza dettagli gruppo**.

5. Consultare la sezione Panoramica, che mostra le seguenti informazioni per ciascun gruppo:
   - Nome visualizzato
   - Nome univoco
   - Tipo
   - Modalità di accesso
   - Permessi
   - Policy S3
   - Numero di utenti in questo gruppo
   - Ulteriori campi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando il gruppo nella griglia di origine del tenant:
     - Stato di cloning, **Success** o **Failure**
     - Un banner blu che indica che se modifichi o elimini questo gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
6. Modificare le impostazioni di gruppo in base alle esigenze. Vedere "Creare gruppi per un tenant S3" e. "Creare gruppi per un tenant Swift" per informazioni dettagliate su cosa inserire.
   a. Nella sezione Panoramica, modificare il nome visualizzato selezionando il nome o l'icona di modifica .
   b. Nella scheda **permessi di gruppo**, aggiornare le autorizzazioni e selezionare **Salva modifiche**.
   c. Nella scheda **Criteri di gruppo**, apportare le modifiche desiderate e selezionare **Salva modifiche**.
      - Se si sta modificando un gruppo S3, è possibile selezionare un criterio di gruppo S3 diverso o inserire la stringa JSON per un criterio personalizzato, come richiesto.
      - Se si sta modificando un gruppo Swift, selezionare o deselezionare la casella di controllo **Swift Administrator**.
7. Per aggiungere uno o più utenti locali al gruppo:
   a. Selezionare la scheda Users (utenti).



   b. Selezionare **Aggiungi utenti**.
   c. Selezionare gli utenti che si desidera aggiungere e selezionare **Aggiungi utenti**.

In alto a destra viene visualizzato il messaggio Success (operazione riuscita).

8. Per rimuovere utenti locali dal gruppo:
   a. Selezionare la scheda Users (utenti).
   b. Selezionare **Rimuovi utenti**.
   c. Selezionare gli utenti che si desidera rimuovere e selezionare **Rimuovi utenti**.

   In alto a destra viene visualizzato il messaggio Success (operazione riuscita).

9. Confermare di aver selezionato **Save Changes** (Salva modifiche) per ciascuna sezione modificata.

Gruppo duplicato

È possibile duplicare un gruppo esistente per creare nuovi gruppi più rapidamente.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si duplica un gruppo dalla griglia di origine del tenant, il gruppo duplicato verrà clonato nella griglia di destinazione del tenant.

Fasi

1. Selezionare **GESTIONE ACCESSI** > **gruppi**.
2. Selezionare la casella di controllo del gruppo che si desidera duplicare.
3. Selezionare **azioni** > **Duplica gruppo**.
4. Vedere "Creare gruppi per un tenant S3" oppure "Creare gruppi per un tenant Swift" per informazioni dettagliate su cosa inserire.
5. Selezionare **Crea gruppo**.

Riprova clone di gruppo

Per riprovare un clone non riuscito:

1. Selezionare ciascun gruppo che indica *(clonazione non riuscita)* sotto il nome del gruppo.
2. Selezionare **azioni** > **Clona gruppi**.
3. Visualizzare lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun gruppo da clonare.

Per ulteriori informazioni, vedere "Clonare utenti e gruppi tenant".

Eliminare uno o più gruppi

È possibile eliminare uno o più gruppi. Gli utenti che appartengono solo a un gruppo cancellato non potranno più accedere al tenant manager o utilizzare l'account tenant.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si elimina un gruppo, StorageGRID non eliminerà il gruppo corrispondente sull'altra griglia. Se è necessario mantenere queste informazioni sincronizzate, è necessario eliminare lo stesso gruppo da entrambe le griglie.

Fasi

1. Selezionare **GESTIONE ACCESSI** > **gruppi**.

2. Selezionare la casella di controllo per ciascun gruppo che si desidera eliminare.
3. Selezionare **azioni** > **Elimina gruppo** o **azioni** > **Elimina gruppi**.

   Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Delete group** (Elimina gruppo) o **Delete groups** (Elimina gruppi).

Gestire gli utenti locali

È possibile creare utenti locali e assegnarli a gruppi locali per determinare le funzionalità a cui questi utenti possono accedere. Tenant Manager include un utente locale predefinito, denominato "root". Sebbene sia possibile aggiungere e rimuovere utenti locali, non è possibile rimuovere l'utente root.

> Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti locali non potranno accedere al Gestore tenant o all'API di gestione tenant, anche se possono utilizzare le applicazioni client per accedere alle risorse del tenant, in base alle autorizzazioni di gruppo.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".
- Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, hai esaminato il flusso di lavoro e le considerazioni per "clonazione di utenti e gruppi tenant"e hai effettuato l'accesso alla griglia di origine del tenant.

Crea un utente locale

È possibile creare un utente locale e assegnarlo a uno o più gruppi locali per controllarne le autorizzazioni di accesso.

Gli utenti S3 che non appartengono a nessun gruppo non dispongono di autorizzazioni di gestione o criteri di gruppo S3 applicati. Questi utenti potrebbero avere accesso al bucket S3 concesso tramite una policy bucket.

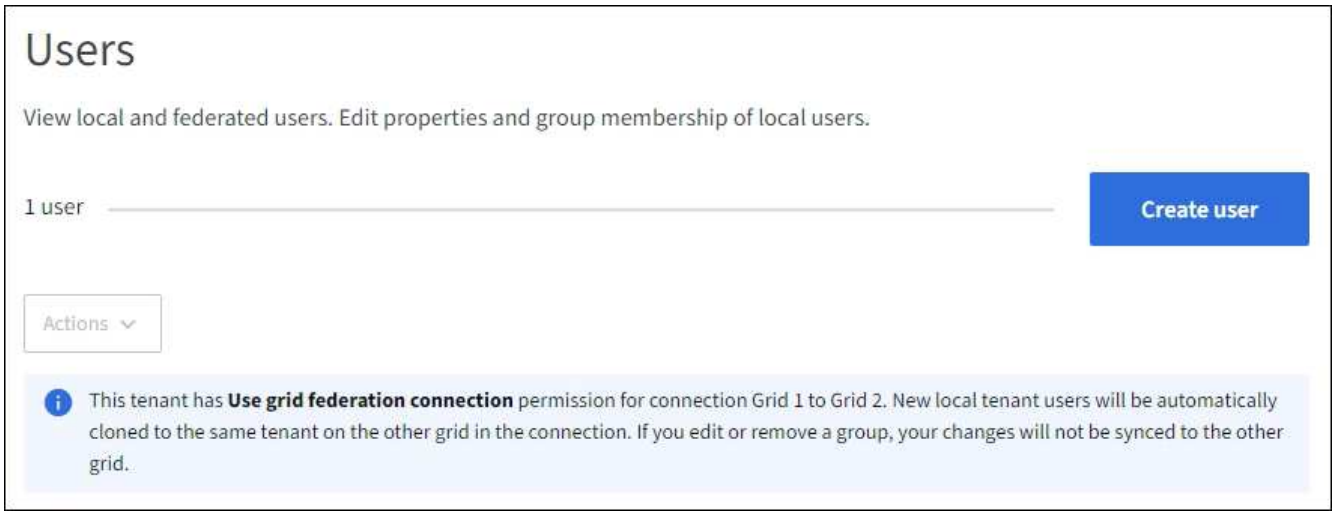
Gli utenti Swift che non appartengono a nessun gruppo non dispongono di autorizzazioni di gestione o di accesso a container Swift.

Accedere alla procedura guidata Crea utente

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Users**.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, un banner blu indica che si tratta della griglia di origine del tenant. Tutti gli utenti locali creati in questa griglia verranno clonati nell'altra griglia della connessione.



2. Selezionare **Crea utente**.

Immettere le credenziali

Fasi

1. Per il passo **inserire le credenziali utente**, completare i seguenti campi.

Campo	Descrizione
Nome completo	Il nome completo dell'utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
Nome utente	Il nome che l'utente utilizzerà per accedere. I nomi utente devono essere univoci e non possono essere modificati. **Nota**: Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, si verificherà un errore di clonazione se lo stesso **Nome utente** esiste già per il tenant nella griglia di destinazione.
Password e Conferma password	La password che l'utente utilizzerà inizialmente al momento dell'accesso.
Negare l'accesso	Selezionare **Sì** per impedire a questo utente di accedere all'account tenant, anche se potrebbe ancora appartenere a uno o più gruppi. Ad esempio, selezionare **Sì** per sospendere temporaneamente la possibilità di accesso dell'utente.

2. Selezionare **continua**.

Assegnare ai gruppi

Fasi

1. Assegnare l'utente a uno o più gruppi locali per determinare quali attività possono eseguire.

   L'assegnazione di un utente ai gruppi è facoltativa. Se preferisci, puoi selezionare gli utenti quando crei o

modifichi i gruppi.

Gli utenti che non appartengono a nessun gruppo non disporranno di autorizzazioni di gestione. Le autorizzazioni sono cumulative. Gli utenti disporranno di tutte le autorizzazioni per tutti i gruppi a cui appartengono. Vedere "Permessi di gestione del tenant".

2. Selezionare **Crea utente**.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ci si trova nella griglia di origine del tenant, il nuovo utente locale viene clonato nella griglia di destinazione del tenant. **Success** viene visualizzato come **Cloning status** nella sezione Overview della pagina dei dettagli dell'utente.

3. Selezionare **fine** per tornare alla pagina utenti.

Visualizzare o modificare l'utente locale

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Users**.
2. Consultare le informazioni fornite nella pagina utenti, che elenca le informazioni di base per tutti gli utenti locali e federati per questo account tenant.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando l'utente nella griglia di origine del tenant:

   - Un messaggio banner indica che se si modifica o si rimuove un utente, le modifiche non verranno sincronizzate con l'altra griglia.
   - Se necessario, un messaggio di intestazione indica se gli utenti non sono stati clonati nel tenant sulla griglia di destinazione. È possibile riprovare un clone utente non riuscito.

3. Se si desidera modificare il nome completo dell'utente:
   a. Selezionare la casella di controllo dell'utente.
   b. Selezionare **azioni** > **Modifica nome completo**.
   c. Inserire il nuovo nome.
   d. Selezionare **Salva modifiche.**
4. Se si desidera visualizzare ulteriori dettagli o apportare modifiche aggiuntive, effettuare una delle seguenti operazioni:
   - Selezionare il nome utente.
   - Selezionare la casella di controllo dell'utente e selezionare **azioni** > **Visualizza dettagli utente**.
5. Consultare la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:
   - Nome completo
   - Nome utente
   - Tipo di utente
   - Accesso negato
   - Modalità di accesso
   - Appartenenza al gruppo
   - Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione**

griglia e l'utente viene visualizzato nella griglia di origine del tenant:

- Stato di cloning, **Success** o **Failure**
- Un banner blu che indica che se modifichi questo utente, le modifiche non verranno sincronizzate con l'altra griglia.

6. Modificare le impostazioni utente in base alle esigenze. Vedere Creare un utente locale per informazioni dettagliate su cosa inserire.
   a. Nella sezione Panoramica, modificare il nome completo selezionando il nome o l'icona di modifica .

      Impossibile modificare il nome utente.

   b. Nella scheda **Password**, modificare la password dell'utente e selezionare **Salva modifiche**.
   c. Nella scheda **Access**, selezionare **No** per consentire all'utente di accedere o selezionare **Sì** per impedire all'utente di accedere. Quindi, selezionare **Save Changes** (Salva modifiche).
   d. Nella scheda **tasti di accesso**, selezionare **Crea chiave** e seguire le istruzioni per "Creazione delle chiavi di accesso S3 di un altro utente".
   e. Nella scheda **gruppi**, selezionare **Modifica gruppi** per aggiungere l'utente ai gruppi o rimuoverlo dai gruppi. Quindi, selezionare **Save Changes** (Salva modifiche).
7. Confermare di aver selezionato **Save Changes** (Salva modifiche) per ciascuna sezione modificata.

Utente locale duplicato

È possibile duplicare un utente locale per creare un nuovo utente più rapidamente.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si duplica un utente dalla griglia di origine del tenant, l'utente duplicato verrà clonato nella griglia di destinazione del tenant.

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Users**.
2. Selezionare la casella di controllo dell'utente che si desidera duplicare.
3. Selezionare **azioni** > **Duplica utente**.
4. Vedere Creare un utente locale per informazioni dettagliate su cosa inserire.
5. Selezionare **Crea utente**.

Riprova clone utente

Per riprovare un clone non riuscito:

1. Selezionare ogni utente che indica *(clonazione non riuscita)* sotto il nome utente.
2. Selezionare **azioni** > **Clona utenti**.
3. Visualizzare lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun utente che si sta clonando.

Per ulteriori informazioni, vedere "Clonare utenti e gruppi tenant".

Eliminare uno o più utenti locali

È possibile eliminare in modo permanente uno o più utenti locali che non hanno più bisogno di accedere all'account tenant StorageGRID.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si elimina un utente locale, StorageGRID non eliminerà l'utente corrispondente sull'altra griglia. Se è necessario mantenere queste informazioni sincronizzate, è necessario eliminare lo stesso utente da entrambe le griglie.

> Per eliminare gli utenti federati, è necessario utilizzare l'origine delle identità federate.

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Users**.
2. Selezionare la casella di controllo per ciascun utente che si desidera eliminare.
3. Selezionare **azioni** > **Elimina utente** o **azioni** > **Elimina utenti**.

   Viene visualizzata una finestra di dialogo di conferma.
4. Selezionare **Delete user** (Elimina utente) o **Delete users** (Elimina utenti).

Gestire le chiavi di accesso S3

Manage S3 access key (Gestisci tasti di accesso S3): Panoramica

Ogni utente di un account tenant S3 deve disporre di una chiave di accesso per memorizzare e recuperare oggetti nel sistema StorageGRID. Una chiave di accesso è costituita da un ID della chiave di accesso e da una chiave di accesso segreta.

Le chiavi di accesso S3 possono essere gestite come segue:

- Gli utenti che dispongono dell'autorizzazione **Gestisci le tue 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 e tutti gli altri utenti. Le chiavi di accesso root forniscono l'accesso completo a tutti i bucket e gli oggetti per il tenant, a meno che non siano esplicitamente disabilitate da una policy bucket.

StorageGRID supporta l'autenticazione Firma versione 2 e Firma versione 4. L'accesso multiaccount non è consentito a meno che non sia esplicitamente abilitato da una policy bucket.

Creare le proprie chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone dell'autorizzazione appropriata, è possibile creare le proprie chiavi di accesso S3. Per accedere ai bucket e agli oggetti, è necessario disporre di una chiave di accesso.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestisci le tue credenziali S3 o l'autorizzazione di accesso root".

A proposito di questa attività

È possibile creare una o più chiavi di accesso S3 che consentono di creare e gestire i bucket per l'account tenant. Dopo aver creato una nuova chiave di accesso, aggiornare l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quante ne hai bisogno ed eliminare le chiavi che non stai utilizzando. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

Ogni chiave può avere un tempo di scadenza specifico o nessuna scadenza. Seguire queste linee guida per la scadenza:

- Impostare una scadenza per le chiavi in modo da limitare l'accesso a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre il rischio in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio di sicurezza nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare un periodo di scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.

> È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **STORAGE (S3)** > **My access key**.

   Viene visualizzata la pagina My access keys (i miei tasti di accesso) che elenca tutti i tasti di accesso esistenti.

2. Selezionare **Crea chiave**.
3. Effettuare una delle seguenti operazioni:
   - Selezionare **non impostare una scadenza** per creare una chiave che non scadrà. (Impostazione predefinita)
   - Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.

     > La data di scadenza può essere un massimo di cinque anni dalla data corrente. La scadenza può essere di almeno un minuto dall'ora corrente.

4. Selezionare **Crea chiave di accesso**.

   Viene visualizzata la finestra di dialogo Download access key (Scarica chiave di accesso), in cui sono elencati l'ID della chiave di accesso e la chiave di accesso segreta.

5. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni. Una volta chiusa la finestra di dialogo, non è possibile copiare o scaricare le chiavi.

6. Selezionare **fine**.

   La nuova chiave è elencata nella pagina i miei tasti di accesso.

7. Se l'account tenant dispone dell'autorizzazione **use grid Federation Connection**, utilizzare facoltativamente l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedere "Clonare le chiavi di accesso S3 utilizzando l'API".

Visualizzare le chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone di "autorizzazione appropriata", È possibile visualizzare un elenco dei tasti di accesso S3. È possibile ordinare l'elenco in base alla data di scadenza, in modo da determinare quali chiavi scadranno a breve. In base alle esigenze, è possibile "creare nuove chiavi" oppure "eliminare le chiavi" che non stai più utilizzando.

È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone delle credenziali S3 Manage Your Own (Gestisci le tue credenziali S3) "permesso".

Fasi

1. Selezionare **STORAGE (S3)** > **My access key**.
2. Dalla pagina My access keys (i miei tasti di accesso), ordinare le chiavi di accesso esistenti in base a **Expiration Time** (ora di scadenza) o **Access key ID** (ID chiave di accesso).
3. Se necessario, creare nuove chiavi o eliminare le chiavi che non si stanno più utilizzando.

   Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, è possibile iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

   Le chiavi scadute vengono rimosse automaticamente.

Eliminare le proprie chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le proprie chiavi di accesso S3. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- Hai il "Gestisci le tue autorizzazioni per le credenziali S3".

> È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **STORAGE (S3)** > **My access key**.
2. Nella pagina i miei tasti di accesso, selezionare la casella di controllo per ciascun tasto di accesso che si desidera rimuovere.
3. Selezionare **Delete key** (Elimina chiave).
4. Nella finestra di dialogo di conferma, selezionare **Elimina tasto**.

   Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina.

Creare le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone dell'autorizzazione appropriata, è possibile creare chiavi di accesso S3 per altri utenti, ad esempio applicazioni che richiedono l'accesso a bucket e oggetti.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".

A proposito di questa attività

È possibile creare una o più chiavi di accesso S3 per altri utenti in modo che possano creare e gestire i bucket per il proprio account tenant. Dopo aver creato una nuova chiave di accesso, aggiornare l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quelle richieste dall'utente ed eliminare le chiavi che non vengono utilizzate. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

Ogni chiave può avere un tempo di scadenza specifico o nessuna scadenza. Seguire queste linee guida per la scadenza:

- Impostare una scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre i rischi in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio di protezione nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare un tempo di scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.

È possibile accedere ai bucket S3 e agli oggetti appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Users**.
2. Selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.

   Viene visualizzata la pagina User Detail (Dettagli utente).

3. Selezionare **Access keys**, quindi selezionare **Create key**.
4. Effettuare una delle seguenti operazioni:
   - Selezionare **non impostare un tempo di scadenza** per creare una chiave che non scade. (Impostazione predefinita)
   - Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.

     La data di scadenza può essere un massimo di cinque anni dalla data corrente. La scadenza può essere di almeno un minuto dall'ora corrente.

5. Selezionare **Crea chiave di accesso**.

   Viene visualizzata la finestra di dialogo Download access key (Scarica chiave di accesso), che elenca l'ID della chiave di accesso e la chiave di accesso segreta.

6. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni. Una volta chiusa la finestra di dialogo, non è possibile copiare o scaricare le chiavi.

7. Selezionare **fine**.

   La nuova chiave è elencata nella scheda Access Keys della pagina User Details (Dettagli utente).

8. Se l'account tenant dispone dell'autorizzazione **use grid Federation Connection**, utilizzare facoltativamente l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedere "Clonare le chiavi di accesso S3 utilizzando l'API".

Visualizzare le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile visualizzare le chiavi di accesso S3 di un altro utente. È possibile ordinare l'elenco in base all'ora di scadenza, in modo da determinare quali chiavi scadranno a breve. Se necessario, è possibile creare nuove chiavi ed eliminare chiavi che non sono più in uso.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

> È possibile accedere ai bucket S3 e agli oggetti appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Users**.
2. Nella pagina utenti, selezionare l'utente di cui si desidera visualizzare i tasti di accesso S3.
3. Nella pagina User details (Dettagli utente), selezionare **Access keys** (chiavi di accesso).
4. Ordinare le chiavi in base a **scadenza** o **ID chiave di accesso**.
5. Se necessario, creare nuove chiavi ed eliminare manualmente le chiavi che non sono più in uso.

   Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, l'utente può iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

   Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

"Creare le chiavi di accesso S3 di un altro utente"

"Eliminare le chiavi di accesso S3 di un altro utente"

Eliminare le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le chiavi di accesso S3 di un altro utente. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

> È possibile accedere ai bucket S3 e agli oggetti appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Users**.
2. Nella pagina utenti, selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.

3. Nella pagina Dettagli utente, selezionare **tasti di accesso**, quindi selezionare la casella di controllo per ciascun tasto di accesso
che si desidera eliminare.
4. Selezionare **azioni** > **Elimina tasto selezionato**.
5. Nella finestra di dialogo di conferma, selezionare **Elimina tasto**.

   Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina.

Gestire i bucket S3

Creare un bucket S3

È possibile utilizzare Tenant Manager per creare bucket S3 per i dati dell'oggetto.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone dell'accesso Root o di Manage All bucket (Gestisci tutti i bucket) "permesso". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

  > Le autorizzazioni per impostare o modificare le proprietà di blocco oggetti S3 di bucket o oggetti possono essere concesse da "policy bucket o policy di gruppo".

- Se si prevede di attivare il blocco oggetti S3 per un bucket, un amministratore della griglia ha attivato l'impostazione globale di blocco oggetti S3 per il sistema StorageGRID e sono stati esaminati i requisiti per i bucket e gli oggetti blocco oggetti S3. Vedere "USA il blocco oggetti S3 per conservare gli oggetti".

Accedere alla procedura guidata

Fasi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
2. Selezionare **Crea bucket**.

Inserire i dettagli

Fasi

1. Inserire i dettagli del bucket.

Campo	Descrizione
Nome bucket	Un nome per il bucket conforme alle seguenti regole: • Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). • Deve essere conforme al DNS. • Deve contenere almeno 3 e non più di 63 caratteri. • Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. • Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. Per ulteriori informazioni, consultare "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione del bucket". **Nota**: Non è possibile modificare il nome del bucket dopo averlo creato.
Regione	La regione del bucket. L'amministratore di StorageGRID gestisce le regioni disponibili. L'area di un bucket può influire sulla policy di protezione dei dati applicata agli oggetti. Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione. **Nota**: Non è possibile modificare l'area dopo aver creato il bucket.

2. Selezionare **continua**.

Gestire le impostazioni degli oggetti

Fasi

1. Facoltativamente, attivare il controllo della versione degli oggetti per il bucket.

   Abilitare la versione degli oggetti se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto in base alle esigenze. Se il bucket verrà utilizzato per la replica cross-grid, è necessario attivare il controllo delle versioni degli oggetti.

2. Se l'impostazione globale S3 Object Lock (blocco oggetti S3) è attivata, attivare facoltativamente S3 Object Lock (blocco oggetti S3) per memorizzare gli oggetti utilizzando un modello WORM (Write-Once-Read-Many).

   Attivare il blocco oggetti S3 per un bucket solo se è necessario mantenere gli oggetti per un periodo di tempo fisso, ad esempio per soddisfare determinati requisiti normativi. S3 Object Lock è un'impostazione permanente che consente di evitare l'eliminazione o la sovrascrittura degli oggetti per un periodo di tempo fisso o indefinito.

   > Una volta attivata l'impostazione S3 Object Lock per un bucket, non è possibile disattivarla. Chiunque disponga delle autorizzazioni corrette può aggiungere a questo bucket oggetti che non possono essere modificati. Potrebbe non essere possibile eliminare questi oggetti o il bucket stesso.

Se si attiva il blocco oggetti S3 per un bucket, il controllo della versione del bucket viene attivato automaticamente.

3. Se si seleziona **Enable S3 Object Lock** (attiva blocco oggetti S3), attivare facoltativamente **Default Retention** per questo bucket.

   Quando l'opzione **Default Retention** (conservazione predefinita) è attivata, i nuovi oggetti aggiunti al bucket saranno automaticamente protetti dall'eliminazione o dalla sovrascrittura. L'impostazione **Default Retention** non si applica agli oggetti che hanno periodi di conservazione propri.

   a. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare una **modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
Governance	• Utenti con `s3:BypassGovernanceRetention` l'autorizzazione può utilizzare `x-amz-bypass-governance-retention: true` richiedi intestazione per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

   b. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare il **Default Retention Period** (periodo di conservazione predefinito) per il bucket.

      Il **Default Retention Period** indica per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. Specificare un valore compreso tra 1 e 36,500 giorni o tra 1 e 100 anni, inclusi.

4. Selezionare **Crea bucket**.

   Il bucket viene creato e aggiunto alla tabella nella pagina Bucket.

5. Facoltativamente, selezionare **Vai alla pagina dei dettagli del bucket** a. "visualizza i dettagli del bucket" ed eseguire una configurazione aggiuntiva.

Visualizza i dettagli del bucket

È possibile visualizzare i bucket nell'account tenant.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione accesso root, Gestisci tutti i bucket o Visualizza tutti i bucket". Queste autorizzazioni hanno la precedenza sulle impostazioni di autorizzazione nei criteri di gruppo o bucket.

Fasi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.

   Viene visualizzata la pagina Bucket.

2. Rivedere le informazioni di riepilogo per ciascun bucket.

   In base alle esigenze, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco in avanti e indietro.

   I valori Object Count (Conteggio oggetti) e Space used (spazio utilizzato) visualizzati sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi. Se nei bucket è attivata la versione, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

Colonna	Descrizione
Nome	Il nome univoco del bucket, che non può essere modificato.
Funzionalità attivate	L'elenco delle funzioni attivate per il bucket.
Blocco oggetti S3	Se S3 Object Lock è attivato per il bucket. Questa colonna viene visualizzata solo se S3 Object Lock (blocco oggetti S3) è attivato per la griglia. Questa colonna mostra anche informazioni relative a qualsiasi bucket compatibile legacy.
Regione	La regione del bucket, che non può essere modificata.
Numero di oggetti	Il numero di oggetti in questo bucket. Quando gli oggetti vengono aggiunti o cancellati, questo valore potrebbe non essere aggiornato immediatamente. Se nei bucket è attivata la versione, le versioni degli oggetti non correnti vengono incluse in questo valore.
Spazio utilizzato	La dimensione logica di tutti gli oggetti nel bucket. La dimensione logica non include lo spazio effettivo richiesto per le copie replicate o codificate in cancellazione o per i metadati degli oggetti.
Data di creazione	La data e l'ora di creazione del bucket.

3. Per visualizzare i dettagli di un bucket specifico, selezionare il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket. Da questa pagina, è possibile eseguire le seguenti attività se si dispone delle autorizzazioni richieste:

- Configurare e gestire le opzioni bucket:
  - "Tag dei criteri ILM"
  - "Gestire la coerenza del bucket"
  - "Aggiornamenti dell'ora dell'ultimo accesso"
  - "Versione degli oggetti"
  - "Blocco oggetti S3"
  - "Ritenzione bucket predefinita"
- Configurare l'accesso al bucket, ad esempio "Condivisione delle risorse tra origini (CORS)"
- "Gestire i servizi della piattaforma" (Se consentito per il tenant), inclusa la replica di CloudMirror, le notifiche degli eventi e l'integrazione della ricerca
- Attivare e. "gestire la replica cross-grid" (Se consentito dal tenant) per replicare gli oggetti acquisiti in questo bucket in un altro sistema StorageGRID
- Accedere a. "S3 Console" per gestire gli oggetti nel bucket
- "Elimina tutti gli oggetti in un bucket"
- "Eliminare un bucket" questo è già vuoto

Applicare un tag di criterio ILM a un bucket

Scegli un tag di policy ILM da applicare a un bucket in base ai tuoi requisiti di storage a oggetti.

Il criterio ILM controlla la posizione di memorizzazione dei dati dell'oggetto e se vengono eliminati dopo un determinato periodo di tempo. L'amministratore di grid crea criteri ILM e li assegna ai tag dei criteri ILM quando si utilizzano più criteri attivi.

> Evitare di riassegnare frequentemente il tag di un bucket. In caso contrario, potrebbero verificarsi problemi di prestazioni.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione accesso root, Gestisci tutti i bucket o Visualizza tutti i bucket". Queste autorizzazioni hanno la precedenza sulle impostazioni di autorizzazione nei criteri di gruppo o bucket.

Fasi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.

   Viene visualizzata la pagina Bucket. In base alle esigenze, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco in avanti e indietro.

2. Selezionare il nome del bucket a cui si desidera assegnare un tag di criterio ILM.

   È inoltre possibile modificare l'assegnazione dei tag dei criteri ILM per un bucket a cui è già stato assegnato un tag.

I valori Object Count (Conteggio oggetti) e Space used (spazio utilizzato) visualizzati sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi. Se nei bucket è attivata la versione, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

3. Nella scheda Opzioni bucket, espandere il tag criterio ILM fisarmonica. Questa fisarmonica viene visualizzata solo se l'amministratore della griglia ha attivato l'uso di tag di criteri personalizzati.
4. Leggere la descrizione di ciascun tag di criterio per determinare quale tag applicare al bucket.

La modifica del tag di criterio ILM per un bucket attiva la rivalutazione ILM di tutti gli oggetti nel bucket. Se la nuova policy mantiene gli oggetti per un periodo di tempo limitato, gli oggetti meno recenti verranno eliminati.

5. Selezionare il pulsante di opzione per il tag che si desidera assegnare al bucket.
6. Selezionare **Save Changes** (Salva modifiche). Con la chiave, sulla benna viene impostata una nuova etichetta della benna S3 `NTAP-SG-ILM-BUCKET-TAG` E il valore del tag del criterio ILM.

Assicurarsi che le applicazioni S3 non sovrascrivano o eliminino accidentalmente la nuova etichetta del bucket. Se questo tag viene omesso quando si applica un nuovo TagSet al bucket, gli oggetti nel bucket torneranno a essere valutati in base al criterio ILM predefinito.

Impostare e modificare i tag dei criteri ILM utilizzando solo l'API di Tenant Manager o di Tenant Manager in cui il tag dei criteri ILM viene convalidato. Non modificare `NTAP-SG-ILM-BUCKET-TAG` Tag dei criteri ILM che utilizza l'API S3 PutBucketTagging o l'API S3 DeleteBucketTagging.

La modifica del tag della policy assegnato a un bucket ha un impatto temporaneo sulle performance, mentre gli oggetti vengono rivalutati utilizzando la nuova policy ILM.

Gestire la coerenza del bucket

I valori di coerenza possono essere utilizzati per specificare la disponibilità delle modifiche alle impostazioni del bucket e per fornire un equilibrio tra la disponibilità degli oggetti all'interno di un bucket e la coerenza di tali oggetti in diversi nodi e siti di archiviazione. È possibile modificare i valori di coerenza in modo che siano diversi dai valori predefiniti in modo che le applicazioni client possano soddisfare le proprie esigenze operative.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

Linee guida per la coerenza della benna

La coerenza del bucket viene utilizzata per determinare la coerenza delle applicazioni client che influiscono sugli oggetti all'interno del bucket S3. In generale, si dovrebbe usare la coerenza **Read-after-new-write** per i

propri bucket.

modificare la coerenza del bucket

Se la coerenza **Read-after-new-write** non soddisfa i requisiti dell'applicazione client, è possibile modificare la coerenza impostando la coerenza del bucket o utilizzando `Consistency-Control` intestazione. Il `Consistency-Control` la testata esclude la coerenza della benna.

> Quando si modifica la consistenza di un bucket, solo gli oggetti che vengono acquisiti dopo la modifica sono garantiti per soddisfare l'impostazione modificata.

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.
2. Selezionare il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **.
4. Selezionare una coerenza per le operazioni eseguite sugli oggetti in questo bucket.
   - **Tutti**: Offre il massimo livello di coerenza. Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
   - **Strong-Global**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
   - **Strong-Site**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
   - **Read-after-new-write** (valore predefinito): Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
   - **Available**: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.
5. Selezionare **Save Changes** (Salva modifiche).

Cosa accade quando si modificano le impostazioni della benna

I bucket hanno impostazioni multiple che influiscono sul comportamento dei bucket e degli oggetti all'interno di tali bucket.

Per impostazione predefinita, le seguenti impostazioni del bucket utilizzano la coerenza **strong**. Se due o più nodi di archiviazione non sono disponibili all'interno di un sito o se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

- "Eliminazione bucket vuoto in background"
- "Ora ultimo accesso"
- "Ciclo di vita del bucket"
- "Politica del bucket"

- "Etichettatura della benna"
- "Versione bucket"
- "Blocco oggetti S3"
- "Crittografia bucket"

> Il valore di coerenza per la versione bucket, blocco oggetto S3 e crittografia bucket non può essere impostato su un valore non fortemente coerente.

Le seguenti impostazioni della benna non utilizzano una forte coerenza e hanno una maggiore disponibilità per le modifiche. Le modifiche a queste impostazioni potrebbero richiedere del tempo prima di avere effetto.

- "Configurazione dei servizi della piattaforma: Integrazione di notifica, replica o ricerca"
- "Configurazione CORS"
- Modificare la coerenza della benna

> Se la coerenza predefinita utilizzata durante la modifica delle impostazioni del bucket non soddisfa i requisiti dell'applicazione client, è possibile modificare la coerenza utilizzando `Consistency-Control` intestazione per "API REST S3" oppure utilizzando `reducedConsistency` oppure `force` in "API di gestione del tenant".

Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso

Quando gli amministratori della griglia creano le regole ILM (Information Lifecycle Management) per un sistema StorageGRID, possono facoltativamente specificare che l'ultimo tempo di accesso di un oggetto deve essere utilizzato per determinare se spostare l'oggetto in una posizione di storage diversa. Se si utilizza un tenant S3, è possibile sfruttare tali regole attivando gli ultimi aggiornamenti del tempo di accesso per gli oggetti in un bucket S3.

Queste istruzioni si applicano solo ai sistemi StorageGRID che includono almeno una regola ILM che utilizza l'opzione **ultimo tempo di accesso** come filtro avanzato o come tempo di riferimento. È possibile ignorare queste istruzioni se il sistema StorageGRID non include tale regola. Vedere "USA l'ultimo tempo di accesso nelle regole ILM" per ulteriori informazioni.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

A proposito di questa attività

Ultimo tempo di accesso è una delle opzioni disponibili per l'istruzione di posizionamento **tempo di riferimento** per una regola ILM. L'impostazione del tempo di riferimento per una regola su ultimo tempo di accesso consente agli amministratori della griglia di specificare che gli oggetti devono essere posizionati in determinate posizioni di storage in base al momento dell'ultimo recupero (lettura o visualizzazione) di tali oggetti.

Ad esempio, per garantire che gli oggetti visualizzati di recente rimangano sullo storage più veloce, un amministratore della griglia può creare una regola ILM specificando quanto segue:

- Gli oggetti recuperati nell'ultimo mese devono rimanere sui nodi di storage locali.
- Gli oggetti che non sono stati recuperati nell'ultimo mese devono essere spostati in una posizione off-site.

Per impostazione predefinita, gli aggiornamenti dell'ultimo tempo di accesso sono disattivati. Se il sistema StorageGRID include una regola ILM che utilizza l'opzione **ultimo tempo di accesso** e si desidera che questa opzione venga applicata agli oggetti in questo bucket, è necessario abilitare gli aggiornamenti dell'ultimo tempo di accesso per i bucket S3 specificati in tale regola.

> L'aggiornamento dell'ultimo tempo di accesso durante il recupero di un oggetto può ridurre le prestazioni di StorageGRID, in particolare per gli oggetti di piccole dimensioni.

Si verifica un impatto sulle performance con gli ultimi aggiornamenti dell'orario di accesso, perché StorageGRID deve eseguire questi passaggi aggiuntivi ogni volta che vengono recuperati gli oggetti:

- Aggiornare gli oggetti con nuovi timestamp
- Aggiungere gli oggetti alla coda ILM, in modo che possano essere rivalutati in base alle regole e ai criteri ILM correnti

La tabella riassume il comportamento applicato a tutti gli oggetti nel bucket quando l'ultimo tempo di accesso è disattivato o attivato.

Tipo di richiesta	Comportamento se l'ultimo tempo di accesso è disattivato (impostazione predefinita)		Comportamento se è attivata l'ultima ora di accesso	
	Ultimo aggiornamento dell'orario di accesso?	Oggetto aggiunto alla coda di valutazione ILM?	Ultimo aggiornamento dell'orario di accesso?	Oggetto aggiunto alla coda di valutazione ILM?
Richiesta di recuperare un oggetto, il relativo elenco di controllo degli accessi o i relativi metadati	No	No	Sì	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì	Sì	Sì
Richiesta di copia di un oggetto da un bucket all'altro	• No, per la copia di origine • Sì, per la copia di destinazione	• No, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione

Richiesta di completare un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Fasi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
2. Selezionare il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **ultimi aggiornamenti dell'ora di accesso**.
4. Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso.
5. Selezionare **Save Changes** (Salva modifiche).

Modificare la versione degli oggetti per un bucket

Se si utilizza un tenant S3, è possibile modificare lo stato di versione per i bucket S3.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- Tutti i nodi storage sono disponibili.

A proposito di questa attività

È possibile attivare o sospendere il controllo delle versioni degli oggetti per un bucket. Una volta attivata la versione per un bucket, non è possibile tornare allo stato senza versione. Tuttavia, è possibile sospendere il controllo delle versioni per il bucket.

- Disabled (Disattivato): La versione non è mai stata attivata
- Enabled (attivato): Il controllo delle versioni è attivato
- Suspended (sospeso): Il controllo delle versioni era stato precedentemente attivato e sospeso

Per ulteriori informazioni, vedere quanto segue:

- "Versione degli oggetti"
- "Regole e criteri ILM per gli oggetti con versione S3 (esempio 4)"
- "Modalità di eliminazione degli oggetti"

Fasi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
2. Selezionare il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **versione oggetto**.

4. Selezionare uno stato di versione per gli oggetti in questo bucket.

   La versione degli oggetti deve rimanere abilitata per un bucket utilizzato per la replica cross-grid. Se S3 Object Lock (blocco oggetti S3) o legacy compliance (compliance legacy) è attivato, le opzioni **Object versioning** (versione oggetto) sono disattivate.

Opzione	Descrizione
Abilitare il controllo delle versioni	Abilitare la versione degli oggetti se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto in base alle esigenze. Gli oggetti già presenti nel bucket verranno sottoposti alla versione quando vengono modificati da un utente.
Sospendere il controllo delle versioni	Sospendere la versione degli oggetti se non si desidera più creare nuove versioni degli oggetti. È comunque possibile recuperare le versioni di oggetti esistenti.

5. Selezionare **Save Changes** (Salva modifiche).

USA il blocco oggetti S3 per conservare gli oggetti

È possibile utilizzare il blocco oggetti S3 se i bucket e gli oggetti devono soddisfare i requisiti normativi per la conservazione.

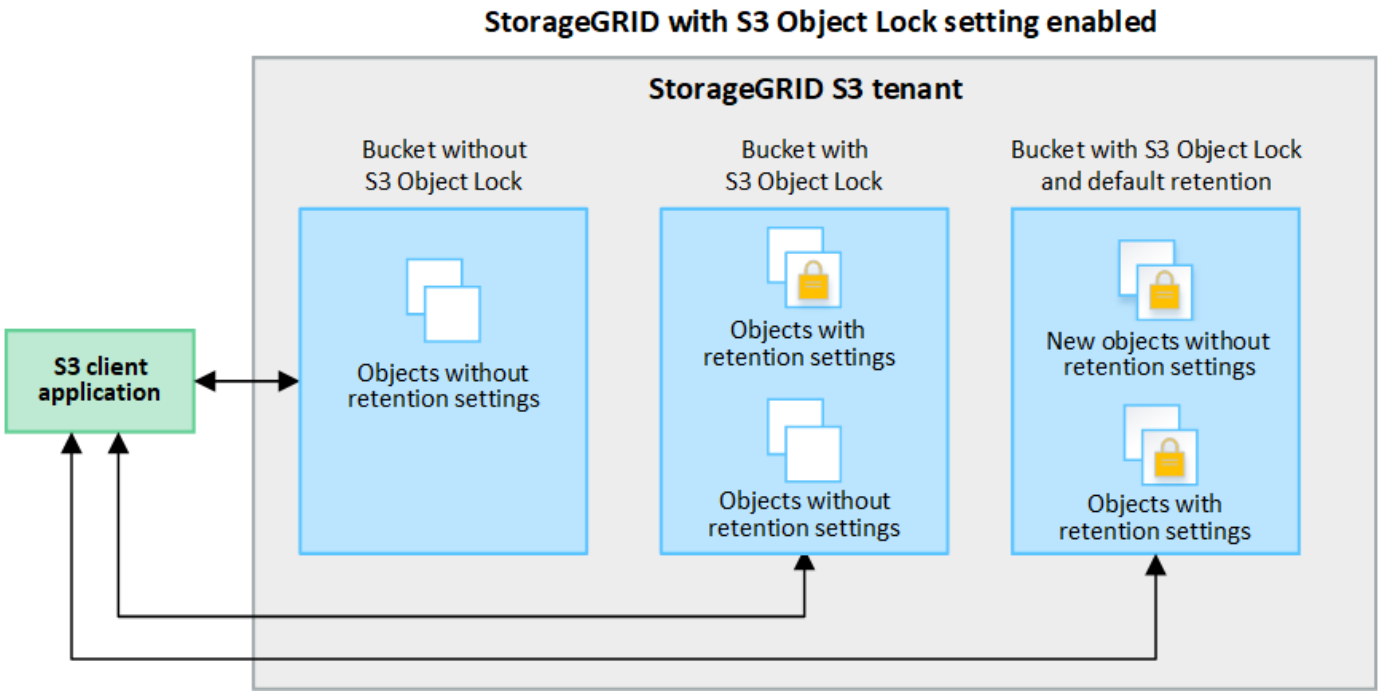
Che cos'è il blocco oggetti S3?

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).

Come mostrato nella figura, quando l'impostazione globale S3 Object Lock è attivata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se un bucket ha S3 Object Lock attivato, è necessario il controllo della versione del bucket e viene attivato automaticamente.

Se un bucket ha attivato il blocco oggetti S3, le applicazioni client S3 possono specificare le impostazioni di conservazione per qualsiasi versione di oggetto salvata in quel bucket.

Inoltre, un bucket con S3 Object Lock attivato può avere una modalità di conservazione e un periodo di conservazione predefiniti. Le impostazioni predefinite si applicano solo agli oggetti aggiunti al bucket senza le proprie impostazioni di conservazione.



Modalità di conservazione

La funzione blocco oggetti di StorageGRID S3 supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità equivalgono alle modalità di conservazione Amazon S3.

- In modalità compliance:
  - L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
  - La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità governance:
  - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare alcune impostazioni di conservazione.
  - Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
  - Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

Impostazioni di conservazione per le versioni degli oggetti

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono utilizzare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ogni oggetto aggiunto al bucket:

- **Modalità di conservazione**: Conformità o governance.
- **Mantieni-fino-data**: Se la data di conservazione di una versione dell'oggetto è futura, l'oggetto può essere recuperato, ma non può essere cancellato.
- **Conservazione legale**: L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa. Le conservazioni legali sono

indipendenti dalla conservazione fino alla data odierna.

> Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Per ulteriori informazioni sulle impostazioni dell'oggetto, vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

Impostazione di conservazione predefinita per i bucket

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita**: Conformità o governance.
- **Default Retention Period** (periodo di conservazione predefinito): Per quanto tempo le nuove versioni degli oggetti aggiunte a questo bucket devono essere conservate, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non dispongono di proprie impostazioni di conservazione. Gli oggetti bucket esistenti non vengono influenzati quando si aggiungono o si modificano queste impostazioni predefinite.

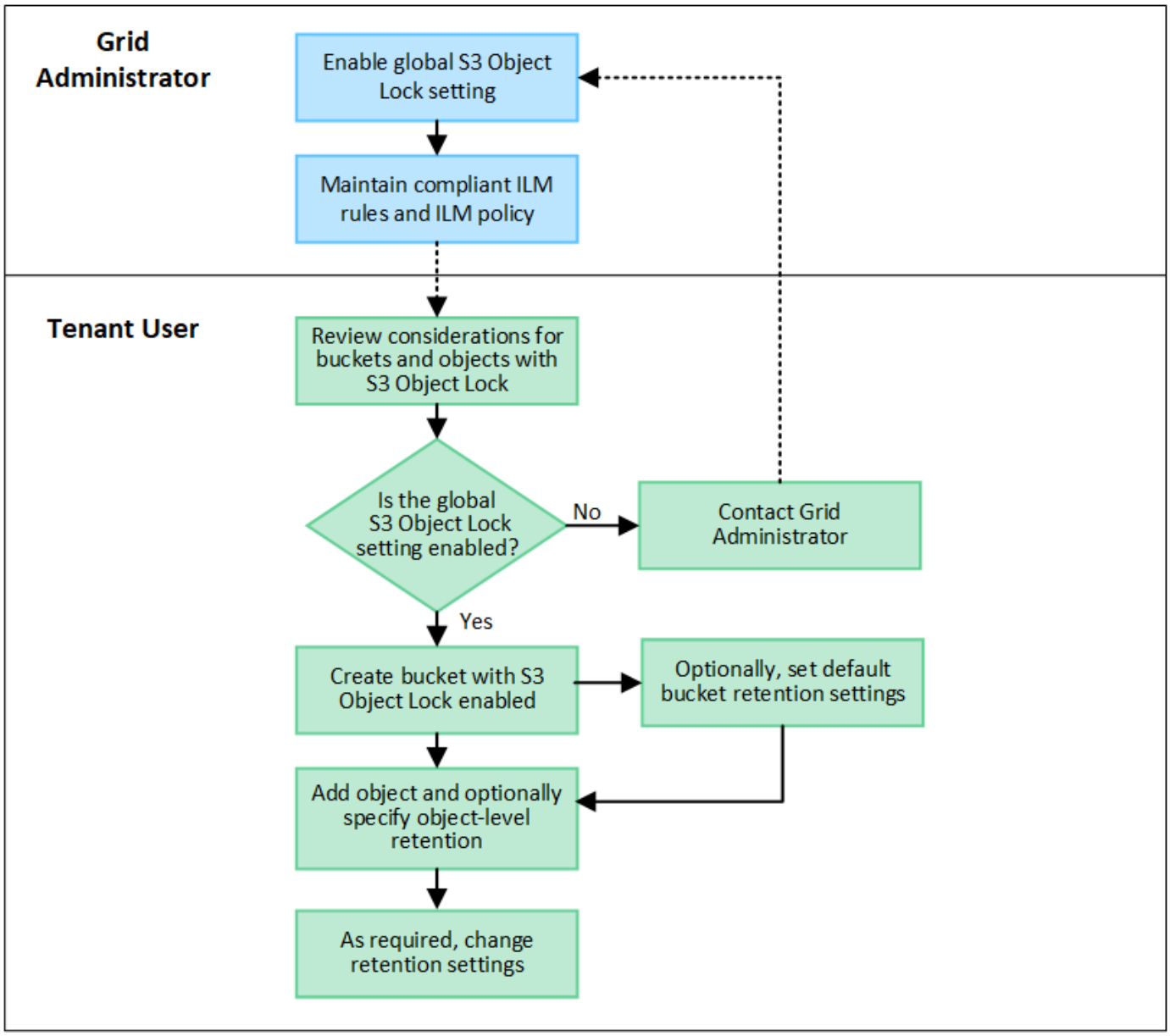
Vedere "Creare un bucket S3" e. "Aggiorna la conservazione predefinita del blocco oggetti S3".

Workflow di blocco oggetti S3

Il diagramma del flusso di lavoro mostra i passaggi di alto livello per l'utilizzo della funzione blocco oggetti S3 in StorageGRID.

Prima di poter creare bucket con blocco oggetti S3 attivato, l'amministratore della griglia deve attivare l'impostazione di blocco oggetti S3 globale per l'intero sistema StorageGRID. L'amministratore di rete deve inoltre garantire che il criterio ILM (Information Lifecycle Management) sia "conforme"; deve soddisfare i requisiti dei bucket con blocco oggetti S3 abilitato. Per ulteriori informazioni, contattare l'amministratore della griglia o consultare le istruzioni di "Gestire gli oggetti con S3 Object Lock".

Una volta attivata l'impostazione globale S3 Object Lock, è possibile creare bucket con S3 Object Lock attivato e specificare facoltativamente le impostazioni di conservazione predefinite per ciascun bucket. Inoltre, è possibile utilizzare l'applicazione client S3 per specificare facoltativamente le impostazioni di conservazione per ciascuna versione dell'oggetto.



Requisiti per i bucket con S3 Object Lock attivato

- Se l'impostazione blocco oggetto S3 globale è attivata per il sistema StorageGRID, è possibile utilizzare Gestione tenant, API di gestione tenant o API REST S3 per creare bucket con blocco oggetto S3 attivato.
- Se si intende utilizzare il blocco oggetti S3, è necessario attivare il blocco oggetti S3 quando si crea il bucket. Impossibile attivare il blocco oggetti S3 per un bucket esistente.
- Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket. Non puoi disattivare il blocco oggetti S3 o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione e un periodo di conservazione predefiniti per ciascun bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di proprie impostazioni di conservazione. È possibile eseguire l'override di queste impostazioni predefinite specificando una modalità di conservazione e conservarla fino alla data per ogni versione dell'oggetto al momento del caricamento.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con blocco oggetti S3 attivato.

- La replica di CloudMirror non è supportata per i bucket con blocco oggetti S3 attivato.

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

- Per proteggere una versione dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure le impostazioni di conservazione per ciascuna versione dell'oggetto. È possibile specificare le impostazioni di conservazione a livello di oggetto utilizzando l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni di oggetti. Una versione a oggetti può avere un'impostazione di conservazione fino alla data e un'impostazione di conservazione legale, una ma non l'altra o nessuna delle due. La specifica di un'impostazione di conservazione fino a data o di conservazione legale per un oggetto protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

Ciclo di vita degli oggetti nei bucket con S3 Object Lock attivato

Ogni oggetto salvato in un bucket con S3 Object Lock attivato passa attraverso le seguenti fasi:

1. **Acquisizione oggetto**

   Quando una versione dell'oggetto viene aggiunta al bucket con S3 Object Lock attivato, le impostazioni di conservazione vengono applicate come segue:

   - Se per l'oggetto sono specificate le impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.
   - Se non sono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se presenti.
   - Se non sono specificate impostazioni di conservazione per l'oggetto o il bucket, l'oggetto non è protetto da S3 Object Lock.

   Se vengono applicate le impostazioni di conservazione, vengono protetti sia l'oggetto che i metadati S3 definiti dall'utente.

2. **Conservazione ed eliminazione degli oggetti**

   StorageGRID memorizza più copie di ciascun oggetto protetto per il periodo di conservazione specificato. Il numero e il tipo esatti delle copie degli oggetti e le posizioni dello storage sono determinati dalle regole di conformità nelle policy ILM attive. La possibilità di eliminare un oggetto protetto prima che venga raggiunta la data di conservazione dipende dalla modalità di conservazione.

   - Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Posso comunque gestire i bucket conformi alle versioni precedenti?

La funzione blocco oggetti S3 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Se sono stati creati bucket conformi utilizzando una versione precedente di StorageGRID, è possibile continuare a gestire le impostazioni di questi bucket; tuttavia, non è più possibile creare nuovi bucket conformi. Per istruzioni, vedere
"Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5".

Aggiorna la conservazione predefinita del blocco oggetti S3

Se al momento della creazione del bucket è stato attivato il blocco oggetti S3, è possibile

modificare il bucket per modificare le impostazioni di conservazione predefinite. È possibile attivare (o disattivare) la conservazione predefinita e impostare una modalità di conservazione e un periodo di conservazione predefiniti.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- Il blocco oggetti S3 è attivato globalmente per il sistema StorageGRID e il blocco oggetti S3 è stato attivato quando è stato creato il bucket. Vedere "USA il blocco oggetti S3 per conservare gli oggetti".

Fasi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
2. Selezionare il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **S3 Object Lock**.
4. Facoltativamente, attivare o disattivare **Default Retention** per questo bucket.

   Le modifiche apportate a questa impostazione non si applicano agli oggetti già presenti nel bucket o a qualsiasi oggetto che potrebbe avere periodi di conservazione propri.

5. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare una **modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
Governance	• Utenti con `s3:BypassGovernanceRetention` l'autorizzazione può utilizzare `x-amz-bypass-governance-retention: true` richiedi intestazione per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

6. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare il **Default Retention Period** (periodo di conservazione predefinito) per il bucket.

Il **Default Retention Period** indica per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. Specificare un valore compreso tra 1 e 36,500 giorni o tra 1 e 100 anni, inclusi.

7. Selezionare **Save Changes** (Salva modifiche).

Configurare la condivisione delle risorse tra origini (CORS)

È possibile configurare la condivisione delle risorse cross-origin (CORS) per un bucket S3 se si desidera che quel bucket e gli oggetti in quel bucket siano accessibili alle applicazioni web in altri domini.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

A proposito di questa attività

La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni Web client di un dominio di accedere alle risorse di un dominio diverso. Si supponga, ad esempio, di utilizzare un bucket S3 denominato `Images` per memorizzare le immagini. Configurando CORS per `Images` bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito web `http://www.example.com`.

Abilitare il CORS per un bucket

Fasi

1. Utilizzare un editor di testo per creare l'XML richiesto.

   Questo esempio mostra l'XML utilizzato per abilitare il CORS per un bucket S3. Questo XML consente a qualsiasi dominio di inviare richieste GET al bucket, ma consente solo il `http://www.example.com` Dominio per inviare richieste DI POST ed ELIMINAZIONE. Sono consentite tutte le intestazioni delle richieste.

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

Per ulteriori informazioni sull'XML di configurazione CORS, vedere "Documentazione Amazon Web Services (AWS): Guida per sviluppatori Amazon Simple Storage Service".

2. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.
3. Selezionare il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Dalla scheda **bucket access**, selezionare la fisarmonica **Cross-Origin Resource Sharing (CORS)**.
5. Selezionare la casella di controllo **Enable CORS** (attiva CORS*).
6. Incollare l'XML di configurazione CORS nella casella di testo.
7. Selezionare **Save Changes** (Salva modifiche).

Modificare l'impostazione CORS

Fasi

1. Aggiornare l'XML di configurazione CORS nella casella di testo oppure selezionare **Clear** per ricominciare.
2. Selezionare **Save Changes** (Salva modifiche).

Disattiva l'impostazione CORS

Fasi

1. Deselezionare la casella di controllo **Enable CORS** (attiva CORS*).
2. Selezionare **Save Changes** (Salva modifiche).

Eliminare gli oggetti nel bucket

È possibile utilizzare Tenant Manager per eliminare gli oggetti in uno o più bucket.

Considerazioni e requisiti

Prima di eseguire questa procedura, tenere presente quanto segue:

- Quando si eliminano gli oggetti in un bucket, StorageGRID rimuove in modo permanente tutti gli oggetti e tutte le versioni degli oggetti in ogni bucket selezionato da tutti i nodi e siti nel sistema StorageGRID. StorageGRID rimuove anche i metadati degli oggetti correlati. Non sarà possibile recuperare queste informazioni.
- L'eliminazione di tutti gli oggetti in un bucket può richiedere minuti, giorni o persino settimane, in base al numero di oggetti, copie di oggetti e operazioni simultanee.
- Se un bucket ha "Blocco oggetti S3 attivato", Potrebbe rimanere nello stato **Deleting Objects: Read-only** per *anni*.

> Un bucket che utilizza il blocco oggetti S3 rimarrà nello stato **Deleting Objects: Read-only** (eliminazione oggetti: Sola lettura) fino a quando non viene raggiunta la data di conservazione per tutti gli oggetti e non vengono rimosse le conservazioni legali.

- Durante l'eliminazione degli oggetti, lo stato del bucket è **eliminazione degli oggetti: Sola lettura**. In questo stato, non è possibile aggiungere nuovi oggetti al bucket.
- Una volta cancellati tutti gli oggetti, il bucket rimane in stato di sola lettura. È possibile eseguire una delle seguenti operazioni:
  - Riportare il bucket in modalità di scrittura e riutilizzarlo per nuovi oggetti
  - Eliminare il bucket
  - Mantenere il bucket in modalità di sola lettura per riservare il proprio nome per un utilizzo futuro
- Se in un bucket è attivata la versione oggetto, è possibile rimuovere i marcatori di eliminazione creati in StorageGRID 11,8 o versioni successive utilizzando le operazioni Elimina oggetti nel bucket.
- Se in un bucket è attivata la versione oggetto, l'operazione di eliminazione degli oggetti non rimuoverà i marcatori di eliminazione creati in StorageGRID 11,7 o versioni precedenti. Vedere le informazioni sull'eliminazione di oggetti in un bucket in "Modalità di eliminazione degli oggetti con versione S3".
- Se si utilizza "replica cross-grid", tenere presente quanto segue:
  - L'utilizzo di questa opzione non elimina alcun oggetto dal bucket dell'altra griglia.
  - Se si seleziona questa opzione per il bucket di origine, l'avviso **errore replica cross-grid** verrà attivato se si aggiungono oggetti al bucket di destinazione sull'altra griglia. Se non puoi garantire che nessuno aggiungerà oggetti al bucket sull'altra griglia, "disattiva la replica cross-grid" per quel bucket prima di eliminare tutti gli oggetti bucket.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root". Questa autorizzazione sovrascrive le impostazioni delle autorizzazioni nei criteri di gruppo o bucket.

Fasi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.

   Viene visualizzata la pagina bucket che mostra tutti i bucket S3 esistenti.

2. Utilizzare il menu **azioni** o la pagina dei dettagli per un bucket specifico.

Menu delle azioni

a. Selezionare la casella di controllo per ciascun bucket da cui si desidera eliminare gli oggetti.

b. Selezionare **azioni** > **Elimina oggetti nel bucket**.

Pagina dei dettagli

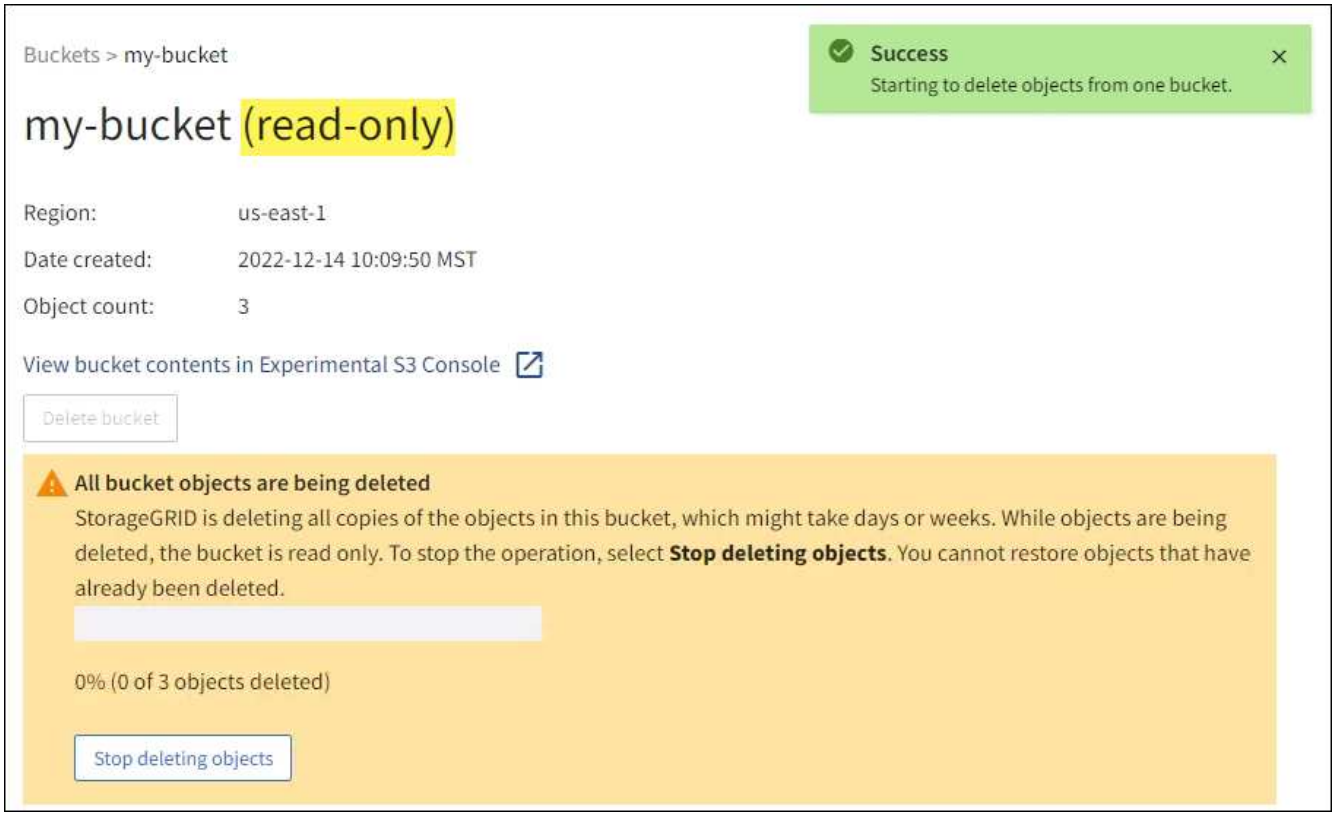
a. Selezionare il nome di un bucket per visualizzarne i dettagli.

b. Selezionare **Elimina oggetti nel bucket**.

3. Quando viene visualizzata la finestra di dialogo di conferma, rivedere i dettagli, inserire **Sì** e selezionare **OK**.
4. Attendere l'inizio dell'operazione di eliminazione.

   Dopo alcuni minuti:

   - Nella pagina dei dettagli del bucket viene visualizzato un banner di stato giallo. La barra di avanzamento indica la percentuale di oggetti eliminati.
   - * (sola lettura)* viene visualizzato dopo il nome del bucket nella pagina dei dettagli del bucket.
   - **(eliminazione di oggetti: Sola lettura)** viene visualizzato accanto al nome del bucket nella pagina bucket.

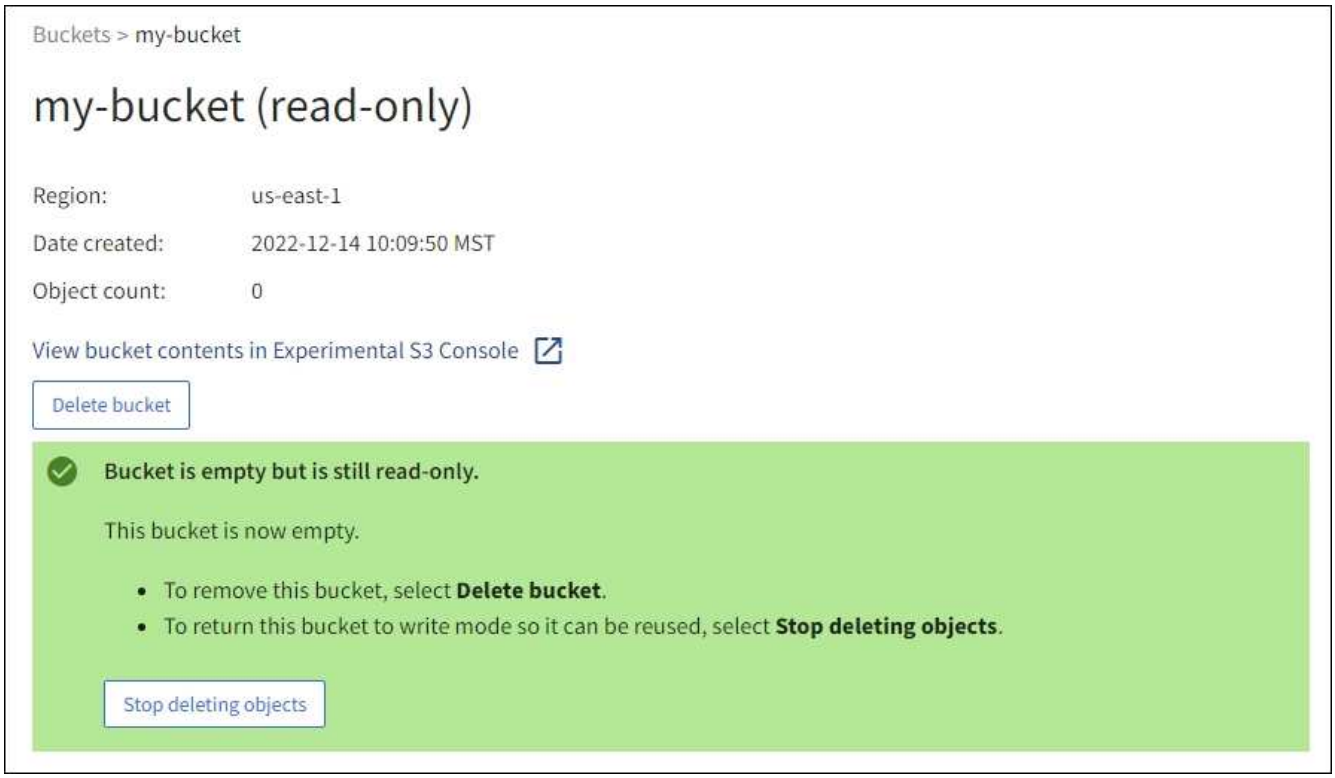


5. Quando l'operazione è in esecuzione, selezionare **Stop deleting objects** (Interrompi eliminazione oggetti) per interrompere il processo. Quindi, se si desidera, selezionare **Delete Objects in bucket** (Elimina oggetti nel bucket) per riprendere il processo.

   Quando si seleziona **Stop deleting objects**, il bucket torna alla modalità di scrittura; tuttavia, non è possibile accedere o ripristinare gli oggetti che sono stati cancellati.

6. Attendere il completamento dell'operazione.

   Quando il bucket è vuoto, il banner di stato viene aggiornato, ma il bucket rimane di sola lettura.



7. Effettuare una delle seguenti operazioni:
   - Uscire dalla pagina per mantenere il bucket in modalità di sola lettura. Ad esempio, è possibile mantenere un bucket vuoto in modalità di sola lettura per riservare il nome del bucket per un utilizzo futuro.
   - Eliminare il bucket. È possibile selezionare **Delete bucket** (Elimina bucket) per eliminare un singolo bucket o tornare alla pagina Bucket e selezionare **Actions** > **Delete** bucket (azioni* > **Delete** bucket) per rimuovere più bucket.

     > Se non si riesce a eliminare un bucket con versione dopo l'eliminazione di tutti gli oggetti, i contrassegni di eliminazione potrebbero rimanere. Per eliminare il bucket, è necessario rimuovere tutti gli altri marker di eliminazione.

   - Riportare il bucket in modalità di scrittura e, se si desidera, riutilizzarlo per nuovi oggetti. È possibile selezionare **Interrompi eliminazione oggetti** per un singolo bucket o tornare alla pagina bucket e selezionare **azione** > **Interrompi eliminazione oggetti** per più bucket.

Elimina bucket S3

È possibile utilizzare Tenant Manager per eliminare uno o più bucket S3 vuoti.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

- I bucket che si desidera eliminare sono vuoti. Se i bucket che si desidera eliminare sono *non* vuoti, "eliminare gli oggetti dal bucket".

A proposito di questa attività

Queste istruzioni descrivono come eliminare un bucket S3 utilizzando il Tenant Manager. È inoltre possibile eliminare i bucket S3 utilizzando "API di gestione del tenant" o il "API REST S3".

Non è possibile eliminare un bucket S3 se contiene oggetti, versioni di oggetti non correnti o contrassegni di eliminazione. Per informazioni sull'eliminazione degli oggetti con versione S3, vedere "Modalità di eliminazione degli oggetti".

Fasi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.

   Viene visualizzata la pagina bucket che mostra tutti i bucket S3 esistenti.

2. Utilizzare il menu **azioni** o la pagina dei dettagli per un bucket specifico.

   Menu delle azioni

   a. Selezionare la casella di controllo per ciascun bucket che si desidera eliminare.
   b. Selezionare **azioni** > **Elimina bucket**.

   Pagina dei dettagli

   a. Selezionare il nome di un bucket per visualizzarne i dettagli.
   b. Selezionare **Delete bucket** (Elimina bucket).

3. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Sì**.

   StorageGRID conferma che ogni bucket è vuoto e quindi elimina ogni bucket. Questa operazione potrebbe richiedere alcuni minuti.

   Se un bucket non è vuoto, viene visualizzato un messaggio di errore. È necessario "eliminare tutti gli oggetti ed eventuali marcatori di eliminazione nel bucket" prima di eliminare il bucket.

Utilizzare la console S3

È possibile utilizzare S3 Console per visualizzare e gestire gli oggetti in un bucket S3.

La console S3 consente di:

- Caricamento, download, ridenominazione, copia, spostamento, ed eliminare gli oggetti
- Visualizzare, ripristinare, scaricare ed eliminare le versioni degli oggetti
- Cercare gli oggetti in base al prefisso
- Gestire tag di oggetti
- Visualizzare i metadati degli oggetti
- Visualizzare, creare, rinominare, copiare, spostare, ed eliminare le cartelle

La console S3 offre un'esperienza utente migliorata per i casi più comuni. Non è progettato per sostituire le operazioni CLI o API in tutte le situazioni.

Se l'utilizzo di S3 Console comporta un'operazione troppo lunga (ad esempio, minuti o ore), considerare quanto segue:

- Riduzione del numero di oggetti selezionati
- Utilizzando metodi non grafici (API o CLI) per accedere ai dati

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- Se si desidera gestire gli oggetti, si appartiene a un gruppo di utenti che dispone dell'autorizzazione di accesso principale. In alternativa, si appartiene a un gruppo di utenti che dispone dell'autorizzazione Usa scheda Console S3 e dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket. Vedere "Permessi di gestione del tenant".
- Per l'utente è stato configurato un criterio Gruppo S3 o bucket. Vedere "Utilizza policy di accesso a bucket e gruppi".
- Conosci l'ID della chiave di accesso dell'utente e la chiave di accesso segreta. Se si desidera, si dispone di un `.csv` file contenente queste informazioni. Vedere "istruzioni per la creazione delle chiavi di accesso".

Fasi

1. Selezionare **STORAGE** > **bucket** > ***bucket name***.
2. Selezionare la scheda Console S3.
3. Incollare l'ID della chiave di accesso e la chiave di accesso segreta nei campi. In caso contrario, selezionare **carica chiavi di accesso** e selezionare il `.csv` file.
4. Selezionare **Accedi**.
5. Viene visualizzata la tavola degli oggetti bucket. È possibile gestire gli oggetti in base alle esigenze.

Ulteriori informazioni

- **Cerca per prefisso**: La funzione di ricerca del prefisso ricerca solo gli oggetti che iniziano con una parola specifica relativa alla cartella corrente. La ricerca non include oggetti che contengono la parola altrove. Questa regola si applica anche agli oggetti all'interno delle cartelle. Ad esempio, una ricerca di `folder1/folder2/somefile-` restituisce gli oggetti all'interno di `folder1/folder2/` e iniziare con la parola `somefile-`.
- **Trascinare e rilasciare**: È possibile trascinare i file dal file manager del computer a S3 Console. Tuttavia, non è possibile caricare le cartelle.
- **Operazioni sulle cartelle**: Quando si sposta, copia o rinomina una cartella, tutti gli oggetti nella cartella vengono aggiornati uno alla volta, il che potrebbe richiedere del tempo.
- **Eliminazione permanente quando la versione bucket è disattivata**: Quando si sovrascrive o si elimina un oggetto in un bucket con la versione disattivata, l'operazione è permanente. Vedere "Modificare la versione degli oggetti per un bucket".

Gestire i servizi della piattaforma S3

Gestione dei servizi della piattaforma: Panoramica

I servizi della piattaforma StorageGRID possono aiutarti a implementare una strategia di

cloud ibrido consentendo di inviare notifiche di eventi e copie di oggetti S3 e metadati di oggetti a destinazioni esterne.

Se l'utilizzo dei servizi della piattaforma è consentito per l'account tenant, è possibile configurare i seguenti servizi per qualsiasi bucket S3:

Replica di CloudMirror

Utilizzare "Servizio di replica di StorageGRID CloudMirror" Per eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.

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.

> La replica di CloudMirror non è supportata se il bucket di origine ha attivato il blocco oggetti S3.

Notifiche

Utilizzare "notifiche di eventi per bucket" Per inviare notifiche su azioni specifiche eseguite su oggetti a un Amazon Simple Notification Service (Amazon SNS) esterno specificato.

Ad esempio, è possibile configurare gli avvisi da inviare agli amministratori in merito a ciascun oggetto aggiunto a un bucket, in cui gli oggetti rappresentano i file di registro associati a un evento di sistema critico.

> Sebbene la notifica degli eventi possa essere configurata su un bucket con blocco oggetti S3 attivato, i metadati del blocco oggetti S3 (inclusi lo stato Mantieni fino alla data e conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.

Servizio di integrazione della ricerca

Utilizzare "servizio di integrazione della ricerca" Per inviare i metadati dell'oggetto S3 a un indice Elasticsearch specificato, in cui è possibile cercare o analizzare i metadati utilizzando il servizio esterno.

Ad esempio, è possibile configurare i bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. È quindi possibile utilizzare Elasticsearch per eseguire ricerche tra bucket ed eseguire analisi sofisticate dei modelli presenti nei metadati degli oggetti.

> Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock attivato, i metadati S3 Object Lock (inclusi Retain until Date e Legal Hold status) degli oggetti non saranno inclusi nei messaggi di notifica.

Poiché la posizione di destinazione dei servizi della piattaforma è generalmente esterna all'implementazione di StorageGRID, i servizi della piattaforma offrono la potenza e la flessibilità derivanti dall'utilizzo di risorse di storage esterne, servizi di notifica e servizi di ricerca o analisi per i dati.

È possibile configurare qualsiasi combinazione di servizi di piattaforma per un singolo bucket S3. Ad esempio, è possibile configurare il servizio CloudMirror e le notifiche su un bucket StorageGRID S3 in modo da eseguire il mirroring di oggetti specifici al servizio di storage semplice Amazon, inviando una notifica relativa a ciascun oggetto a un'applicazione di monitoraggio di terze parti per tenere traccia delle spese AWS.

> L'utilizzo dei servizi della piattaforma deve essere abilitato per ciascun account tenant da un amministratore StorageGRID utilizzando il gestore di griglia o l'API di gestione del grid.

Modalità di configurazione dei servizi della piattaforma

I servizi della piattaforma comunicano con gli endpoint esterni configurati tramite "Manager tenant" o il "API di gestione del tenant". Ogni endpoint rappresenta una destinazione esterna, come un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento di Amazon SNS o un cluster Elasticsearch ospitato localmente, su AWS o altrove.

Dopo aver creato un endpoint esterno, è possibile attivare un servizio di piattaforma per un bucket aggiungendo la configurazione XML al bucket. La configurazione XML identifica gli oggetti su cui il bucket deve agire, l'azione che il bucket deve intraprendere e l'endpoint che il bucket deve utilizzare per il servizio.

È necessario aggiungere configurazioni XML separate per ogni servizio di piattaforma che si desidera configurare. Ad esempio:

- Se si desidera che tutti gli oggetti le cui chiavi iniziano con `/images` Per essere replicati in un bucket Amazon S3, è necessario aggiungere una configurazione di replica al bucket di origine.
- Se si desidera anche inviare notifiche quando questi oggetti vengono memorizzati nel bucket, è necessario aggiungere una configurazione di notifica.
- Infine, se si desidera indicizzare i metadati per questi oggetti, è necessario aggiungere la configurazione di notifica dei metadati utilizzata per implementare l'integrazione della ricerca.

Il formato per l'XML di configurazione è regolato dalle API REST S3 utilizzate per implementare i servizi della piattaforma StorageGRID:

Servizio di piattaforma	API REST S3	Fare riferimento a.
Replica di CloudMirror	• GetBucketReplication • PutBucketReplication	• "Replica di CloudMirror" • "Operazioni sui bucket"
Notifiche	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Notifiche" • "Operazioni sui bucket"
Integrazione della ricerca	• OTTIENI la configurazione della notifica dei metadati del bucket • INSERIRE la configurazione della notifica dei metadati del bucket	• "Integrazione della ricerca" • "Operazioni personalizzate di StorageGRID"

Informazioni correlate

"Considerazioni per i servizi della piattaforma"

Servizio di replica di CloudMirror

È possibile attivare la replica di CloudMirror per un bucket S3 se si desidera che StorageGRID replici gli oggetti specificati aggiunti al bucket in uno o più bucket di destinazione.

La replica CloudMirror funziona indipendentemente dalle policy ILM attive del grid. Il servizio CloudMirror replica gli oggetti memorizzati nel bucket di origine e li consegna al bucket di destinazione il prima possibile. La consegna degli oggetti replicati viene attivata quando l'acquisizione degli oggetti ha esito positivo.

> La replica di CloudMirror presenta importanti analogie e differenze con la funzionalità di replica cross-grid. Per ulteriori informazioni, vedere "Confronta la replica cross-grid e la replica CloudMirror".

Se si attiva la replica CloudMirror per un bucket esistente, vengono replicati solo i nuovi oggetti aggiunti a tale bucket. Gli oggetti esistenti nel bucket non vengono replicati. Per forzare la replica degli oggetti esistenti, è possibile aggiornare i metadati dell'oggetto esistente eseguendo una copia dell'oggetto.

> Se si utilizza la replica CloudMirror per copiare oggetti in una destinazione Amazon S3, tenere presente che Amazon S3 limita la dimensione dei metadati definiti dall'utente all'interno di ogni intestazione della richiesta PUT a 2 KB. Se un oggetto ha metadati definiti dall'utente superiori a 2 KB, tale oggetto non verrà replicato.

In StorageGRID, è possibile replicare gli oggetti in un singolo bucket in più bucket di destinazione. A tale scopo, specificare la destinazione di ciascuna regola nel file XML di configurazione della replica. Non è possibile replicare un oggetto in più bucket contemporaneamente.

Inoltre, è possibile configurare la replica di CloudMirror su bucket con versione o senza versione e specificare un bucket con versione o senza versione come destinazione. È possibile utilizzare qualsiasi combinazione di bucket con versione e senza versione. Ad esempio, è possibile specificare un bucket con versione come destinazione per un bucket di origine senza versione o viceversa. È inoltre possibile eseguire la replica tra bucket senza versione.

Il comportamento di eliminazione per il servizio di replica CloudMirror è lo stesso del comportamento di eliminazione del servizio CRR (Cross Region Replication) fornito da Amazon S3: L'eliminazione di un oggetto in un bucket di origine non elimina mai un oggetto replicato nella destinazione. Se sia il bucket di origine che quello di destinazione sono entrambi con versione, il marker di eliminazione viene replicato. Se il bucket di destinazione non è dotato di versione, l'eliminazione di un oggetto nel bucket di origine non replica il marker di eliminazione nel bucket di destinazione né elimina l'oggetto di destinazione.

Quando gli oggetti vengono replicati nel bucket di destinazione, StorageGRID li contrassegna come "repliche". Un bucket StorageGRID di destinazione non replicerà gli oggetti contrassegnati come repliche, proteggendoti da loop di replica accidentali. Questo contrassegno di replica è interno a StorageGRID e non impedisce di sfruttare AWS CRR quando si utilizza un bucket Amazon S3 come destinazione.

> L'intestazione personalizzata utilizzata per contrassegnare una replica è `x-ntap-sg-replica`. Questo contrassegno impedisce un mirror a cascata. StorageGRID supporta un CloudMirror bidirezionale tra due griglie.

L'unicità e l'ordinamento degli eventi nel bucket di destinazione non sono garantiti. Più di una copia identica di un oggetto di origine potrebbe essere consegnata alla destinazione in seguito alle operazioni eseguite per garantire il successo della consegna. In rari casi, quando lo stesso oggetto viene aggiornato simultaneamente da due o più siti StorageGRID diversi, l'ordine delle operazioni sul bucket di destinazione potrebbe non corrispondere all'ordine degli eventi sul bucket di origine.

La replica di CloudMirror è generalmente configurata per utilizzare un bucket S3 esterno come destinazione. Tuttavia, è anche possibile configurare la replica in modo che utilizzi un'altra implementazione StorageGRID o qualsiasi servizio compatibile con S3.

È possibile attivare la notifica degli eventi per un bucket S3 se si desidera che StorageGRID invii notifiche relative agli eventi specificati a un cluster Kafka di destinazione o a un servizio di notifica Amazon Simple.

È possibile "configurare le notifiche degli eventi" Associando XML di configurazione delle notifiche a un bucket di origine. La configurazione delle notifiche XML segue le convenzioni S3 per la configurazione delle notifiche bucket, con l'argomento Kafka o Amazon SNS di destinazione specificato come URN di un endpoint.

Le notifiche degli eventi vengono create nel bucket di origine come specificato nella configurazione della notifica e vengono inviate alla destinazione. Se un evento associato a un oggetto ha esito positivo, viene creata una notifica relativa a tale evento e messa in coda per il recapito.

L'unicità e l'ordine delle notifiche non sono garantiti. È possibile che più di una notifica di un evento venga inviata alla destinazione a seguito delle operazioni eseguite per garantire il successo della consegna. Inoltre, poiché la consegna è asincrona, non è garantito che l'ordine temporale delle notifiche alla destinazione corrisponda all'ordine degli eventi nel bucket di origine, in particolare per le operazioni provenienti da diversi siti StorageGRID. È possibile utilizzare `sequencer` Digitare il messaggio dell'evento per determinare l'ordine degli eventi per un particolare oggetto, come descritto nella documentazione di Amazon S3.

Notifiche e messaggi supportati

Le notifiche degli eventi StorageGRID seguono l'API Amazon S3 con alcune limitazioni:

- Sono supportati i seguenti tipi di evento:
  - s3:ObjectCreated:*
  - s3:ObjectCreated:put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copy
  - s3:ObjectCreated:CompleteMultipartUpload
  - s3:ObjectRemoved:*
  - s3:ObjectRemoved:Elimina
  - s3:ObjectRemoved:DeleteMarkerCreated
  - s3:ObjectRestore:Post
- Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ma non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nella tabella:

Nome della chiave	Valore StorageGRID
EventSource	`sgws:s3`
AwsRegion	non incluso
x-amz-id-2	non incluso
arn	`urn:sgws:s3:::bucket_name`

È possibile attivare l'integrazione della ricerca per un bucket S3 se si desidera utilizzare un servizio di ricerca e analisi dei dati esterno per i metadati degli oggetti.

Il servizio di integrazione della ricerca è un servizio StorageGRID personalizzato che invia automaticamente e in modo asincrono i metadati dell'oggetto S3 a un endpoint di destinazione ogni volta che un oggetto o i relativi metadati vengono aggiornati. Potrai quindi utilizzare sofisticati strumenti di ricerca, analisi dei dati, visualizzazione o apprendimento automatico forniti dal servizio di destinazione per cercare, analizzare e ottenere informazioni dai dati degli oggetti.

È possibile attivare il servizio di integrazione della ricerca per qualsiasi bucket con versione o senza versione. L'integrazione della ricerca viene configurata associando XML di configurazione della notifica dei metadati al bucket che specifica gli oggetti su cui agire e la destinazione dei metadati dell'oggetto.

Le notifiche vengono generate sotto forma di un documento JSON denominato con il nome del bucket, il nome dell'oggetto e l'ID della versione, se presenti. Ogni notifica di metadati contiene un set standard di metadati di sistema per l'oggetto, oltre a tutti i tag dell'oggetto e ai metadati dell'utente.

> Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Prima di configurare il servizio di integrazione della ricerca, è necessario attivare le mappature dinamiche dei campi sull'indice. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Le notifiche vengono generate e messe in coda per la consegna ogni volta che:

- Viene creato un oggetto.
- Un oggetto viene eliminato, anche quando gli oggetti vengono eliminati in seguito all'operazione della policy ILM della griglia.
- I tag o i metadati degli oggetti vengono aggiunti, aggiornati o cancellati. L'insieme completo di metadati e tag viene sempre inviato in seguito all'aggiornamento, non solo i valori modificati.

Dopo aver aggiunto XML per la configurazione delle notifiche dei metadati a un bucket, vengono inviate notifiche per i nuovi oggetti creati e per gli oggetti modificati aggiornando i dati, i metadati dell'utente o i tag. Tuttavia, non vengono inviate notifiche per oggetti già presenti nel bucket. Per garantire che i metadati degli oggetti per tutti gli oggetti nel bucket vengano inviati alla destinazione, eseguire una delle seguenti operazioni:

- Configurare il servizio di integrazione della ricerca subito dopo la creazione del bucket e prima di aggiungere oggetti.
- Eseguire un'azione su tutti gli oggetti già presenti nel bucket che attiverà l'invio di un messaggio di notifica dei metadati alla destinazione.

Il servizio di integrazione della ricerca di StorageGRID supporta un cluster Elasticsearch come destinazione. Come per gli altri servizi della piattaforma, la destinazione viene specificata nell'endpoint il cui URN viene utilizzato nel XML di configurazione per il servizio. Utilizzare "Tool di matrice di interoperabilità NetApp" Per determinare le versioni supportate di Elasticsearch.

Informazioni correlate

"XML di configurazione per l'integrazione della ricerca"

"Metadati degli oggetti inclusi nelle notifiche dei metadati"

"JSON generato dal servizio di integrazione della ricerca"

"Configurare il servizio di integrazione della ricerca"

Considerazioni per i servizi della piattaforma

Prima di implementare i servizi della piattaforma, esaminare i consigli e le considerazioni per l'utilizzo di questi servizi.

Per informazioni su S3, vedere "UTILIZZARE L'API REST S3".

Considerazioni sull'utilizzo dei servizi della piattaforma

Considerazione	Dettagli
Monitoraggio degli endpoint di destinazione	È necessario monitorare la disponibilità di ciascun endpoint di destinazione. Se la connettività all'endpoint di destinazione viene persa per un periodo di tempo prolungato ed esiste un grande backlog di richieste, le richieste client aggiuntive (come LE richieste PUT) a StorageGRID non avranno esito positivo. È necessario riprovare queste richieste non riuscite quando l'endpoint diventa raggiungibile.
Rallentamento dell'endpoint di destinazione	Il software StorageGRID potrebbe ridurre le richieste S3 in entrata per un bucket se la velocità con cui le richieste vengono inviate supera la velocità con cui l'endpoint di destinazione può ricevere le richieste. La limitazione si verifica solo quando è presente un backlog di richieste in attesa di essere inviate all'endpoint di destinazione. L'unico effetto visibile è che l'esecuzione delle richieste S3 in entrata richiederà più tempo. Se si inizia a rilevare performance significativamente più lente, è necessario ridurre il tasso di acquisizione o utilizzare un endpoint con capacità superiore. Se il backlog delle richieste continua a crescere, le operazioni del client S3 (come LE richieste PUT) finiranno per fallire. È più probabile che le richieste CloudMirror siano influenzate dalle performance dell'endpoint di destinazione, perché queste richieste comportano in genere un maggior numero di trasferimenti di dati rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.
Garanzie di ordinazione	StorageGRID garantisce l'ordine delle operazioni su un oggetto all'interno di un sito. Finché tutte le operazioni relative a un oggetto si trovano all'interno dello stesso sito, lo stato finale dell'oggetto (per la replica) sarà sempre uguale allo stato in StorageGRID. StorageGRID tenta al meglio di ordinare le richieste quando le operazioni vengono eseguite nei siti StorageGRID. Ad esempio, se si scrive inizialmente un oggetto nel sito A e successivamente si sovrascrive lo stesso oggetto nel sito B, l'oggetto finale replicato da CloudMirror nel bucket di destinazione non è garantito come l'oggetto più recente.

Considerazione	Dettagli
Eliminazioni di oggetti basate su ILM	Per far fronte al comportamento di eliminazione del CRR AWS e del servizio di notifica Amazon Simple, CloudMirror e le richieste di notifica degli eventi non vengono inviate quando un oggetto nel bucket di origine viene eliminato a causa delle regole ILM di StorageGRID. Ad esempio, se una regola ILM elimina un oggetto dopo 14 giorni, non viene inviata alcuna richiesta di notifica di CloudMirror o di evento. Al contrario, le richieste di integrazione della ricerca vengono inviate quando gli oggetti vengono eliminati a causa di ILM.
Utilizzo degli endpoint Kafka	Per gli endpoint Kafka, il TLS reciproco non è supportato. Di conseguenza, se avete `ssl.client.auth` impostare su `required` Nella configurazione del broker Kafka, potrebbe causare problemi di configurazione degli endpoint Kafka. L'autenticazione degli endpoint Kafka utilizza i seguenti tipi di autenticazione. Questi tipi sono diversi da quelli utilizzati per l'autenticazione di altri endpoint, come Amazon SNS, e richiedono credenziali per nome utente e password. • SASL/SEMPLICE • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Nota:** le impostazioni proxy di archiviazione configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Considerazioni sull'utilizzo del servizio di replica CloudMirror

Considerazione	Dettagli
Stato della replica	StorageGRID non supporta `x-amz-replication-status` intestazione.
Dimensione dell'oggetto	La dimensione massima per gli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è 5 TIB, che corrisponde alla dimensione massima dell'oggetto *supportata*. **Nota**: La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.
Versioni e ID della versione del bucket	Se il bucket S3 di origine in StorageGRID ha attivato la versione, è necessario attivare anche la versione per il bucket di destinazione. Quando si utilizza la versione, tenere presente che l'ordinamento delle versioni degli oggetti nel bucket di destinazione è il massimo sforzo e non garantito dal servizio CloudMirror, a causa delle limitazioni del protocollo S3. **Nota**: Gli ID della versione per il bucket di origine in StorageGRID non sono correlati agli ID della versione per il bucket di destinazione.

Considerazione	Dettagli
Tagging per le versioni degli oggetti	Il servizio CloudMirror non replica le richieste PutObjectTagging o DeleteObjectTagging che forniscono un ID di versione, a causa delle limitazioni del protocollo S3. Poiché gli ID di versione per l'origine e la destinazione non sono correlati, non esiste alcun modo per garantire che venga replicato un aggiornamento del tag a un ID di versione specifico. Al contrario, il servizio CloudMirror replica le richieste PutObjectTagging o DeleteObjectTagging che non specificano un ID di versione. Queste richieste aggiornano i tag per la chiave più recente (o la versione più recente se il bucket è in versione). Vengono replicati anche i normali ingest con tag (senza tagging degli aggiornamenti).
Caricamenti multiparte e. `ETag` valori	Quando si esegue il mirroring degli oggetti caricati utilizzando un caricamento multiparte, il servizio CloudMirror non conserva le parti. Di conseguenza, il `ETag` il valore dell'oggetto mirrorato sarà diverso da `ETag` valore dell'oggetto originale.
Oggetti crittografati con SSE-C (crittografia lato server con chiavi fornite dal cliente)	Il servizio CloudMirror non supporta gli oggetti crittografati con SSE-C. Se si tenta di acquisire un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione non riesce.
Bucket con blocco oggetti S3 attivato	Se il bucket S3 di destinazione per la replica CloudMirror ha S3 Object Lock attivato, il tentativo di configurare la replica bucket (PutBucketReplication) non riesce e viene visualizzato un errore AccessDenied.

Configurare gli endpoint dei servizi della piattaforma

Prima di poter configurare un servizio di piattaforma per un bucket, è necessario configurare almeno un endpoint in modo che sia la destinazione del servizio di piattaforma.

L'accesso ai servizi della piattaforma viene attivato per tenant da un amministratore di StorageGRID. Per creare o utilizzare un endpoint di servizi di piattaforma, è necessario essere un utente tenant con autorizzazione di accesso Gestisci endpoint o root, in una griglia la cui rete è stata configurata per consentire ai nodi di storage di accedere alle risorse esterne degli endpoint. Per un singolo tenant, è possibile configurare un massimo di 500 endpoint di servizi della piattaforma. Per ulteriori informazioni, contattare l'amministratore di StorageGRID.

Che cos'è un endpoint di servizi di piattaforma?

Quando si crea un endpoint di servizi di piattaforma, si specificano le informazioni necessarie a StorageGRID per accedere alla destinazione esterna.

Ad esempio, se si desidera replicare gli oggetti da un bucket StorageGRID a un bucket Amazon S3, si crea un endpoint dei servizi della piattaforma che include le informazioni e le credenziali necessarie a StorageGRID per accedere al bucket di destinazione su Amazon.

Ogni tipo di servizio di piattaforma richiede un proprio endpoint, pertanto è necessario configurare almeno un endpoint per ogni servizio di piattaforma che si intende utilizzare. Dopo aver definito un endpoint di servizi di piattaforma, si utilizza l'URN dell'endpoint come destinazione nel XML di configurazione utilizzato per attivare il

servizio.

È possibile utilizzare lo stesso endpoint della destinazione per più bucket di origine. Ad esempio, è possibile configurare diversi bucket di origine per inviare metadati di oggetto allo stesso endpoint di integrazione della ricerca, in modo da poter eseguire ricerche in più bucket. È inoltre possibile configurare un bucket di origine per utilizzare più endpoint come destinazione, che consente di eseguire operazioni quali l'invio di notifiche sulla creazione di oggetti a un argomento Amazon Simple Notification Service (Amazon SNS) e notifiche sull'eliminazione di oggetti a un secondo argomento Amazon SNS.

Endpoint per la replica di CloudMirror

StorageGRID supporta endpoint di replica che rappresentano i bucket S3. Questi bucket potrebbero essere ospitati su Amazon Web Services, sullo stesso o in un'implementazione remota di StorageGRID o su un altro servizio.

Endpoint per le notifiche

StorageGRID supporta gli endpoint Amazon SNS e Kafka. Gli endpoint SQS (Simple Queue Service) o AWS Lambda non sono supportati.

Per gli endpoint Kafka, il TLS reciproco non è supportato. Di conseguenza, se avete `ssl.client.auth` impostare su `required` Nella configurazione del broker Kafka, potrebbe causare problemi di configurazione degli endpoint Kafka.

Endpoint per il servizio di integrazione della ricerca

StorageGRID supporta endpoint di integrazione della ricerca che rappresentano cluster Elasticsearch. Questi cluster di Elasticsearch possono trovarsi in un data center locale o in un cloud AWS o altrove.

L'endpoint di integrazione della ricerca si riferisce a un tipo e un indice Elasticsearch specifici. È necessario creare l'indice in Elasticsearch prima di creare l'endpoint in StorageGRID, altrimenti la creazione dell'endpoint non avrà esito positivo. Non è necessario creare il tipo prima di creare l'endpoint. StorageGRID crea il tipo, se necessario, quando invia i metadati dell'oggetto all'endpoint.

Informazioni correlate

"Amministrare StorageGRID"

Specificare URN per l'endpoint dei servizi della piattaforma

Quando si crea un endpoint dei servizi della piattaforma, è necessario specificare un nome di risorsa (URN) univoco. Verrà utilizzato l'URN per fare riferimento all'endpoint quando si crea un XML di configurazione per il servizio di piattaforma. L'URN per ciascun endpoint deve essere univoco.

StorageGRID convalida gli endpoint dei servizi della piattaforma durante la loro creazione. Prima di creare un endpoint di servizi di piattaforma, verificare che la risorsa specificata nell'endpoint esista e che sia possibile raggiungerla.

Elementi DI URNA

L'URN per un endpoint di servizi di piattaforma deve iniziare con entrambi `arn:aws` oppure `urn:mysite`, come segue:

- Se il servizio è ospitato su Amazon Web Services (AWS), utilizzare `arn:aws`

- Se il servizio è ospitato su Google Cloud Platform (GCP), utilizzare `arn:aws`
- Se il servizio è ospitato localmente, utilizzare `urn:mysite`

Ad esempio, se si specifica l'URN per un endpoint CloudMirror ospitato su StorageGRID, l'URN potrebbe iniziare con `urn:sgws`.

L'elemento successivo dell'URN specifica il tipo di servizio della piattaforma, come segue:

Servizio	Tipo
Replica di CloudMirror	`s3`
Notifiche	`sns` oppure `kafka`
Integrazione della ricerca	`es`

Ad esempio, per continuare a specificare l'URN per un endpoint CloudMirror ospitato su StorageGRID, è necessario aggiungere `s3` per ottenere `urn:sgws:s3`.

L'elemento finale dell'URN identifica la risorsa di destinazione specifica nell'URI di destinazione.

Servizio	Risorsa specifica
Replica di CloudMirror	`bucket-name`
Notifiche	`sns-topic-name` oppure `kafka-topic-name`
Integrazione della ricerca	`domain-name/index-name/type-name` **Nota:** se il cluster Elasticsearch è **non** configurato per creare gli indici automaticamente, è necessario creare l'indice manualmente prima di creare l'endpoint.

Urns per i servizi ospitati su AWS e GCP

Per le entità AWS e GCP, l'URN completo è un ARN AWS valido. Ad esempio:

- Replica di CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notifiche:

```
arn:aws:sns:region:account-id:topic-name
```

- Integrazione della ricerca:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

Per un endpoint di integrazione della ricerca AWS, il `domain-name` deve includere la stringa letterale `domain/`, come mostrato qui.

Urns per servizi in hosting locale

Quando si utilizzano servizi ospitati in locale invece di servizi cloud, è possibile specificare l'URN in qualsiasi modo che crei un URN valido e univoco, purché l'URN includa gli elementi richiesti nella terza e ultima posizione. È possibile lasciare vuoti gli elementi indicati da opzionale oppure specificarli in qualsiasi modo che consenta di identificare la risorsa e rendere l'URN unico. Ad esempio:

- Replica di CloudMirror:

  ```
  urn:mysite:s3:optional:optional:bucket-name
  ```

  Per un endpoint CloudMirror ospitato su StorageGRID, è possibile specificare un URN valido che inizia con `urn:sgws`:

  ```
  urn:sgws:s3:optional:optional:bucket-name
  ```

- Notifiche:

  Specificare un endpoint di Amazon Simple Notification Service:

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Specificare un endpoint Kafka:

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

- Integrazione della ricerca:

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

  Per gli endpoint di integrazione della ricerca ospitati localmente, il `domain-name` L'elemento può essere qualsiasi stringa, purché l'URN dell'endpoint sia univoco.

Creare endpoint di servizi di piattaforma

È necessario creare almeno un endpoint del tipo corretto prima di poter attivare un

servizio di piattaforma.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire gli endpoint o l'autorizzazione di accesso root".
- La risorsa a cui fa riferimento l'endpoint dei servizi della piattaforma è stata creata:
  - Replica di CloudMirror: Bucket S3
  - Notifica dell'evento: Argomento Kafka o Amazon Simple Notification Service (Amazon SNS)
  - Notifica di ricerca: Indice Elasticsearch, se il cluster di destinazione non è configurato per creare automaticamente gli indici.
- Si dispone delle informazioni relative alla risorsa di destinazione:
  - Host e porta per l'Uniform Resource Identifier (URI)

    > Se si prevede di utilizzare un bucket ospitato su un sistema StorageGRID come endpoint per la replica di CloudMirror, contattare l'amministratore del grid per determinare i valori da inserire.

  - Nome risorsa univoco (URN)

    "Specificare URN per l'endpoint dei servizi della piattaforma"

  - Credenziali di autenticazione (se richieste):

Endpoint di integrazione della ricerca

Per gli endpoint di integrazione della ricerca, è possibile utilizzare le seguenti credenziali:

- Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key
- HTTP di base: Nome utente e password

Endpoint di replica CloudMirror

Per la replica di CloudMirror, è possibile utilizzare le seguenti credenziali:

- Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key
- CAP (C2S Access Portal): URL con credenziali temporanee, certificati server e client, chiavi client e passphrase opzionale con chiave privata del client.

Endpoint Amazon SNS

Per gli endpoint Amazon SNS, è possibile utilizzare le seguenti credenziali:

- Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key

Endpoint Kafka

Per gli endpoint Kafka, è possibile utilizzare le seguenti credenziali:

- SASL/PLAIN: Nome utente e password
- SASL/SCRAM-SHA-256: Nome utente e password
- SASL/SCRAM-SHA-512: Nome utente e password

  - Certificato di protezione (se si utilizza un certificato CA personalizzato)

- Se le funzioni di protezione di Elasticsearch sono attivate, si dispone del privilegio del cluster di monitoraggio per il test di connettività e del privilegio di scrittura dell'indice o di entrambi i privilegi di indice e di eliminazione per gli aggiornamenti dei documenti.

Fasi

1. Selezionare **STORAGE (S3)** > **Platform Services Endpoint**. Viene visualizzata la pagina Platform Services Endpoint.
2. Selezionare **Crea endpoint**.
3. Inserire un nome visualizzato per descrivere brevemente l'endpoint e il suo scopo.

   Il tipo di servizio della piattaforma supportato dall'endpoint viene visualizzato accanto al nome dell'endpoint quando viene elencato nella pagina degli endpoint, quindi non è necessario includere tali informazioni nel nome.

4. Nel campo **URI**, specificare l'URI (Unique Resource Identifier) dell'endpoint.

   Utilizzare uno dei seguenti formati:

```
https://host:port
http://host:port
```

Se non si specifica una porta, vengono utilizzate le seguenti porte predefinite:

- Porta 443 per URI HTTPS e porta 80 per URI HTTP (la maggior parte degli endpoint)
- Porta 9092 per URI HTTPS e HTTP (solo endpoint Kafka)

Ad esempio, l'URI per un bucket ospitato su StorageGRID potrebbe essere:

```
https://s3.example.com:10443
```

In questo esempio, `s3.example.com` Rappresenta la voce DNS per l'IP virtuale (VIP) del gruppo ha (StorageGRID High Availability), e. `10443` rappresenta la porta definita nell'endpoint del bilanciamento del carico.

> Quando possibile, è necessario connettersi a un gruppo ha di nodi per il bilanciamento del carico per evitare un singolo punto di errore.

Analogamente, l'URI per un bucket ospitato su AWS potrebbe essere:

```
https://s3-aws-region.amazonaws.com
```

> Se l'endpoint viene utilizzato per il servizio di replica CloudMirror, non includere il nome del bucket nell'URI. Il nome del bucket viene incluso nel campo **URN**.

5. Immettere il nome di risorsa (URN) univoco per l'endpoint.

> Non è possibile modificare l'URN di un endpoint dopo la creazione dell'endpoint.

6. Selezionare **continua**.
7. Selezionare un valore per **tipo di autenticazione**.

Endpoint di integrazione della ricerca

Immettere o caricare le credenziali per un endpoint di integrazione della ricerca.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta
HTTP di base	Utilizza un nome utente e una password per autenticare le connessioni alla destinazione.	• Nome utente • Password

Endpoint di replica CloudMirror

Immettere o caricare le credenziali per un endpoint di replica CloudMirror.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta
CAP (portale di accesso C2S)	Utilizza certificati e chiavi per autenticare le connessioni alla destinazione.	• URL temporaneo delle credenziali • Certificato CA del server (caricamento file PEM) • Certificato client (caricamento file PEM) • Chiave privata del client (caricamento file PEM, formato crittografato OpenSSL o formato chiave privata non crittografato) • Passphrase della chiave privata del client (opzionale)

Endpoint Amazon SNS

Immettere o caricare le credenziali per un endpoint Amazon SNS.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta

Endpoint Kafka

Immettere o caricare le credenziali per un endpoint Kafka.

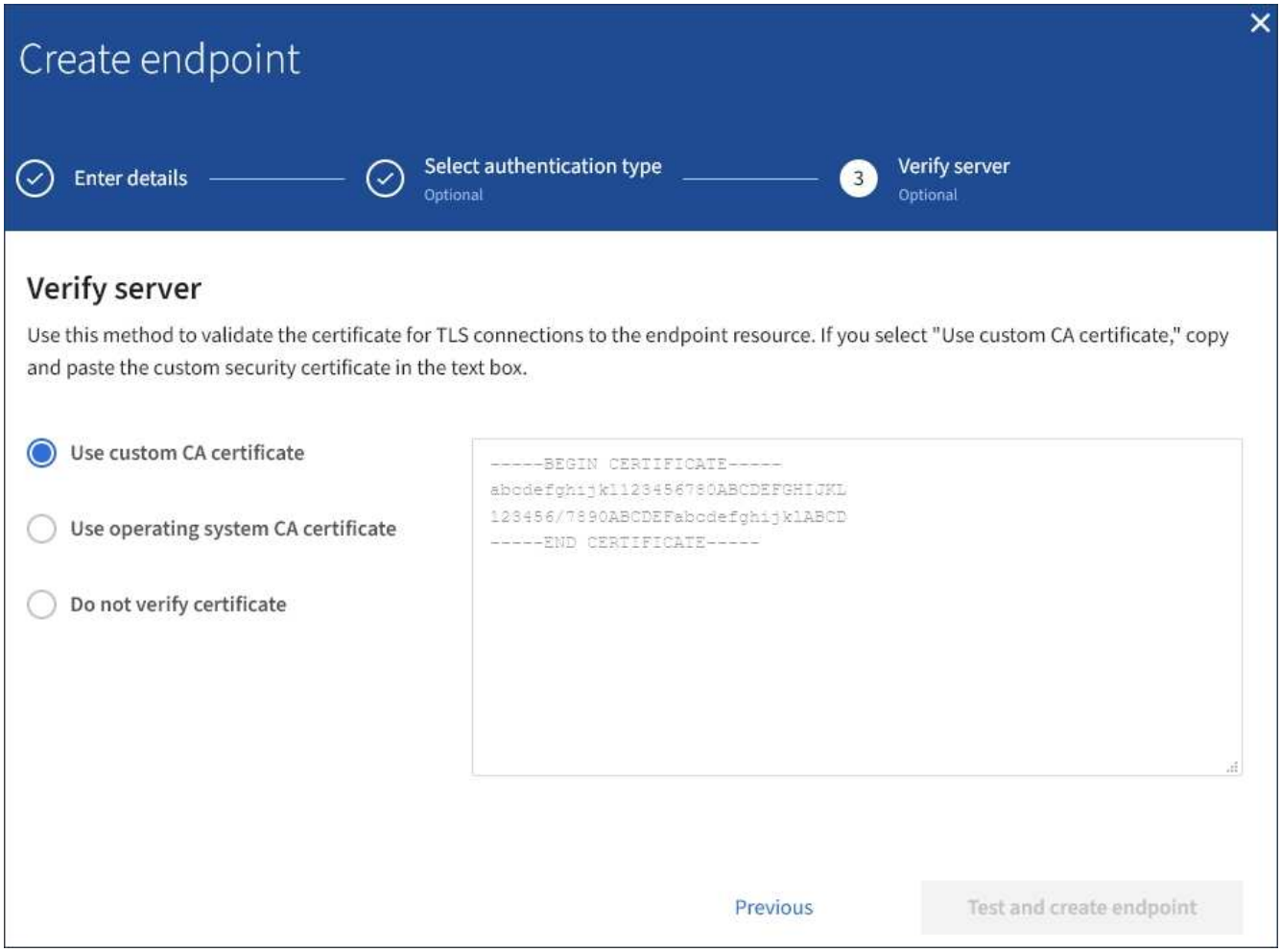
Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
SASL/SEMPLICE	Utilizza un nome utente e una password con testo normale per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-256	Utilizza un nome utente e una password utilizzando un protocollo di risposta alla verifica e l'hash SHA-256 per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-512	Utilizza un nome utente e una password utilizzando un protocollo di risposta alla verifica e l'hash SHA-512 per autenticare le connessioni alla destinazione.	• Nome utente • Password

Selezionare **Usa autenticazione con delega** se il nome utente e la password sono derivati da un token di delega ottenuto da un cluster Kafka.

8. Selezionare **continua**.

9. Selezionare un pulsante di opzione per **verify server** (verifica server) per scegliere la modalità di verifica della connessione TLS all'endpoint.



Tipo di verifica del certificato	Descrizione
USA certificato CA personalizzato	Utilizzare un certificato di protezione personalizzato. Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo **certificato CA**.
Utilizzare il certificato CA del sistema operativo	Utilizzare il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato. Questa opzione non è sicura.

10. Selezionare **Test e creare endpoint**.
    - Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene convalidata da un nodo in ogni sito.
    - Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Se è necessario modificare l'endpoint per correggere l'errore, selezionare **Torna ai dettagli dell'endpoint** e aggiornare le informazioni. Quindi, selezionare **Test e creare endpoint**.

La creazione dell'endpoint non riesce se i servizi della piattaforma non sono abilitati per l'account tenant. Contattare l'amministratore di StorageGRID.

Dopo aver configurato un endpoint, è possibile utilizzare il relativo URN per configurare un servizio di piattaforma.

Informazioni correlate

"Specificare URN per l'endpoint dei servizi della piattaforma"

"Configurare la replica di CloudMirror"

"Configurare le notifiche degli eventi"

"Configurare il servizio di integrazione della ricerca"

Verifica della connessione per l'endpoint dei servizi della piattaforma

Se la connessione a un servizio della piattaforma è stata modificata, è possibile verificare la connessione per l'endpoint per verificare l'esistenza della risorsa di destinazione e che sia possibile raggiungerla utilizzando le credenziali specificate.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire gli endpoint o l'autorizzazione di accesso root".

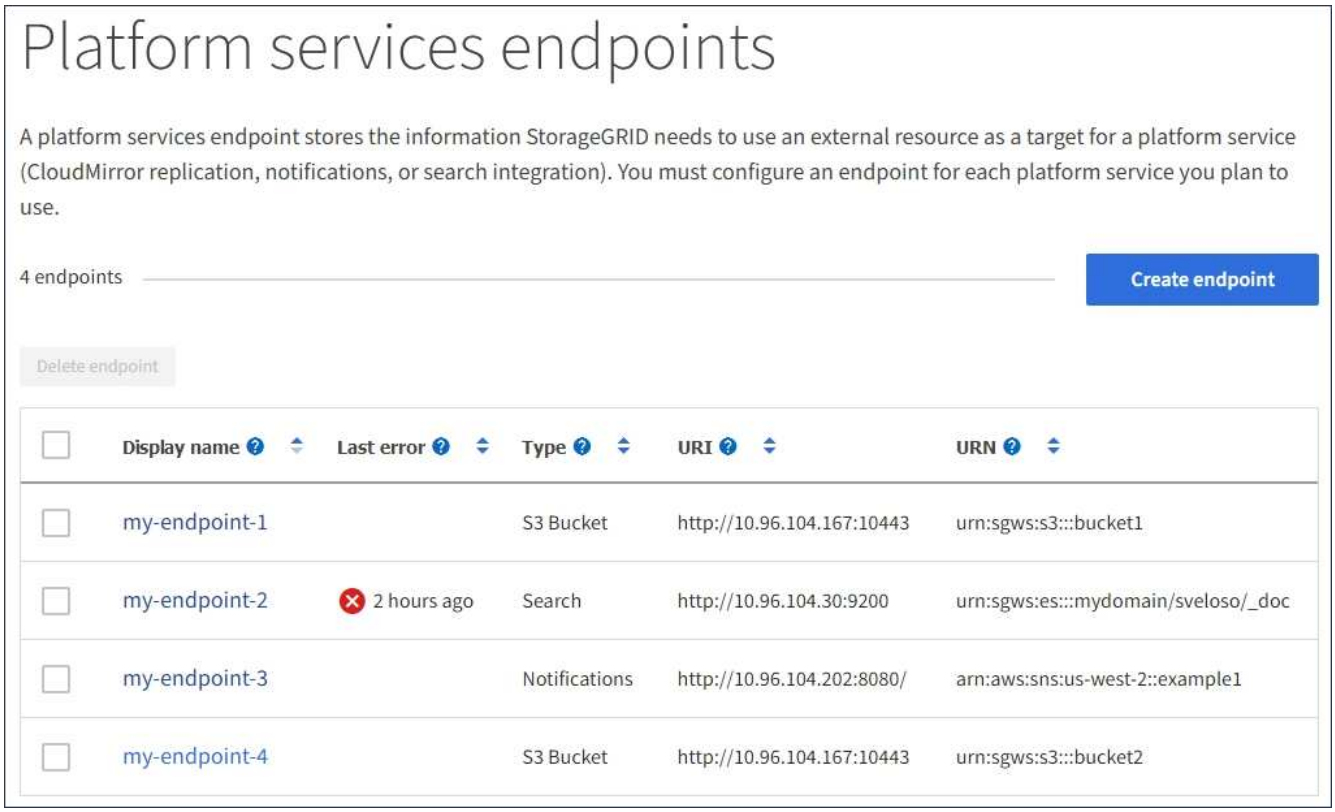
A proposito di questa attività

StorageGRID non convalida che le credenziali dispongano delle autorizzazioni corrette.

Fasi

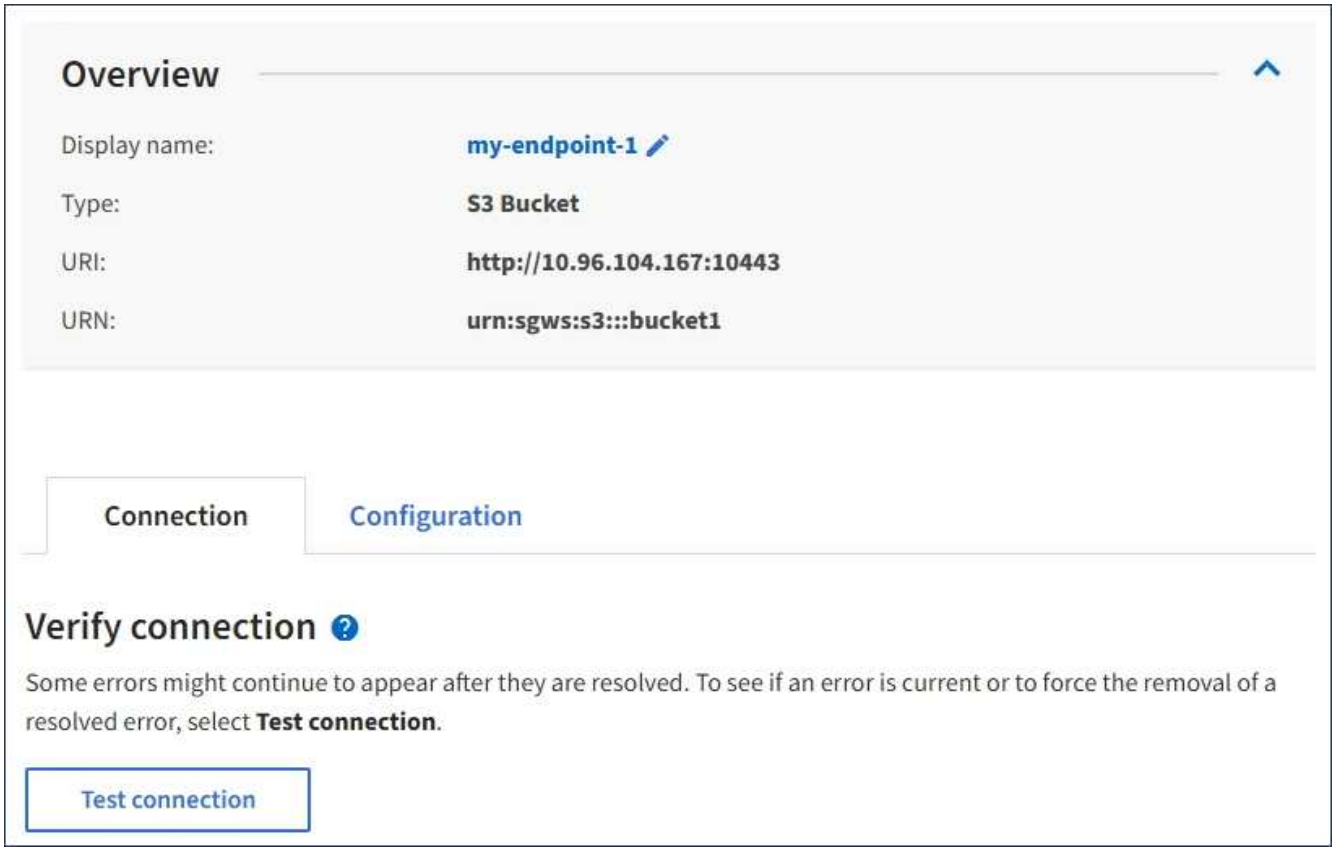
1. Selezionare **STORAGE (S3)** > **Platform Services Endpoint**.

   Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.



2. Selezionare l'endpoint di cui si desidera verificare la connessione.

   Viene visualizzata la pagina dei dettagli dell'endpoint.



3. Selezionare **Test di connessione**.

- Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene convalidata da un nodo in ogni sito.
- Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Se è necessario modificare l'endpoint per correggere l'errore, selezionare **Configuration** (Configurazione) e aggiornare le informazioni. Quindi, selezionare **Test e salvare le modifiche**.

Modifica dell'endpoint dei servizi della piattaforma

È possibile modificare la configurazione di un endpoint di servizi di piattaforma per modificarne il nome, l'URI o altri dettagli. Ad esempio, potrebbe essere necessario aggiornare le credenziali scadute o modificare l'URI in modo che punti a un indice Elasticsearch di backup per il failover. Non è possibile modificare l'URN per un endpoint di servizi di piattaforma.

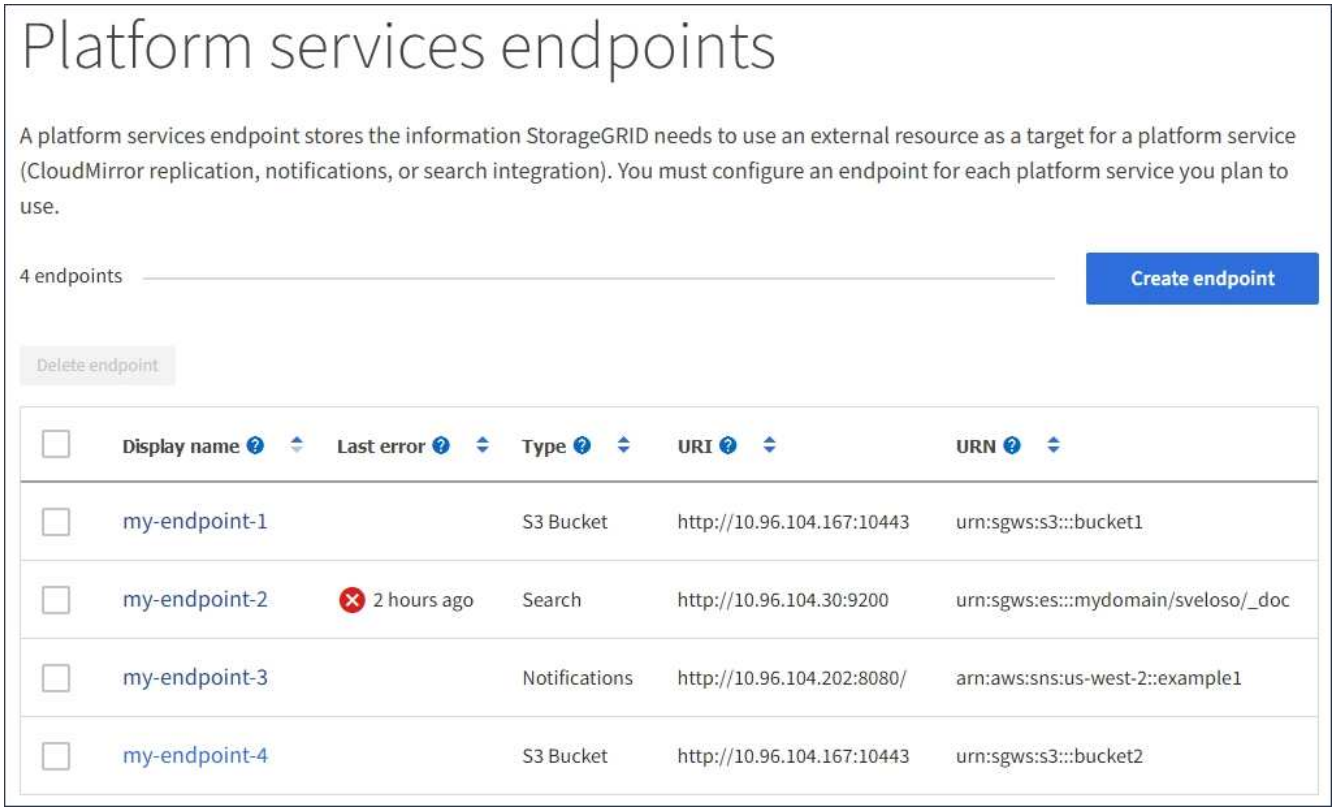
Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire gli endpoint o l'autorizzazione di accesso root".

Fasi

1. Selezionare **STORAGE (S3)** > **Platform Services Endpoint**.

   Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.



2. Selezionare l'endpoint che si desidera modificare.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Configurazione**.
4. Se necessario, modificare la configurazione dell'endpoint.

   Non è possibile modificare l'URN di un endpoint dopo la creazione dell'endpoint.

   a. Per modificare il nome visualizzato per l'endpoint, selezionare l'icona di modifica .
   b. Se necessario, modificare l'URI.
   c. Se necessario, modificare il tipo di autenticazione.
      - Per l'autenticazione della chiave di accesso, modificare la chiave in base alle necessità selezionando **Modifica chiave S3** e incollando un nuovo ID della chiave di accesso e una chiave di accesso segreta. Se si desidera annullare le modifiche, selezionare **Ripristina modifica tasto S3**.
      - Per l'autenticazione CAP (C2S Access Portal), modificare l'URL delle credenziali temporanee o la passphrase della chiave privata del client opzionale e caricare nuovi file di certificato e chiavi in base alle necessità.

        La chiave privata del client deve essere in formato crittografato OpenSSL o non crittografato.

   d. Se necessario, modificare il metodo di verifica del server.
5. Selezionare **Test e salvare le modifiche**.
   - Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene verificata da un nodo in ogni sito.
   - Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Modificare l'endpoint per correggere l'errore, quindi selezionare **Test e salvare le modifiche**.

Eliminare l'endpoint dei servizi della piattaforma

È possibile eliminare un endpoint se non si desidera più utilizzare il servizio di piattaforma associato.

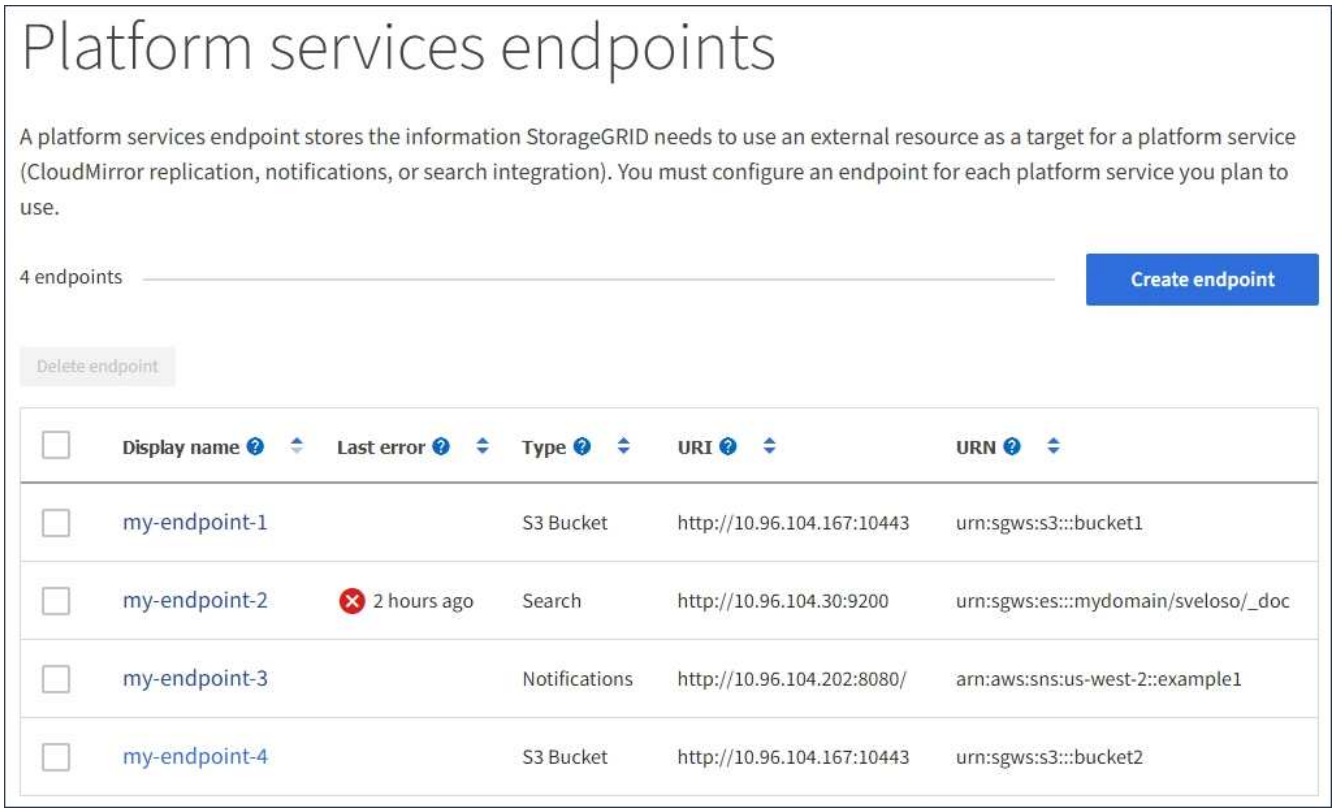
Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire gli endpoint o l'autorizzazione di accesso root".

Fasi

1. Selezionare **STORAGE (S3)** > **Platform Services Endpoint**.

   Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.

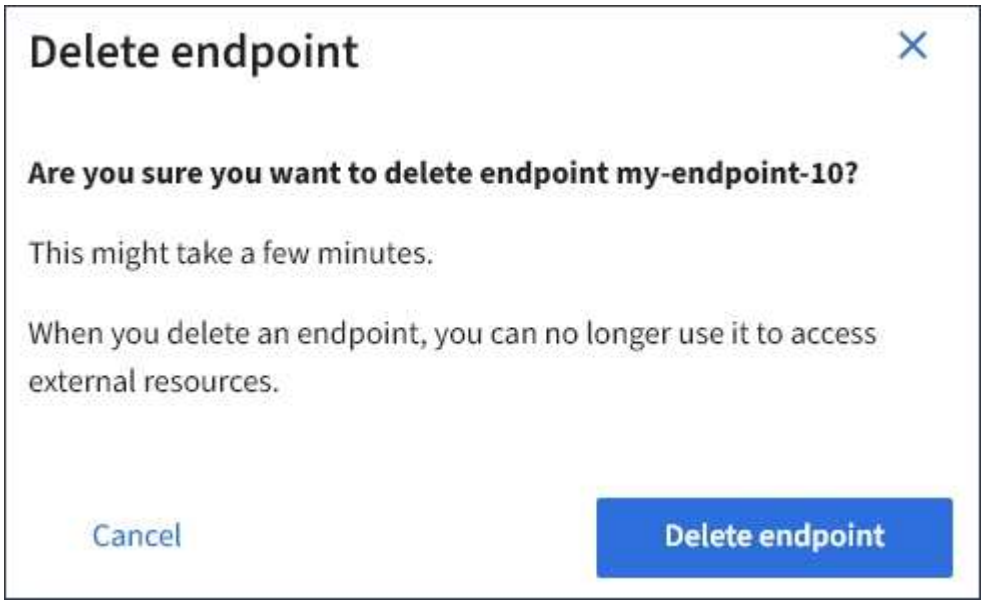


2. Selezionare la casella di controllo per ciascun endpoint che si desidera eliminare.

> Se elimini un endpoint di servizi di piattaforma in uso, il servizio di piattaforma associato verrà disattivato per tutti i bucket che utilizzano l'endpoint. Tutte le richieste non ancora completate verranno interrotte. Le nuove richieste continueranno a essere generate fino a quando non si modifica la configurazione del bucket per non fare più riferimento all'URN cancellato. StorageGRID segnalerà queste richieste come errori irrecuperabili.

3. Selezionare **azioni** > **Elimina endpoint**.

   Viene visualizzato un messaggio di conferma.



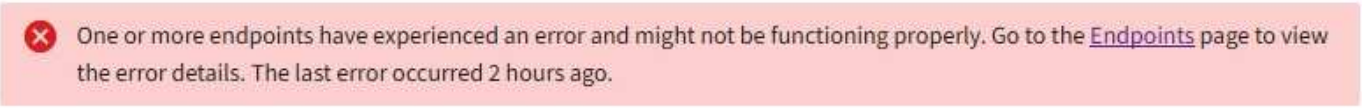
4. Selezionare **Delete endpoint** (Elimina endpoint).

Risolvere gli errori degli endpoint dei servizi della piattaforma

Se si verifica un errore quando StorageGRID tenta di comunicare con un endpoint dei servizi della piattaforma, viene visualizzato un messaggio sul dashboard. Nella pagina Platform Services Endpoint, la colonna Last error (ultimo errore) indica per quanto tempo si è verificato l'errore. Se le autorizzazioni associate alle credenziali di un endpoint non sono corrette, non viene visualizzato alcun errore.

Determinare se si è verificato un errore

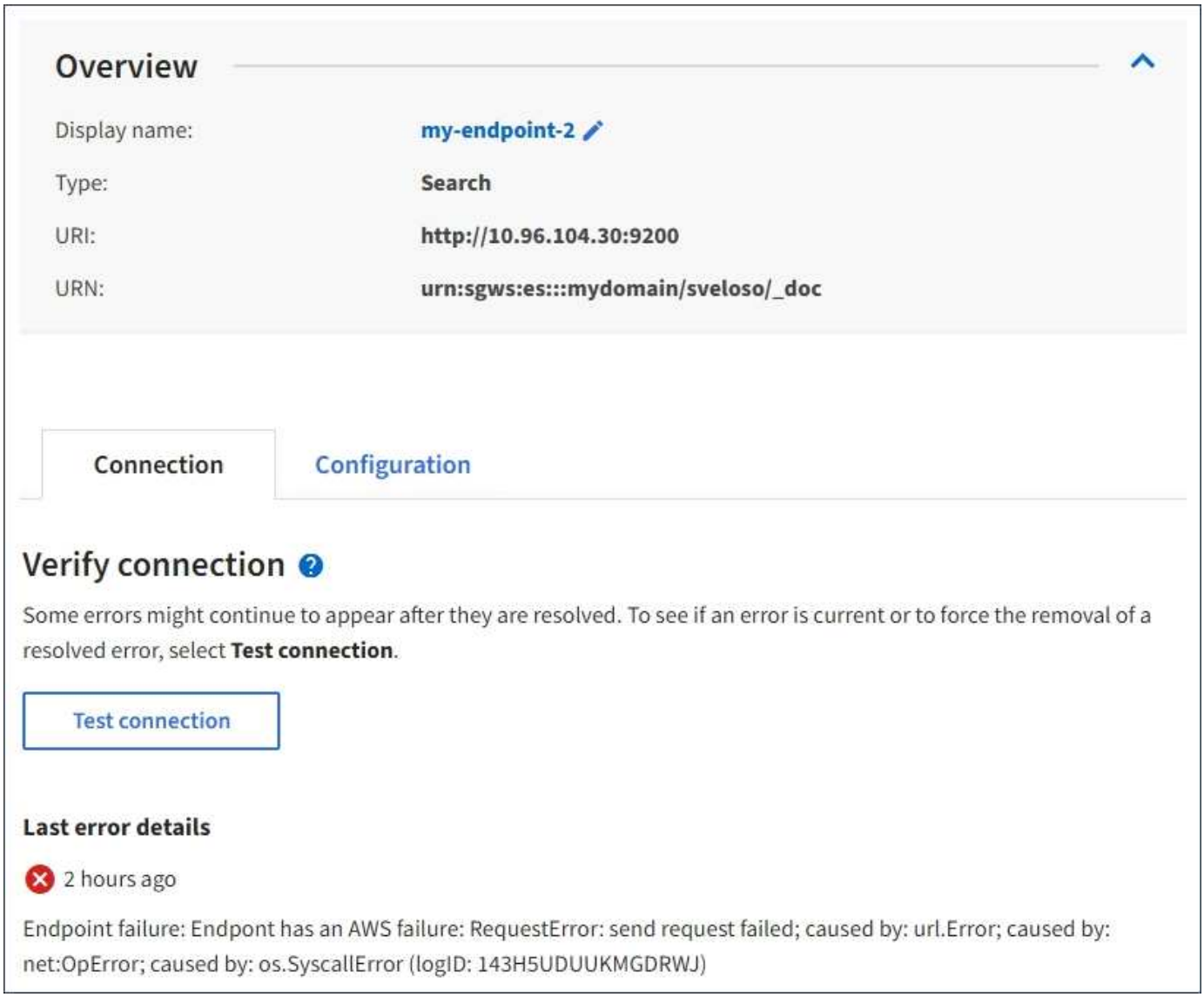
Se si sono verificati errori degli endpoint dei servizi della piattaforma negli ultimi 7 giorni, la dashboard di Tenant Manager visualizza un messaggio di avviso. Per ulteriori informazioni sull'errore, visitare la pagina relativa agli endpoint dei servizi della piattaforma.



Lo stesso errore visualizzato nella dashboard viene visualizzato anche nella parte superiore della pagina Platform Services Endpoint. Per visualizzare un messaggio di errore più dettagliato:

Fasi

1. Dall'elenco degli endpoint, selezionare l'endpoint che presenta l'errore.
2. Nella pagina dei dettagli dell'endpoint, selezionare **connessione**. Questa scheda visualizza solo l'errore più recente per un endpoint e indica quanto tempo fa si è verificato l'errore. Errori che includono l'icona X rossa si è verificato negli ultimi 7 giorni.



Controllare se l'errore è ancora aggiornato

Alcuni errori potrebbero continuare a essere visualizzati nella colonna **ultimo errore** anche dopo la risoluzione. Per verificare se un errore è corrente o per forzare la rimozione di un errore risolto dalla tabella:

Fasi

1. Selezionare l'endpoint.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

2. Selezionare **connessione** > **verifica connessione**.

Selezionando **verifica connessione**, StorageGRID convalida l'esistenza dell'endpoint dei servizi della piattaforma e può essere raggiunto con le credenziali correnti. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Risolvi gli errori degli endpoint

È possibile utilizzare il messaggio **Last error** (ultimo errore) nella pagina dei dettagli dell'endpoint per determinare la causa dell'errore. Alcuni errori potrebbero richiedere la modifica dell'endpoint per risolvere il

problema. Ad esempio, se StorageGRID non riesce ad accedere al bucket S3 di destinazione perché non dispone delle autorizzazioni di accesso corrette o la chiave di accesso è scaduta, può verificarsi un errore di CloudMirroring. Il messaggio è "è necessario aggiornare le credenziali dell'endpoint o l'accesso alla destinazione" e i dettagli sono "AccessDenied" o "InvalidAccessKeyId".

Se è necessario modificare l'endpoint per risolvere un errore, selezionando **verifica e salva modifiche** StorageGRID convalida l'endpoint aggiornato e conferma che è possibile raggiungerlo con le credenziali correnti. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Fasi

1. Selezionare l'endpoint.
2. Nella pagina dei dettagli dell'endpoint, selezionare **Configurazione**.
3. Modificare la configurazione dell'endpoint in base alle necessità.
4. Selezionare **connessione** > **verifica connessione**.

Credenziali endpoint con autorizzazioni insufficienti

Quando StorageGRID convalida un endpoint di servizi di piattaforma, conferma che le credenziali dell'endpoint possono essere utilizzate per contattare la risorsa di destinazione ed esegue un controllo delle autorizzazioni di base. Tuttavia, StorageGRID non convalida tutte le autorizzazioni richieste per determinate operazioni di servizi della piattaforma. Per questo motivo, se si riceve un errore quando si tenta di utilizzare un servizio di piattaforma (ad esempio "403 Proibito"), controllare le autorizzazioni associate alle credenziali dell'endpoint.

Informazioni correlate

- **Amministrare StorageGRID › risolvere i problemi relativi ai servizi della piattaforma**
- "Creare endpoint di servizi di piattaforma"
- "Verifica della connessione per l'endpoint dei servizi della piattaforma"
- "Modifica dell'endpoint dei servizi della piattaforma"

Configurare la replica di CloudMirror

Il "Servizio di replica di CloudMirror" È uno dei tre servizi della piattaforma StorageGRID. È possibile utilizzare la replica CloudMirror per replicare automaticamente gli oggetti in un bucket S3 esterno.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- È già stato creato un bucket per fungere da origine della replica.
- L'endpoint che si intende utilizzare come destinazione per la replica CloudMirror esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

La replica di CloudMirror copia gli oggetti da un bucket di origine a un bucket di destinazione specificato in un endpoint.

La replica di CloudMirror presenta importanti analogie e differenze con la funzionalità di replica cross-grid. Per ulteriori informazioni, vedere "Confronta la replica cross-grid e la replica CloudMirror".

Per attivare la replica CloudMirror per un bucket, è necessario creare e applicare un XML di configurazione di replica bucket valido. L'XML di configurazione della replica deve utilizzare l'URN di un endpoint del bucket S3 per ciascuna destinazione.

La replica non è supportata per i bucket di origine o di destinazione con blocco oggetti S3 attivato.

Per informazioni generali sulla replica bucket e su come configurarla, vedere "Documentazione di Amazon Simple Storage Service (S3): Replica di oggetti". Per informazioni su come StorageGRID implementa GetBucketReplication, DeleteBucketReplication e PutBucketReplication, vedere "Operazioni sui bucket".

Se si attiva la replica CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket vengono replicati, ma gli oggetti esistenti nel bucket non vengono replicati. È necessario aggiornare gli oggetti esistenti per attivare la replica.

Se si specifica una classe di storage nell'XML di configurazione della replica, StorageGRID utilizza tale classe quando esegue operazioni sull'endpoint S3 di destinazione. L'endpoint di destinazione deve supportare anche la classe di storage specificata. Assicurarsi di seguire le raccomandazioni fornite dal vendor del sistema di destinazione.

Fasi

1. Abilita la replica per il bucket di origine:

   Utilizzare un editor di testo per creare l'XML di configurazione della replica richiesto per attivare la replica, come specificato nell'API di replica S3. Durante la configurazione dell'XML:

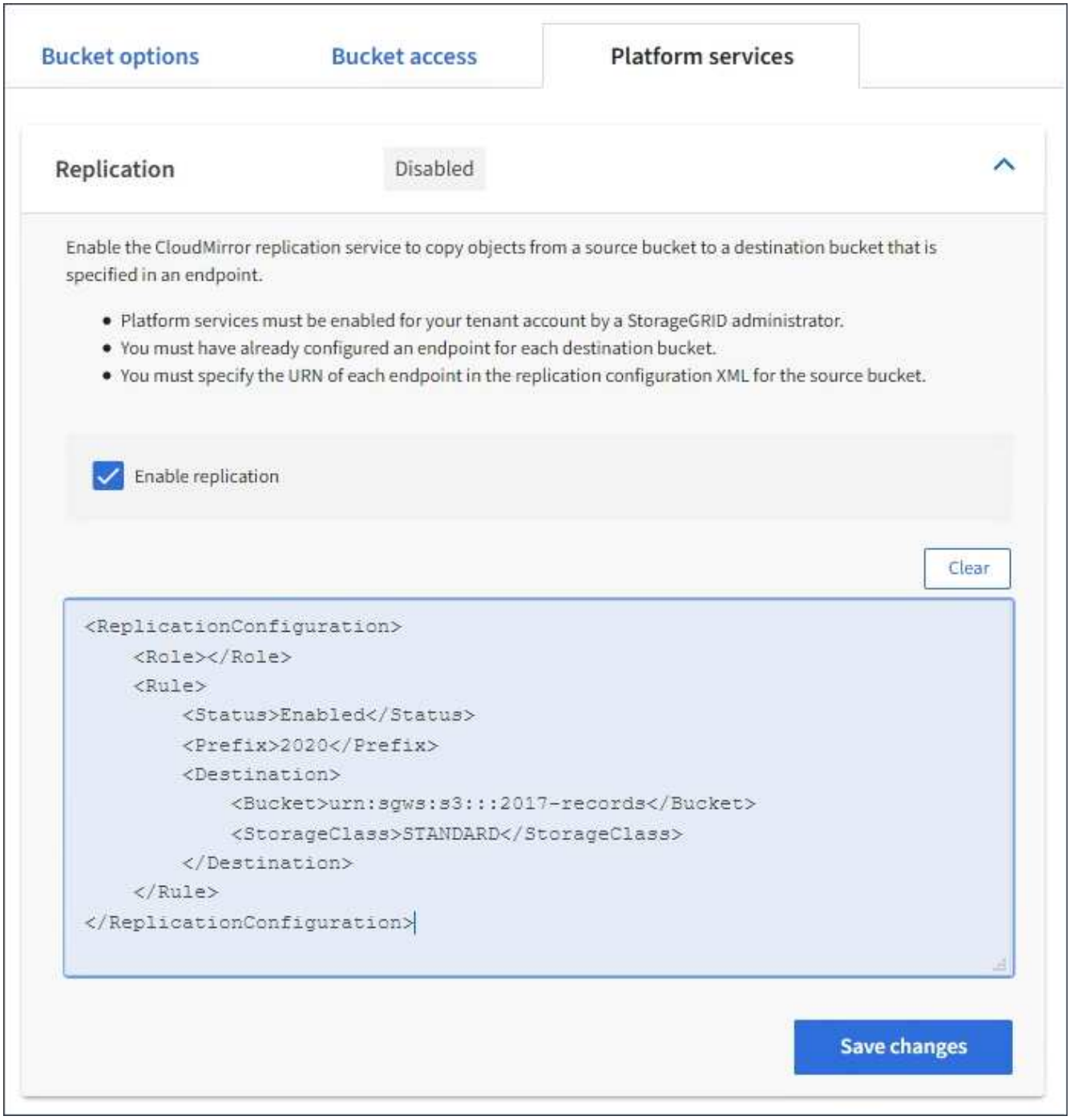
   - Tenere presente che StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo di `Filter` Per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per ulteriori informazioni, consultare la documentazione di Amazon sulla configurazione della replica.
   - Utilizzare l'URN di un endpoint del bucket S3 come destinazione.
   - Se si desidera, aggiungere `<StorageClass>` e specificare una delle seguenti opzioni:
     - `STANDARD`: La classe di storage predefinita. Se non si specifica una classe di storage quando si carica un oggetto, il `STANDARD` viene utilizzata la classe di storage.
     - `STANDARD_IA`: (Standard - accesso non frequente). Utilizzare questa classe di storage per i dati a cui si accede meno frequentemente, ma che richiedono comunque un accesso rapido quando necessario.
     - `REDUCED_REDUNDANCY`: Utilizzare questa classe di storage per i dati non critici e riproducibili che possono essere memorizzati con una ridondanza inferiore rispetto a. `STANDARD` classe di storage.
   - Se si specifica un `Role` Nel file XML di configurazione, verrà ignorato. Questo valore non viene utilizzato da StorageGRID.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **STORAGE (S3)** > **bucket**.
3. Selezionare il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services** > **Replication**.
5. Selezionare la casella di controllo **Enable Replication** (attiva replica).
6. Incollare il file XML di configurazione della replica nella casella di testo e selezionare **Save changes** (Salva modifiche).



I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID utilizzando l'API di gestione griglia o di gestione griglia. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che la replica sia configurata correttamente:
   a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per la replica come specificato nella configurazione della replica.

      Nell'esempio illustrato in precedenza, gli oggetti che corrispondono al prefisso "2020" vengono replicati.

b. Verificare che l'oggetto sia stato replicato nel bucket di destinazione.

   Per gli oggetti di piccole dimensioni, la replica avviene rapidamente.

Informazioni correlate

"Creare endpoint di servizi di piattaforma"

Configurare le notifiche degli eventi

Il servizio di notifica è uno dei tre servizi della piattaforma StorageGRID. È possibile abilitare le notifiche per un bucket per inviare informazioni su eventi specifici a un cluster o servizio Kafka di destinazione che supporta AWS Simple Notification Service (Amazon SNS).

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- Hai già creato un bucket per fungere da origine delle notifiche.
- L'endpoint che si intende utilizzare come destinazione per le notifiche degli eventi esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

Dopo aver configurato le notifiche degli eventi, ogni volta che si verifica un evento specifico per un oggetto nel bucket di origine, viene generata una notifica e inviata all'argomento Amazon SNS o Kafka utilizzato come endpoint di destinazione. Per attivare le notifiche per un bucket, è necessario creare e applicare un XML di configurazione delle notifiche valido. L'XML di configurazione delle notifiche deve utilizzare l'URN di un endpoint delle notifiche degli eventi per ciascuna destinazione.

Per informazioni generali sulle notifiche degli eventi e su come configurarle, consulta la documentazione Amazon. Per informazioni su come StorageGRID implementa l'API di configurazione delle notifiche bucket S3, vedere "Istruzioni per l'implementazione delle applicazioni client S3".

Se si abilitano le notifiche degli eventi per un bucket che contiene oggetti, le notifiche vengono inviate solo per le azioni eseguite dopo il salvataggio della configurazione della notifica.

Fasi

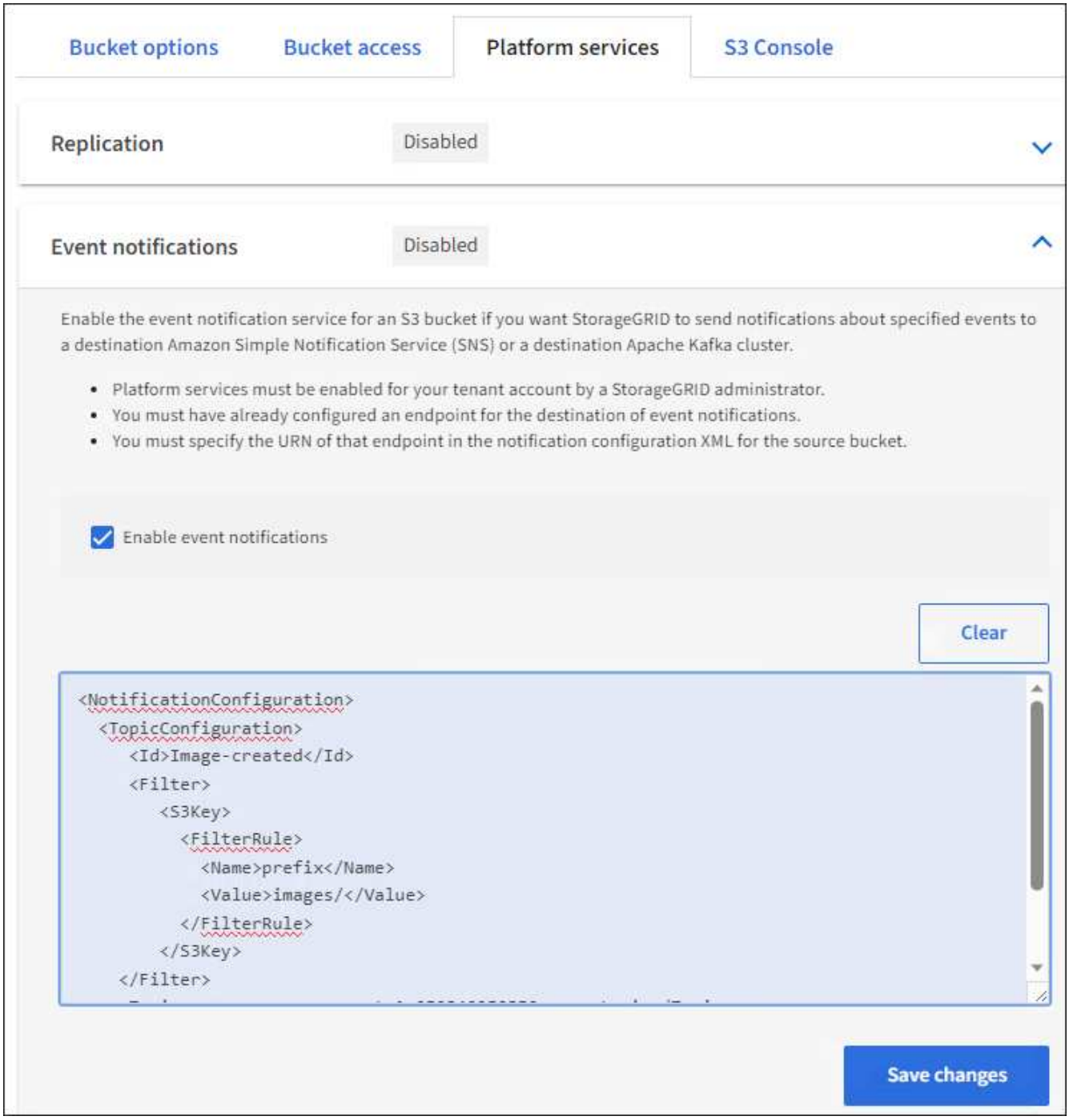
1. Abilita le notifiche per il bucket di origine:
   - Utilizzare un editor di testo per creare l'XML di configurazione delle notifiche richiesto per attivare le notifiche degli eventi, come specificato nell'API di notifica S3.
   - Quando si configura l'XML, utilizzare l'URN di un endpoint di notifica degli eventi come argomento di destinazione.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. In Tenant Manager, selezionare **STORAGE (S3)** > **Bucket**.
3. Selezionare il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services** > **Event Notifications**.
5. Selezionare la casella di controllo **attiva notifiche eventi**.
6. Incollare l'XML di configurazione della notifica nella casella di testo e selezionare **Salva modifiche**.



I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID utilizzando l'API di gestione griglia o di gestione griglia. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che le notifiche degli eventi siano configurate correttamente:

   a. Eseguire un'azione su un oggetto nel bucket di origine che soddisfi i requisiti per l'attivazione di una notifica come configurato nel XML di configurazione.

      Nell'esempio, viene inviata una notifica di evento ogni volta che viene creato un oggetto con `images/` prefisso.

b. Conferma che è stata inviata una notifica all'argomento Amazon SNS o Kafka di destinazione.

   Ad esempio, se l'argomento di destinazione è ospitato su Amazon SNS, è possibile configurare il servizio in modo che invii un'e-mail al momento della consegna della notifica.


```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


+
Se la notifica viene ricevuta nell'argomento di destinazione, il bucket di origine è stato configurato correttamente per le notifiche StorageGRID.

Informazioni correlate

"Comprendere le notifiche per i bucket"

"UTILIZZARE L'API REST S3"

"Creare endpoint di servizi di piattaforma"

Utilizza il servizio di integrazione della ricerca

Il servizio di integrazione della ricerca è uno dei tre servizi della piattaforma StorageGRID. È possibile consentire a questo servizio di inviare metadati di oggetti a un indice di ricerca della destinazione ogni volta che un oggetto viene creato, cancellato o i relativi metadati o tag vengono aggiornati.

È possibile configurare l'integrazione della ricerca utilizzando Gestione tenant per applicare XML di configurazione StorageGRID personalizzato a un bucket.

> Poiché il servizio di integrazione della ricerca fa sì che i metadati degli oggetti vengano inviati a una destinazione, il relativo XML di configurazione viene definito *metadata notification Configuration XML*. Questo XML di configurazione è diverso dal *XML di configurazione delle notifiche* utilizzato per attivare le notifiche degli eventi.

Vedere "Istruzioni per l'implementazione delle applicazioni client S3" Per informazioni dettagliate sulle seguenti operazioni REST API personalizzate di StorageGRID S3:

- ELIMINA la configurazione di notifica dei metadati del bucket
- OTTIENI la configurazione della notifica dei metadati del bucket
- INSERIRE la configurazione della notifica dei metadati del bucket

Informazioni correlate

"XML di configurazione per l'integrazione della ricerca"

"Metadati degli oggetti inclusi nelle notifiche dei metadati"

"JSON generato dal servizio di integrazione della ricerca"

"Configurare il servizio di integrazione della ricerca"

"UTILIZZARE L'API REST S3"

XML di configurazione per l'integrazione della ricerca

Il servizio di integrazione della ricerca viene configurato utilizzando una serie di regole contenute in `<MetadataNotificationConfiguration>` e. `</MetadataNotificationConfiguration>` tag. Ogni regola specifica gli oggetti a cui si applica la regola e la destinazione in cui StorageGRID deve inviare i metadati di tali oggetti.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, è possibile inviare metadati per oggetti con il prefisso `images` a una destinazione e metadati per gli oggetti con il prefisso `videos` a un altro. Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento

dell'invio. Ad esempio, una configurazione che include una regola per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2` non consentito.

Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID creato per il servizio di integrazione della ricerca. Questi endpoint si riferiscono a un indice e a un tipo definiti in un cluster Elasticsearch.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

La tabella descrive gli elementi contenuti nel file XML di configurazione per la notifica dei metadati.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfiguration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi della regola.	Sì
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato. Le regole con prefissi sovrapposti vengono rifiutate. Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola. Incluso nell'elemento Rule.	No

Nome	Descrizione	Obbligatorio
Stato	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì
Urna	URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • `es` deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel form `domain-name/myindex/mytype`. Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404. L'URN è incluso nell'elemento Destination.	Sì

Utilizza l'XML di configurazione delle notifiche dei metadati di esempio per scoprire come creare il tuo XML.

Configurazione della notifica dei metadati applicabile a tutti gli oggetti

In questo esempio, i metadati degli oggetti per tutti gli oggetti vengono inviati alla stessa destinazione.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Configurazione della notifica dei metadati con due regole

In questo esempio, i metadati degli oggetti per gli oggetti che corrispondono al prefisso `/images` viene inviato a una destinazione, mentre i metadati degli oggetti per gli oggetti che corrispondono al prefisso `/videos` viene inviato a una seconda destinazione.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informazioni correlate

"UTILIZZARE L'API REST S3"

"Metadati degli oggetti inclusi nelle notifiche dei metadati"

"JSON generato dal servizio di integrazione della ricerca"

"Configurare il servizio di integrazione della ricerca"

Configurare il servizio di integrazione della ricerca

Il servizio di integrazione della ricerca 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.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- È già stato creato un bucket S3 di cui si desidera indicizzare il contenuto.
- L'endpoint che si intende utilizzare come destinazione per il servizio di integrazione della ricerca esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

Dopo aver configurato il servizio di integrazione della ricerca per un bucket di origine, la creazione di un oggetto o l'aggiornamento dei metadati o dei tag di un oggetto attiva l'invio dei metadati dell'oggetto all'endpoint di destinazione. Se abiliti il servizio di integrazione della ricerca per un bucket che contiene già oggetti, le notifiche dei metadati non vengono inviate automaticamente per gli oggetti esistenti. È necessario aggiornare questi oggetti esistenti per assicurarsi che i relativi metadati vengano aggiunti all'indice di ricerca della destinazione.

Fasi

1. Utilizzare un editor di testo per creare l'XML di notifica dei metadati necessario per abilitare l'integrazione della ricerca.
   - Per l'integrazione della ricerca, consultare le informazioni relative all'XML di configurazione.
   - Quando si configura l'XML, utilizzare l'URN di un endpoint di integrazione della ricerca come destinazione.

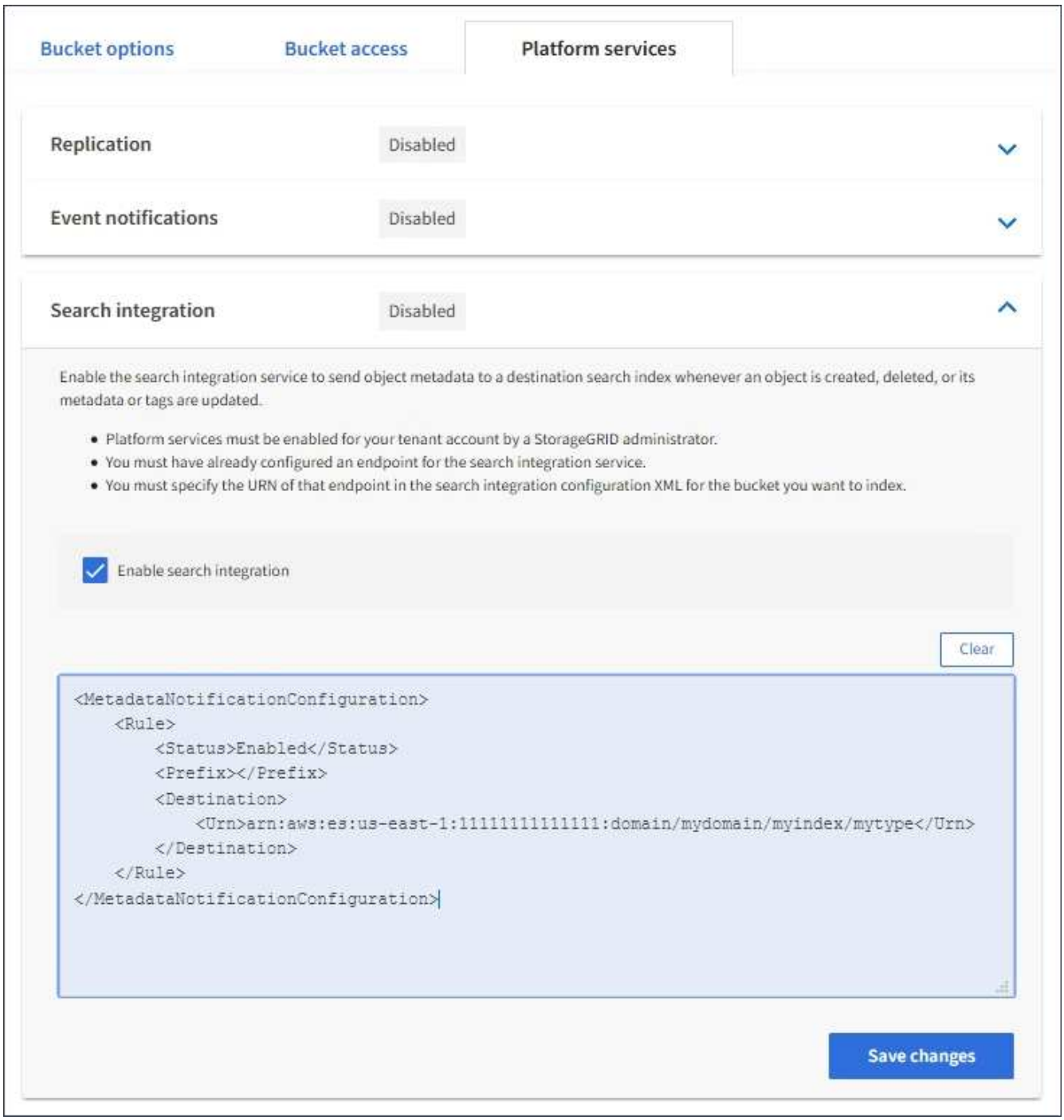
```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. In Tenant Manager, selezionare **STORAGE (S3)** > **Bucket**.
3. Selezionare il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services** > **Search Integration**

5. Selezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).
6. Incollare la configurazione di notifica dei metadati nella casella di testo e selezionare **Salva modifiche**.



I servizi della piattaforma devono essere attivati per ciascun account tenant da un amministratore StorageGRID utilizzando il gestore di griglia o l'API di gestione. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che il servizio di integrazione della ricerca sia configurato correttamente:
   a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per l'attivazione di una notifica dei metadati come specificato nel file XML di configurazione.

Nell'esempio illustrato in precedenza, tutti gli oggetti aggiunti al bucket attivano una notifica dei metadati.

b. Verificare che un documento JSON contenente i metadati e i tag dell'oggetto sia stato aggiunto all'indice di ricerca specificato nell'endpoint.

Al termine

Se necessario, è possibile disattivare l'integrazione della ricerca per un bucket utilizzando uno dei seguenti metodi:

- Selezionare **STORAGE (S3)** > **Bucket** e deselezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).
- Se si utilizza direttamente l'API S3, utilizzare una richiesta DI notifica DELETE Bucket metadata. Consultare le istruzioni per l'implementazione delle applicazioni client S3.

Informazioni correlate

"Comprendere il servizio di integrazione della ricerca"

"XML di configurazione per l'integrazione della ricerca"

"UTILIZZARE L'API REST S3"

"Creare endpoint di servizi di piattaforma"

JSON generato dal servizio di integrazione della ricerca

Quando si attiva il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato all'endpoint di destinazione ogni volta che vengono aggiunti, aggiornati o cancellati metadati o tag dell'oggetto.

Questo esempio mostra un esempio di JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. Il `test` bucket non è configurato, quindi il `versionId` tag vuoto.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadati degli oggetti inclusi nelle notifiche dei metadati

La tabella elenca tutti i campi inclusi nel documento JSON che viene inviato all'endpoint di destinazione quando è attivata l'integrazione della ricerca.

Il nome del documento include il nome del bucket, il nome dell'oggetto e l'ID della versione, se presente.

Tipo	Nome e descrizione dell'elemento
Informazioni su bucket e oggetti	`bucket`: Nome del bucket
`key`: Nome chiave oggetto	`versionID`: Versione oggetto, per gli oggetti nei bucket con versione
`region`: Area bucket, ad esempio `us-east-1`	Metadati di sistema
`size`: Dimensione dell'oggetto (in byte) come visibile a un client HTTP	`md5`: Hash di oggetto
Metadati dell'utente	`metadata`: Tutti i metadati dell'utente per l'oggetto, come coppie chiave-valore `key:value`
Tag	`tags`: Tutti i tag di oggetto definiti per l'oggetto, come coppie chiave-valore `key:value`

Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Prima di configurare il servizio di integrazione della ricerca, è necessario attivare le mappature dinamiche dei campi sull'indice. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

UTILIZZARE L'API REST S3

Versioni e aggiornamenti supportati dall'API REST S3

StorageGRID supporta l'API S3 (Simple Storage Service), implementata come set di servizi Web REST (Representational state Transfer).

Il supporto per l'API REST S3 consente di connettere le applicazioni orientate ai servizi sviluppate per i servizi Web S3 con lo storage a oggetti on-premise che utilizza il sistema StorageGRID. Sono necessarie modifiche minime all'utilizzo corrente delle chiamate API REST S3 da parte di un'applicazione client.

Versioni supportate

StorageGRID supporta le seguenti versioni specifiche di S3 e HTTP.

Elemento	Versione
Specifica API S3	"Documentazione Amazon Web Services (AWS): Riferimento API Amazon Simple Storage Service"
HTTP	1,1 Per ulteriori informazioni su HTTP, vedere HTTP/1.1 (RFC 7230-35). "IETF RFC 2616: Protocollo di trasferimento ipertestuale (HTTP/1.1)" **Nota**: StorageGRID non supporta la pipelining HTTP/1.1.

Aggiornamenti al supporto delle API REST S3

Rilasciare	Commenti
11,8	Aggiornati i nomi delle operazioni S3 in modo che corrispondano ai nomi utilizzati nella "Documentazione Amazon Web Services (AWS): Riferimento API Amazon Simple Storage Service".
11,7	• Aggiunto "Riferimento rapido: Richieste API S3 supportate". • Aggiunto supporto per l'utilizzo della modalità DI GOVERNANCE con S3 Object Lock. • Aggiunto supporto per StorageGRID specifico `x-ntap-sg-cgr-replication-status` Intestazione di risposta per le richieste DI oggetti GET e HEAD. Questa intestazione fornisce lo stato di replica di un oggetto per la replica cross-grid. • Le richieste SelectObjectContent ora supportano gli oggetti Parquet.
11,6	• Aggiunto supporto per l'utilizzo di `partNumber` Parametro di richiesta in GET object e HEAD object requests. • Aggiunto supporto per una modalità di conservazione predefinita e un periodo di conservazione predefinito a livello di bucket per S3 Object Lock. • Aggiunto supporto per `s3:object-lock-remaining-retention-days` policy condition key (chiave condizione policy) per impostare l'intervallo di periodi di conservazione consentiti per gli oggetti. • Modifica della dimensione massima *consigliata* per un'operazione di singolo oggetto PUT in 5 GiB (5,368,709,120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.

Rilasciare	Commenti
11,5	• Aggiunto supporto per la gestione della crittografia bucket. • Aggiunto supporto per S3 Object Lock e richieste legacy di Compliance obsolete. • Aggiunto il supporto per l'utilizzo DELL'ELIMINAZIONE di più oggetti nei bucket con versione. • Il `Content-MD5` l'intestazione della richiesta è ora supportata correttamente.
11,4	• Aggiunto supporto per L'ELIMINAZIONE di tag bucket, L'AGGIUNTA DI tag bucket E L'AGGIUNTA di tag bucket. I tag di allocazione dei costi non sono supportati. • Per i bucket creati in StorageGRID 11.4, non è più necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. • Aggiunto supporto per le notifiche bucket su `s3:ObjectRestore:Post` tipo di evento. • I limiti di dimensione AWS per le parti multicpart vengono ora applicati. Ogni parte di un caricamento multiparte deve essere compresa tra 5 MiB e 5 GiB. L'ultima parte può essere inferiore a 5 MiB. • Aggiunto supporto per TLS 1.3
11,3	• Aggiunto supporto per la crittografia lato server dei dati a oggetti con chiavi fornite dal cliente (SSE-C). • Supporto aggiunto per LE operazioni DI eliminazione, GET e PUT del ciclo di vita del bucket (solo azione di scadenza) e per `x-amz-expiration` intestazione della risposta. • Aggiornamento DI PUT object, PUT object - Copy e Multippart Upload per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono durante l'acquisizione. • Le crittografia TLS 1.1 non sono più supportate.
11,2	Aggiunto supporto per il ripristino POST-oggetto da utilizzare con i Cloud Storage Pools. Aggiunto supporto per l'utilizzo della sintassi AWS per ARN, chiavi di condizione dei criteri e variabili dei criteri in policy di gruppo e bucket. Le policy di gruppo e bucket esistenti che utilizzano la sintassi StorageGRID continueranno a essere supportate. **Nota:** gli utilizzi di ARN/URN in altre configurazioni JSON/XML, inclusi quelli utilizzati nelle funzionalità personalizzate di StorageGRID, non sono cambiati.
11,1	Aggiunto supporto per la condivisione delle risorse tra origini (CORS), HTTP per connessioni client S3 ai nodi di rete e impostazioni di conformità sui bucket.
11,0	Supporto aggiunto per la configurazione dei servizi della piattaforma (replica CloudMirror, notifiche e integrazione della ricerca Elasticsearch) per i bucket. Inoltre, è stato aggiunto il supporto per i vincoli di posizione dei tag degli oggetti per i bucket e la coerenza disponibile.

Rilasciare	Commenti
10,4	Aggiunto supporto per le modifiche di scansione ILM alle versioni, agli aggiornamenti delle pagine dei nomi di dominio degli endpoint, alle condizioni e alle variabili nei criteri, agli esempi di policy e all'autorizzazione PutOverwriteObject.
10,3	Aggiunto supporto per il controllo delle versioni.
10,2	Aggiunto supporto per policy di accesso di gruppo e bucket e per copia multiparte (carica parte - Copia).
10,1	Aggiunto supporto per upload multiparte, richieste virtuali in stile host e autenticazione v4.
10,0	Supporto iniziale dell'API REST S3 da parte del sistema StorageGRID. La versione attualmente supportata del *riferimento API del servizio di storage semplice* è 2006-03-01.

Riferimento rapido: Richieste API S3 supportate

In questa pagina viene riepilogato il modo in cui StorageGRID supporta le API di Amazon Simple Storage Service (S3).

Questa pagina include solo le operazioni S3 supportate da StorageGRID.

> Per visualizzare la documentazione AWS relativa a ciascuna operazione, selezionare il collegamento nell'intestazione.

Parametri di query URI comuni e intestazioni di richiesta

Se non specificato, sono supportati i seguenti parametri di query URI comuni:

- `versionId` (come richiesto per le operazioni a oggetti)

Se non specificato, sono supportate le seguenti intestazioni di richiesta comuni:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informazioni correlate

- "Dettagli sull'implementazione dell'API REST S3"
- "Amazon Simple Storage Service API Reference: Intestazioni di richiesta comuni"

"AbortMultipartUpload"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni Per questa richiesta, più questo parametro di query URI aggiuntivo:

- `uploadId`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni per caricamenti multiparte"

"CompleteMultipartUpload"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni Per questa richiesta, più questo parametro di query URI aggiuntivo:

- `uploadId`

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

Documentazione StorageGRID

"CompleteMultipartUpload"

"Oggetto CopyObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`

- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Oggetto CopyObject"

"CreateBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `x-amz-bucket-object-lock-enabled`

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sui bucket"

"CreateMultipartUpload"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"CreateMultipartUpload"

"DeleteBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketLifecycle"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

- "Operazioni sui bucket"
- "Creare la configurazione del ciclo di vita S3"

"DeleteBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteObject (Elimina oggetto)"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, più questa intestazione di richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sugli oggetti"

"DeleteObjects"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, più questa intestazione di richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sugli oggetti"

"DeleteObjectTagging"

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sugli oggetti"

"GetBucketAcl"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketLifecycleConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

- "Operazioni sui bucket"
- "Creare la configurazione del ciclo di vita S3"

"GetBucketLocation"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketNotificationConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketVersioning"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni Per questa richiesta, più i seguenti parametri di query URI aggiuntivi:

- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

E queste intestazioni di richiesta aggiuntive:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"GetObject"

"GetObjectAcl"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sugli oggetti"

"GetObjectLegalHold"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

"GetObjectLockConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

"GetObjectRetention"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

"GetObjectTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sugli oggetti"

"HeadBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"HeadObject (oggetto intestazione)"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"HeadObject (oggetto intestazione)"

"ListBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

Operazioni sul servizio › ListBuckets

"ListMultipartUploads"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-uploads`

- `prefix`
- `upload-id-marker`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"ListMultipartUploads"

"ListObjects (oggetti elenco)"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"ListObjectsV2"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"ListObjectVersions"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"ListParts"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- `max-parts`
- `part-number-marker`
- `uploadId`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"ListMultipartUploads"

"PutBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketLifecycleConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- `And`
- `Days`
- `Expiration`
- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentazione StorageGRID

- "Operazioni sui bucket"
- "Creare la configurazione del ciclo di vita S3"

"PutBucketNotificationConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Per ulteriori informazioni sui campi corpo JSON supportati, vedere "Utilizza policy di accesso a bucket e gruppi".

"PutBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Tag XML del corpo della richiesta

- `Bucket`
- `Destination`

- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketVersioning"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Parametri del corpo della richiesta

StorageGRID supporta questi parametri del corpo della richiesta:

- `VersioningConfiguration`
- `Status`

Documentazione StorageGRID

"Operazioni sui bucket"

"PutObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `x-amz-server-side-encryption`

- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo della richiesta

- Dati binari dell'oggetto

Documentazione StorageGRID

"PutObject"

"PutObjectLegalHold"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

"PutObjectLockConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

"PutObjectRetention"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta, più questa intestazione aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

"PutObjectTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sugli oggetti"

"RestoreObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Per informazioni dettagliate sui campi corpo supportati, vedere "RestoreObject".

"SelectObjectContent"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Per ulteriori informazioni sui body field supportati, vedere quanto segue:

- "USA S3 Select"
- "SelectObjectContent"

"UploadPart"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni Per questa richiesta, più i seguenti parametri di query URI aggiuntivi:

- `partNumber`
- `uploadId`

E queste intestazioni di richiesta aggiuntive:

- `x-amz-server-side-encryption-customer-algorithm`

- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corpo della richiesta

- Dati binari della parte

Documentazione StorageGRID

"UploadPart"

"UploadPartCopy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti parametri e intestazioni comuni Per questa richiesta, più i seguenti parametri di query URI aggiuntivi:

- `partNumber`
- `uploadId`

E queste intestazioni di richiesta aggiuntive:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"UploadPartCopy"

Eseguire il test della configurazione dell'API REST S3

Puoi utilizzare l'interfaccia a riga di comando (CLI AWS) di Amazon Web Services per verificare la tua connessione al sistema e verificare che sia possibile leggere e scrivere oggetti.

Prima di iniziare

- È stata scaricata e installata la CLI AWS dal sito "aws.amazon.com/cli".
- Se lo si desidera, è necessario "creato un endpoint del bilanciamento del carico". In caso contrario, si conosce l'indirizzo IP del nodo di archiviazione a cui si desidera connettersi e il numero di porta da utilizzare. Vedere "Indirizzi IP e porte per le connessioni client".
- Lo hai fatto "Creato un account tenant S3".
- Hai effettuato l'accesso al tenant e. "ha creato una chiave di accesso".

Per ulteriori informazioni su questi passaggi, vedere "Configurare le connessioni client".

Fasi

1. Configurare le impostazioni dell'interfaccia utente di AWS per utilizzare l'account creato nel sistema StorageGRID:
   a. Accedere alla modalità di configurazione: `aws configure`
   b. Inserire l'ID della chiave di accesso per l'account creato.
   c. Inserire la chiave di accesso segreta per l'account creato.
   d. Immettere la regione predefinita da utilizzare. Ad esempio, `us-east-1`.
   e. Immettere il formato di output predefinito da utilizzare oppure premere **Invio** per selezionare JSON.
2. Creare un bucket.

   In questo esempio si presuppone che sia stato configurato un endpoint del bilanciamento del carico per utilizzare l'indirizzo IP 10.96.101.17 e la porta 10443.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   Se il bucket viene creato correttamente, viene restituita la posizione del bucket, come mostrato nell'esempio seguente:

   ```
   "Location": "/testbucket"
   ```

3. Caricare un oggetto.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   put-object --bucket testbucket --key s3.pdf --body C:\s3-
   test\upload\s3.pdf
   ```

   Se l'oggetto viene caricato correttamente, viene restituito un ETAG che rappresenta un hash dei dati dell'oggetto.

4. Elencare i contenuti del bucket per verificare che l'oggetto sia stato caricato.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Eliminare l'oggetto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Eliminare il bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Come StorageGRID implementa l'API REST S3

Richieste client in conflitto

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite".

La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Valori di coerenza

La coerenza fornisce un equilibrio tra la disponibilità degli oggetti e la loro coerenza in diversi nodi e siti storage. È possibile modificare la coerenza come richiesto dall'applicazione.

Per impostazione predefinita, StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi GET che segue UN PUT completato con successo sarà in grado di leggere i dati appena scritti. Le sovrascritture degli oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni sono coerenti. Le sovrascritture in genere richiedono secondi o minuti per la propagazione, ma possono richiedere fino a 15 giorni.

Se si desidera eseguire operazioni a oggetti con una coerenza diversa, è possibile:

- Specificare una coerenza per ogni secchio.
- Specificare una coerenza per Ogni operazione API.
- Modificare la coerenza predefinita a livello di griglia eseguendo una delle seguenti operazioni:
  - In Grid Manager, andare a **CONFIGURAZIONE** > **sistema** > **Impostazioni di archiviazione** > **coerenza predefinita**.
  - .

Una modifica alla coerenza a livello di griglia si applica solo ai bucket creati dopo la modifica dell'impostazione. Per determinare i dettagli di una modifica, vedere il registro di controllo disponibile all'indirizzo `/var/local/log` (Cercare **consistencyLevel**).

Valori di coerenza

La coerenza influisce sul modo in cui i metadati utilizzati da StorageGRID per tenere traccia degli oggetti vengono distribuiti tra i nodi e, di conseguenza, sulla disponibilità degli oggetti per le richieste dei client.

È possibile impostare la coerenza per un bucket o un'operazione API su uno dei seguenti valori:

- **All**: Tutti i nodi ricevono i dati immediatamente, oppure la richiesta non riesce.
- **Strong-Global**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
- **Strong-Site**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write**: (Default) fornisce coerenza lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available**: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Utilizzare la coerenza "Read-after-new-write" e "available"

Quando un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write", StorageGRID esegue la ricerca in più passaggi, come segue:

- Per prima cosa, cerca l'oggetto utilizzando una bassa coerenza.
- Se la ricerca non riesce, ripete la ricerca al valore di coerenza successivo finché non raggiunge una coerenza equivalente al comportamento per strong-Global.

Se un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write" ma l'oggetto non esiste, la ricerca degli oggetti raggiungerà sempre una coerenza equivalente al comportamento per strong-Global. Poiché questa coerenza richiede la disponibilità di più copie dei metadati degli oggetti in ogni sito, è possibile ricevere un elevato numero di errori del server interno 500 nel caso in cui due o più nodi storage nello stesso sito non fossero disponibili.

A meno che non si richiedano garanzie di coerenza simili a Amazon S3, è possibile evitare questi errori per le operazioni HEAD and GET impostando la coerenza su "disponibile". Quando un'operazione HEAD o GET utilizza la consistenza "disponibile", StorageGRID fornisce solo la consistenza finale. Non ritenta un'operazione non riuscita ad aumentare la coerenza, pertanto non richiede la disponibilità di più copie dei metadati degli oggetti.

specificare la coerenza per l'operazione API

Per impostare la coerenza per una singola operazione API, i valori di coerenza devono essere supportati per l'operazione ed è necessario specificare la coerenza nell'intestazione della richiesta. Nell'esempio riportato di seguito viene impostata la coerenza su "strong-Site" per un'operazione GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

È necessario utilizzare la stessa coerenza per entrambe le operazioni PutObject e GetObject.

specificare la coerenza per il bucket

Per impostare la coerenza per il bucket, è possibile utilizzare StorageGRID "METTI la coerenza del bucket" richiesta. Oppure è possibile "modificare la consistenza di un bucket" Dal responsabile del tenant.

Quando si imposta la consistenza per un secchio, tenere presente quanto segue:

- L'impostazione della consistenza per un bucket determina la consistenza utilizzata per S3 operazioni eseguite sugli oggetti nel bucket o nella configurazione del bucket. Non influisce sulle operazioni sul bucket stesso.
- La coerenza per una singola operazione API sovrascrive la coerenza per il bucket.
- In generale, i bucket devono utilizzare la coerenza predefinita, "Read-after-new-write". Se le richieste non funzionano correttamente, modificare il comportamento del client dell'applicazione, se possibile. In alternativa, configurare il client per specificare la coerenza per ogni richiesta API. Impostare la consistenza a livello del bucket solo come ultima risorsa.

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

Sia la scelta della coerenza che la regola ILM influiscono sulla protezione degli oggetti. Queste impostazioni possono interagire.

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

Quanto segue "opzioni di acquisizione" Sono disponibili per le regole ILM:

Commit doppio
: StorageGRID effettua immediatamente copie provvisorie dell'oggetto e restituisce il successo al cliente. Le copie specificate nella regola ILM vengono eseguite quando possibile.

Rigoroso
: Tutte le copie specificate nella regola ILM devono essere eseguite prima che l'operazione sia restituita al cliente.

Bilanciato
: StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono create copie provvisorie e viene restituita al cliente l'avvenuta esecuzione. Le copie specificate nella regola ILM vengono eseguite quando possibile.

Esempio di interazione tra la regola coerenza e ILM

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

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

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

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

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

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

Versione degli oggetti

È possibile impostare lo stato di versione di un bucket se si desidera mantenere più versioni di ciascun oggetto. L'abilitazione della versione per un bucket può aiutare a proteggere dalla cancellazione accidentale di oggetti e consente di recuperare e ripristinare le versioni precedenti di un oggetto.

Il sistema StorageGRID implementa il controllo delle versioni con il supporto per la maggior parte delle funzionalità e con alcune limitazioni. StorageGRID supporta fino a 1,000 versioni di ciascun oggetto.

La versione degli oggetti può essere combinata con la gestione del ciclo di vita delle informazioni di StorageGRID (ILM) o con la configurazione del ciclo di vita del bucket S3. È necessario attivare esplicitamente il controllo delle versioni per ogni bucket. Quando la versione è abilitata per un bucket, a ogni oggetto aggiunto al bucket viene assegnato un ID di versione, che viene generato dal sistema StorageGRID.

L'utilizzo dell'autenticazione MFA (multi-factor Authentication) Delete non è supportato.

> Il controllo delle versioni può essere attivato solo sui bucket creati con StorageGRID versione 10.3 o successiva.

ILM e versione

I criteri ILM vengono applicati a ogni versione di un oggetto. Un processo di scansione ILM esegue una scansione continua di tutti gli oggetti e li rivaluti in base al criterio ILM corrente. Qualsiasi modifica apportata ai criteri ILM viene applicata a tutti gli oggetti precedentemente acquisiti. Sono incluse le versioni precedentemente ingerite se è abilitato il controllo delle versioni. La scansione ILM applica le nuove modifiche ILM agli oggetti acquisiti in precedenza.

Per gli oggetti S3 nei bucket abilitati per le versioni, il supporto per le versioni consente di creare regole ILM che utilizzano "ora non corrente" come ora di riferimento (selezionare **Sì** per la domanda "Applica questa regola solo alle versioni precedenti degli oggetti?" pollici "Fase 1 della creazione guidata di una regola ILM").

Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. L'utilizzo di un filtro "tempo non corrente" consente di creare policy per ridurre l'impatto sullo storage delle versioni precedenti di oggetti.

> Quando si carica una nuova versione di un oggetto utilizzando un'operazione di caricamento multiparte, l'ora non corrente per la versione originale dell'oggetto si riflette quando il caricamento multiparte è stato creato per la nuova versione, non quando il caricamento multiparte è stato completato. In casi limitati, il tempo non corrente per la versione originale potrebbe essere di ore o giorni prima del tempo per la versione corrente.

Informazioni correlate

- "Modalità di eliminazione degli oggetti con versione S3"
- "Regole e criteri ILM per gli oggetti con versione S3 (esempio 4)".

Utilizzare l'API REST S3 per configurare il blocco oggetti S3

Se l'impostazione blocco oggetti S3 globale è attivata per il sistema StorageGRID, è possibile creare bucket con blocco oggetti S3 attivato. È possibile specificare la conservazione predefinita per ogni bucket o impostazioni di conservazione per ciascuna versione dell'oggetto.

Come attivare il blocco oggetti S3 per un bucket

Se l'impostazione globale di blocco oggetti S3 è attivata per il sistema StorageGRID, è possibile attivare il blocco oggetti S3 quando si crea ciascun bucket.

S3 Object Lock è un'impostazione permanente che può essere attivata solo quando si crea un bucket. Non puoi aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket.

Per attivare il blocco oggetti S3 per un bucket, utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando il tenant Manager. Vedere "Creare un bucket S3".
- Creare il bucket utilizzando una richiesta CreateBucket con `x-amz-bucket-object-lock-enabled` intestazione della richiesta. Vedere "Operazioni sui bucket".

S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando viene creato il bucket. Non puoi sospendere il controllo delle versioni per il bucket. Vedere "Versione degli oggetti".

Impostazioni di conservazione predefinite per un bucket

Quando S3 Object Lock è attivato per un bucket, è possibile attivare la conservazione predefinita per il bucket e specificare una modalità di conservazione predefinita e un periodo di conservazione predefinito.

Modalità di conservazione predefinita

- In modalità COMPLIANCE:
  - L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
  - La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.

- In modalità GOVERNANCE:
  - Utenti con `s3:BypassGovernanceRetention` l'autorizzazione può utilizzare `x-amz-bypass-governance-retention: true` richiedi intestazione per ignorare le impostazioni di conservazione.
  - Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
  - Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

Periodo di conservazione predefinito

Ogni bucket può avere un periodo di conservazione predefinito specificato in anni o giorni.

Come impostare la conservazione predefinita per un bucket

Per impostare la conservazione predefinita per un bucket, utilizzare uno dei seguenti metodi:

- Gestire le impostazioni del bucket da Tenant Manager. Vedere "Creare un bucket S3" e. "Aggiornare la conservazione predefinita del blocco degli oggetti S3".
- Eseguire una richiesta PutObjectLockConfiguration per il bucket per specificare la modalità predefinita e il numero predefinito di giorni o anni.

PutObjectLockConfiguration

La richiesta PutObjectLockConfiguration consente di impostare e modificare la modalità di conservazione predefinita e il periodo di conservazione predefinito per un bucket con blocco oggetti S3 attivato. È inoltre possibile rimuovere le impostazioni di conservazione predefinite precedentemente configurate.

Quando le nuove versioni degli oggetti vengono acquisite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` e. `x-amz-object-lock-retain-until-date` non sono specificati. Il periodo di conservazione predefinito viene utilizzato per calcolare il periodo di conservazione fino alla data se `x-amz-object-lock-retain-until-date` non specificato.

Se il periodo di conservazione predefinito viene modificato dopo l'acquisizione di una versione dell'oggetto, la data di conservazione della versione dell'oggetto rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito.

È necessario disporre di `s3:PutBucketObjectLockConfiguration` autorizzazione, o essere root dell'account, per completare questa operazione.

Il `Content-MD5` L'intestazione della richiesta deve essere specificata nella richiesta PUT.

Esempio di richiesta

Questo esempio attiva il blocco oggetti S3 per un bucket e imposta la modalità di conservazione predefinita su COMPLIANCE e il periodo di conservazione predefinito su 6 anni.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Come determinare la conservazione predefinita per un bucket

Per determinare se S3 Object Lock è attivato per un bucket e per visualizzare la modalità di conservazione e il periodo di conservazione predefiniti, utilizzare uno dei seguenti metodi:

- Visualizza il bucket nel tenant manager. Vedere "Visualizza i bucket S3".
- Eseguire una richiesta GetObjectLockConfiguration.

GetObjectLockConfiguration

La richiesta GetObjectLockConfiguration consente di determinare se S3 Object Lock è attivato per un bucket e, se è attivato, verificare se sono presenti una modalità di conservazione predefinita e un periodo di conservazione configurato per il bucket.

Quando le nuove versioni degli oggetti vengono acquisite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` non specificato. Il periodo di conservazione predefinito viene utilizzato per calcolare il periodo di conservazione fino alla data se `x-amz-object-lock-retain-until-date` non specificato.

È necessario disporre di `s3:GetBucketObjectLockConfiguration` autorizzazione, o essere root dell'account, per completare questa operazione.

Esempio di richiesta

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Esempio di risposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Come specificare le impostazioni di conservazione per un oggetto

Un bucket con S3 Object Lock abilitato può contenere una combinazione di oggetti con e senza le impostazioni di conservazione S3 Object Lock.

Le impostazioni di conservazione a livello di oggetto vengono specificate utilizzando l'API REST S3. Le impostazioni di conservazione per un oggetto sovrascrivono le impostazioni di conservazione predefinite per il bucket.

È possibile specificare le seguenti impostazioni per ciascun oggetto:

- **Modalità di conservazione**: CONFORMITÀ o GOVERNANCE.
- **Conserva-fino-data**: Una data che specifica per quanto tempo la versione dell'oggetto deve essere conservata da StorageGRID.

- In modalità COMPLIANCE, se la data di conservazione è futura, l'oggetto può essere recuperato, ma non può essere modificato o cancellato. È possibile aumentare la data di conservazione fino alla data prevista, ma non è possibile ridurla o rimuoverle.
- In modalità GOVERNANCE, gli utenti con autorizzazioni speciali possono ignorare l'impostazione di conservazione fino alla data odierna. Possono eliminare una versione dell'oggetto prima che sia trascorso il periodo di conservazione. Possono anche aumentare, diminuire o addirittura rimuovere il mantenimento fino ad oggi.

- **Conservazione legale**: L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa.

  L'impostazione di conservazione legale per un oggetto è indipendente dalla modalità di conservazione e dalla conservazione fino alla data. Se una versione dell'oggetto è sottoposta a blocco legale, nessuno può eliminare tale versione.

Per specificare le impostazioni di blocco oggetti S3 quando si aggiunge una versione di oggetto a un bucket, eseguire un "PutObject", "Oggetto CopyObject", o. "CreateMultipartUpload" richiesta.

È possibile utilizzare quanto segue:

- `x-amz-object-lock-mode`, Che può essere COMPLIANCE o GOVERNANCE (sensibile al maiuscolo/minuscolo).

  > Se si specifica `x-amz-object-lock-mode`, è inoltre necessario specificare `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - Il valore di conservazione fino alla data deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
  - La data di conservazione deve essere in futuro.
- `x-amz-object-lock-legal-hold`

  Se la conservazione legale È ATTIVA (sensibile al maiuscolo/minuscolo), l'oggetto viene collocato sotto una conservazione legale. Se l'opzione Legal Hold è disattivata, non viene effettuata alcuna conservazione a fini giudiziari. Qualsiasi altro valore genera un errore 400 Bad Request (InvalidArgument).

Se si utilizza una di queste intestazioni di richiesta, tenere presente le seguenti restrizioni:

- Il `Content-MD5` l'intestazione della richiesta è obbligatoria, se presente `x-amz-object-lock-*` L'intestazione della richiesta è presente nella richiesta PutObject. `Content-MD5` Non è richiesto per CopyObject o CreateMultipartUpload.
- Se il bucket non ha S3 Object Lock abilitato e un `x-amz-object-lock-*` L'intestazione della richiesta è presente, viene restituito un errore 400 Bad Request (InvalidRequest).
- La richiesta PutObject supporta l'uso di `x-amz-storage-class: REDUCED_REDUNDANCY` Per far corrispondere il comportamento di AWS. Tuttavia, quando un oggetto viene acquisito in un bucket con il blocco oggetti S3 attivato, StorageGRID eseguirà sempre un ingest a doppio commit.

- Una successiva risposta alla versione GET o HeadObject includerà le intestazioni `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e. `x-amz-object-lock-legal-hold`, se configurato e se il mittente della richiesta ha il corretto `s3:Get*` permessi.

È possibile utilizzare `s3:object-lock-remaining-retention-days` chiave di condizione dei criteri per limitare i periodi di conservazione minimi e massimi consentiti per gli oggetti.

Come aggiornare le impostazioni di conservazione per un oggetto

Se è necessario aggiornare le impostazioni di conservazione o conservazione a fini giudiziari per una versione di oggetto esistente, è possibile eseguire le seguenti operazioni di sottorisorsa oggetto:

- `PutObjectLegalHold`

  Se IL nuovo valore di conservazione a fini giudiziari è ATTIVO, l'oggetto viene collocato sotto una conservazione a fini giudiziari. Se il valore di conservazione a fini giudiziari è OFF, la conservazione a fini giudiziari viene revocata.

- `PutObjectRetention`
  - Il valore della modalità può essere COMPLIANCE o GOVERNANCE (distinzione tra maiuscole e minuscole).
  - Il valore di conservazione fino alla data deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
  - Se una versione a oggetti ha un valore di conservazione esistente fino alla data odierna, è possibile aumentarlo. Il nuovo valore deve essere in futuro.

Come utilizzare LA modalità DI GOVERNANCE

Utenti che dispongono di `s3:BypassGovernanceRetention` L'autorizzazione può ignorare le impostazioni di conservazione attive di un oggetto che utilizza la modalità DI GOVERNANCE. Tutte le operazioni di ELIMINAZIONE o PutObjectRetention devono includere `x-amz-bypass-governance-retention:true` intestazione della richiesta. Questi utenti possono eseguire queste operazioni aggiuntive:

- Eseguire operazioni DeleteObject o DeleteObjects per eliminare una versione dell'oggetto prima che sia trascorso il periodo di conservazione.

  Non è possibile eliminare gli oggetti che si trovano sotto un blocco legale. La sospensione legale deve essere disattivata.

- Eseguire le operazioni PutObjectRetention che modificano la modalità di una versione dell'oggetto dalla GOVERNANCE alla CONFORMITÀ prima che sia trascorso il periodo di conservazione dell'oggetto.

  Non è mai consentito cambiare la modalità dalla CONFORMITÀ alla GOVERNANCE.

- Eseguire le operazioni PutObjectRetention per aumentare, ridurre o rimuovere il periodo di conservazione di una versione oggetto.

Informazioni correlate

- "Gestire gli oggetti con S3 Object Lock"
- "USA il blocco oggetti S3 per conservare gli oggetti"
- "Amazon Simple Storage Service User Guide (Guida utente di Amazon Simple Storage Service): Utilizzo di

S3 Object Lock"

Creare la configurazione del ciclo di vita S3

È possibile creare una configurazione del ciclo di vita S3 per controllare quando oggetti specifici vengono cancellati dal sistema StorageGRID.

Il semplice esempio di questa sezione illustra come una configurazione del ciclo di vita S3 può controllare quando alcuni oggetti vengono cancellati (scaduti) da specifici bucket S3. L'esempio in questa sezione è a solo scopo illustrativo. Per informazioni dettagliate sulla creazione di configurazioni del ciclo di vita S3, vedere "Guida utente di Amazon Simple Storage Service: Gestione del ciclo di vita degli oggetti". Nota: StorageGRID supporta solo le azioni di scadenza e non le azioni di transizione.

Che cos'è la configurazione del ciclo di vita

Una configurazione del ciclo di vita è un insieme di regole applicate agli oggetti in specifici bucket S3. Ogni regola specifica quali oggetti sono interessati e quando scadranno (in una data specifica o dopo un certo numero di giorni).

StorageGRID supporta fino a 1,000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML:

- Scadenza: Consente di eliminare un oggetto quando viene raggiunta una data specificata o quando viene raggiunto un numero di giorni specificato, a partire dalla data di acquisizione dell'oggetto.
- NoncurrentVersionExpiration (NoncurrentExpiration versione): Consente di eliminare un oggetto quando viene raggiunto un numero di giorni specificato, a partire da quando l'oggetto è diventato non corrente.
- Filtro (prefisso, tag)
- Stato
- ID

Ciascun oggetto segue le impostazioni di conservazione di un ciclo di vita bucket S3 o di un criterio ILM. Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti corrispondenti al filtro del ciclo di vita del bucket. Gli oggetti che non corrispondono al filtro del ciclo di vita del bucket utilizzano le impostazioni di conservazione del criterio ILM. Se un oggetto corrisponde a un filtro del ciclo di vita bucket e non sono specificate esplicitamente azioni di scadenza, le impostazioni di conservazione del criterio ILM non vengono utilizzate ed è implicito che le versioni degli oggetti vengano mantenute per sempre. Vedere "Esempi di priorità per il ciclo di vita dei bucket S3 e la politica ILM".

Di conseguenza, un oggetto potrebbe essere rimosso dalla griglia anche se le istruzioni di posizionamento in una regola ILM sono ancora applicabili all'oggetto. Oppure, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni di posizionamento ILM per l'oggetto. Per ulteriori informazioni, vedere "Come ILM opera per tutta la vita di un oggetto".

> La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.

StorageGRID supporta l'utilizzo delle seguenti operazioni bucket per gestire le configurazioni del ciclo di vita:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration

- PutBucketLifecycleConfiguration

Creare la configurazione del ciclo di vita

Come primo passo nella creazione di una configurazione del ciclo di vita, è possibile creare un file JSON che includa una o più regole. Ad esempio, questo file JSON include tre regole, come segue:

1. La regola 1 si applica solo agli oggetti che corrispondono al prefisso `category1/` e che hanno un `key2` valore di `tag2`. Il `Expiration` Il parametro specifica che gli oggetti corrispondenti al filtro scadranno alla mezzanotte del 22 agosto 2020.
2. La regola 2 si applica solo agli oggetti che corrispondono al prefisso `category2/`. Il `Expiration` parametro specifica che gli oggetti corrispondenti al filtro scadranno 100 giorni dopo l'acquisizione.

   > Le regole che specificano un numero di giorni sono relative al momento in cui l'oggetto è stato acquisito. Se la data corrente supera la data di acquisizione più il numero di giorni, alcuni oggetti potrebbero essere rimossi dal bucket non appena viene applicata la configurazione del ciclo di vita.

3. La regola 3 si applica solo agli oggetti che corrispondono al prefisso `category3/`. Il `Expiration` parametro specifica che qualsiasi versione non corrente degli oggetti corrispondenti scadrà 50 giorni dopo che diventeranno non aggiornati.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Applica la configurazione del ciclo di vita al bucket

Dopo aver creato il file di configurazione del ciclo di vita, applicarlo a un bucket inviando una richiesta PutBucketLifecycleConfiguration.

Questa richiesta applica la configurazione del ciclo di vita nel file di esempio agli oggetti in un bucket denominato `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Per verificare che una configurazione del ciclo di vita sia stata applicata correttamente al bucket, eseguire una richiesta GetBucketLifecycleConfiguration. Ad esempio:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Una risposta corretta elenca la configurazione del ciclo di vita appena applicata.

Verificare che la scadenza del ciclo di vita del bucket si applichi all'oggetto

È possibile determinare se una regola di scadenza nella configurazione del ciclo di vita si applica a un oggetto specifico quando si invia una richiesta PutObject, HeadObject o GetObject. Se si applica una regola, la risposta include un `Expiration` parametro che indica quando l'oggetto scade e quale regola di scadenza è stata associata.

> Poiché il ciclo di vita del bucket ha la priorità su ILM, il sistema `expiry-date` viene visualizzata la data effettiva in cui l'oggetto verrà eliminato. Per ulteriori informazioni, vedere "Come viene determinata la conservazione degli oggetti".

Ad esempio, questa richiesta PutObject è stata emessa il 22 giugno 2020 e inserisce un oggetto in `testbucket` bucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La risposta corretta indica che l'oggetto scadrà tra 100 giorni (01 ottobre 2020) e che corrisponde alla regola 2 della configurazione del ciclo di vita.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Ad esempio, questa richiesta HeadObject è stata utilizzata per ottenere metadati per lo stesso oggetto nel bucket testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La risposta di successo include i metadati dell'oggetto e indica che l'oggetto scadrà tra 100 giorni e che corrisponde alla regola 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Per i bucket abilitati per la versione, la `x-amz-expiration` l'intestazione della risposta si applica solo alle versioni correnti di oggetti.

Raccomandazioni per l'implementazione dell'API REST S3

Seguire questi consigli quando si implementa l'API REST S3 per l'utilizzo con StorageGRID.

Raccomandazioni per la gestione di oggetti inesistenti

Se l'applicazione verifica regolarmente se un oggetto esiste in un percorso in cui non si prevede che l'oggetto esista effettivamente, è necessario utilizzare la casella di controllo "disponibile" "coerenza". Ad esempio, è necessario utilizzare la coerenza "disponibile" se l'applicazione rileva una posizione prima di INVIARLA.

In caso contrario, se l'operazione HEAD non trova l'oggetto, è possibile ricevere un numero elevato di errori del server interno 500 se due o più nodi di archiviazione nello stesso sito non sono disponibili o un sito remoto non è raggiungibile.

È possibile impostare la consistenza "disponibile" per ciascun bucket utilizzando "METTI la coerenza del bucket" Oppure è possibile specificare la coerenza nell'intestazione della richiesta per una singola operazione

API.

Raccomandazioni per le chiavi a oggetti

Seguire questi consigli per i nomi delle chiavi degli oggetti, in base alla prima volta che il bucket è stato creato.

Bucket creati in StorageGRID 11.4 o versioni precedenti

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi oggetto. Ciò è in contrasto con la precedente raccomandazione AWS per i prefissi principali. Utilizzare invece prefissi non casuali e non univoci, ad esempio `image`.
- Se si segue la precedente raccomandazione AWS per utilizzare caratteri casuali e univoci nei prefissi delle chiavi, inserire un prefisso tra le chiavi degli oggetti e il nome della directory. Ovvero, utilizzare questo formato:

  `mybucket/mydir/f8e3-image3132.jpg`

  Invece di questo formato:

  `mybucket/f8e3-image3132.jpg`

Bucket creati in StorageGRID 11.4 o versioni successive

Non è necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. Nella maggior parte dei casi, è possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi degli oggetti.

> Un'eccezione è rappresentata da un carico di lavoro S3 che rimuove continuamente tutti gli oggetti dopo un breve periodo di tempo. Per ridurre al minimo l'impatto delle performance per questo caso d'utilizzo, modificare una parte iniziale del nome della chiave ogni diverse migliaia di oggetti con qualcosa di simile alla data. Si supponga, ad esempio, che un client S3 scriva in genere 2,000 oggetti al secondo e che il criterio del ciclo di vita di ILM o bucket rimuova tutti gli oggetti dopo tre giorni. Per ridurre al minimo l'impatto delle performance, è possibile assegnare un nome alle chiavi utilizzando un modello come questo:
> `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Raccomandazioni per "letture di gamma"

Se il "opzione globale per comprimere gli oggetti memorizzati" È attivato, le applicazioni client S3 devono evitare di eseguire operazioni GetObject che specificano la restituzione di un intervallo di byte. Queste operazioni di "lettura dell'intervallo" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. Le operazioni GetObject che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è inefficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

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

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

Supporto per Amazon S3 REST API

Dettagli sull'implementazione dell'API REST S3

Il sistema StorageGRID implementa l'API del servizio di storage semplice (API versione 2006-03-01) con il supporto per la maggior parte delle operazioni e con alcune limitazioni. È necessario comprendere i dettagli dell'implementazione quando si integrano le applicazioni client API REST S3.

Il sistema StorageGRID supporta sia richieste virtuali in stile host che richieste in stile percorso.

Gestione della data

L'implementazione StorageGRID dell'API REST S3 supporta solo formati di data HTTP validi.

Il sistema StorageGRID supporta solo i formati di data HTTP validi per tutte le intestazioni che accettano i valori di data. La parte temporale della data può essere specificata nel formato GMT (Greenwich Mean Time) o UTC (Universal Coordinated Time) senza offset del fuso orario (deve essere specificato ++1). Se si include `x-amz-date` Intestazione nella richiesta, sovrascrive qualsiasi valore specificato nell'intestazione della richiesta Data. Quando si utilizza la firma AWS versione 4, il `x-amz-date` l'intestazione deve essere presente nella richiesta firmata perché l'intestazione della data non è supportata.

Intestazioni di richiesta comuni

Il sistema StorageGRID supporta le intestazioni di richiesta comuni definite da "Amazon Simple Storage Service API Reference: Intestazioni di richiesta comuni", con un'eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	Supporto completo per firma AWS versione 2 Supporto per firma AWS versione 4, con le seguenti eccezioni: • Il valore SHA256 non viene calcolato per il corpo della richiesta. Il valore inviato dall'utente viene accettato senza convalida, come se il valore `UNSIGNED-PAYLOAD` è stato fornito per `x-amz-content-sha256` intestazione.
x-amz-security-token	Non implementato. Ritorno `XNotImplemented`.

Intestazioni di risposta comuni

Il sistema StorageGRID supporta tutte le intestazioni di risposta comuni definite dal *riferimento API del servizio di storage semplice*, con un'eccezione.

Intestazione della risposta	Implementazione
x-amz-id-2	Non utilizzato

Autenticare le richieste

Il sistema StorageGRID supporta l'accesso anonimo e autenticato agli oggetti utilizzando l'API S3.

L'API S3 supporta Signature versione 2 e Signature versione 4 per l'autenticazione delle richieste API S3.

Le richieste autenticate devono essere firmate utilizzando l'ID della chiave di accesso e la chiave di accesso segreta.

Il sistema StorageGRID supporta due metodi di autenticazione: HTTP `Authorization` intestazione e utilizzo dei parametri di query.

Utilizzare l'intestazione autorizzazione HTTP

Il protocollo HTTP `Authorization` Header viene utilizzato da tutte le operazioni API S3, ad eccezione delle richieste anonime, laddove consentito dalla policy bucket. Il `Authorization` header contiene tutte le informazioni di firma richieste per autenticare una richiesta.

Utilizzare i parametri di query

È possibile utilizzare i parametri di query per aggiungere informazioni di autenticazione a un URL. Questa operazione è nota come prefirma dell'URL, che può essere utilizzata per concedere l'accesso temporaneo a risorse specifiche. Gli utenti con l'URL con prefisso non devono conoscere la chiave di accesso segreta per accedere alla risorsa, consentendo così l'accesso limitato a una risorsa da parte di terze parti.

Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

Operazione	Implementazione
ListBucket (Precedentemente denominato GET Service)	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
OTTIENI l'utilizzo dello storage	Il StorageGRID "OTTIENI l'utilizzo dello storage" la richiesta indica la quantità totale di storage utilizzata da un account e per ogni bucket associato all'account. Si tratta di un'operazione sul servizio con un percorso di / e un parametro di query personalizzato (`?x-ntap-sg-usage`) aggiunto.
OPZIONI /	Le applicazioni client possono avere problemi `OPTIONS /` Richiede alla porta S3 su un nodo di storage, senza fornire credenziali di autenticazione S3, di determinare se il nodo di storage è disponibile. È possibile utilizzare questa richiesta per il monitoraggio o per consentire ai bilanciatori di carico esterni di identificare quando un nodo di storage è inattivo.

Operazioni sui bucket

Il sistema StorageGRID supporta un massimo di 1,000 bucket per ciascun account tenant S3.

Le restrizioni dei nomi dei bucket seguono le restrizioni delle regioni AWS US Standard, ma è necessario limitarle ulteriormente alle convenzioni di denominazione DNS per supportare le richieste di tipo host virtuale

S3.

Per ulteriori informazioni, vedere quanto segue:

- "Guida dell'utente di Amazon Simple Storage Service: Restrizioni e limitazioni dei bucket"
- "Configurare i nomi di dominio degli endpoint S3"

Le operazioni ListObjects (GET Bucket) e ListObjectVersions (GET Bucket Object Versions) supportano StorageGRID "valori di coerenza".

È possibile verificare se gli aggiornamenti dell'ultimo tempo di accesso sono attivati o disattivati per i singoli bucket. Vedere
"OTTIENI l'ultimo tempo di accesso a bucket".

La seguente tabella descrive come StorageGRID implementa le operazioni del bucket API REST S3. Per eseguire una di queste operazioni, è necessario fornire le credenziali di accesso necessarie per l'account.

Operazione	Implementazione
CreateBucket	Crea un nuovo bucket. Creando il bucket, diventerai il proprietario del bucket. • I nomi dei bucket devono rispettare le seguenti regole: ◦ Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). ◦ Deve essere conforme al DNS. ◦ Deve contenere almeno 3 e non più di 63 caratteri. ◦ Può essere una serie di una o più etichette, con etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. ◦ Non deve essere simile a un indirizzo IP formattato con testo. ◦ Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. • Per impostazione predefinita, i bucket vengono creati in `us-east-1` regione; tuttavia, è possibile utilizzare `LocationConstraint` elemento di richiesta nel corpo della richiesta per specificare un'area diversa. Quando si utilizza `LocationConstraint` È necessario specificare il nome esatto di una regione definita utilizzando Grid Manager o l'API Grid Management. Contattare l'amministratore di sistema se non si conosce il nome della regione da utilizzare. **Nota**: Si verifica un errore se la richiesta CreateBucket utilizza una regione non definita in StorageGRID. • È possibile includere `x-amz-bucket-object-lock-enabled` Richiedi intestazione per creare un bucket con blocco oggetti S3 attivato. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3". È necessario attivare il blocco oggetti S3 quando si crea il bucket. Non puoi aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket. S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando si crea il bucket.
DeleteBucket	Elimina il bucket.
DeleteBucketCors	Elimina la configurazione CORS per il bucket.
DeleteBucketEncryption	Elimina la crittografia predefinita dal bucket. Gli oggetti crittografati esistenti rimangono crittografati, ma i nuovi oggetti aggiunti al bucket non vengono crittografati.
DeleteBucketLifecycle	Elimina la configurazione del ciclo di vita dal bucket. Vedere "Creare la configurazione del ciclo di vita S3".

Operazione	Implementazione
DeleteBucketPolicy	Elimina il criterio allegato al bucket.
DeleteBucketReplication	Elimina la configurazione di replica collegata al bucket.
DeleteBucketTagging	Utilizza `tagging` sottorisorsa per rimuovere tutti i tag da un bucket. **Attenzione**: Se per questo bucket è impostato un tag di criterio ILM non predefinito, verrà visualizzato un `NTAP-SG-ILM-BUCKET-TAG` tag bucket a cui è stato assegnato un valore. Non inviare una richiesta DeleteBucketTagging se è presente un `NTAP-SG-ILM-BUCKET-TAG` etichetta benna. Al contrario, eseguire una richiesta PutBucketTagging solo con `NTAP-SG-ILM-BUCKET-TAG` tag e il relativo valore assegnato per rimuovere tutti gli altri tag dal bucket. Non modificare o rimuovere `NTAP-SG-ILM-BUCKET-TAG` etichetta benna.
GetBucketAcl	Restituisce una risposta positiva e l'ID, il DisplayName e l'autorizzazione del proprietario del bucket, indicando che il proprietario ha accesso completo al bucket.
GetBucketCors	Restituisce il `cors` configurazione per il bucket.
GetBucketEncryption	Restituisce la configurazione di crittografia predefinita per il bucket.
GetBucketLifecycleConfiguration (Precedentemente denominato ciclo di vita GET Bucket)	Restituisce la configurazione del ciclo di vita per il bucket. Vedere "Creare la configurazione del ciclo di vita S3".
GetBucketLocation	Restituisce la regione impostata mediante `LocationConstraint` Elemento nella richiesta CreateBucket. Se l'area del bucket è `us-east-1`, viene restituita una stringa vuota per la regione.
GetBucketNotificationConfiguration (In precedenza denominato notifica GET Bucket)	Restituisce la configurazione di notifica collegata al bucket.
GetBucketPolicy	Restituisce la policy allegata al bucket.
GetBucketReplication	Restituisce la configurazione di replica collegata al bucket.

Operazione	Implementazione
GetBucketTagging	Utilizza `tagging` sottorisorsa per restituire tutti i tag per un bucket. **Attenzione**: Se per questo bucket è impostato un tag di criterio ILM non predefinito, verrà visualizzato un `NTAP-SG-ILM-BUCKET-TAG` tag bucket a cui è stato assegnato un valore. Non modificare o rimuovere questo tag.
GetBucketVersioning	Questa implementazione utilizza `versioning` sottorisorsa per restituire lo stato di versione di un bucket. • *Blank*: La versione non è mai stata abilitata (bucket "Unversioned") • Enabled (attivato): Il controllo delle versioni è attivato • Suspended (sospeso): Il controllo delle versioni era stato precedentemente attivato e sospeso
GetObjectLockConfiguration	Restituisce la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito, se configurato. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".
HeadBucket	Determina se esiste un bucket e si dispone dell'autorizzazione per accedervi. Questa operazione restituisce: • `x-ntap-sg-bucket-id`: UUID del bucket in formato UUID. • `x-ntap-sg-trace-id`: L'ID di traccia univoco della richiesta associata.
ListObjects e ListObjectsV2 (Precedentemente denominato GET Bucket)	Restituisce alcuni o tutti gli oggetti (fino a 1.000) in un bucket. La classe Storage per gli oggetti può avere due valori, anche se l'oggetto è stato acquisito con `REDUCED_REDUNDANCY` opzione classe di storage: • `STANDARD`, Che indica che l'oggetto è memorizzato in un pool di storage costituito da nodi di storage. • `GLACIER`, Che indica che l'oggetto è stato spostato nel bucket esterno specificato dal Cloud Storage Pool. Se il bucket contiene un numero elevato di chiavi eliminate con lo stesso prefisso, la risposta potrebbe includere alcune `CommonPrefixes` che non contengono chiavi.
ListObjectVersions (Precedentemente denominate versioni oggetto GET Bucket)	Con accesso di LETTURA su una benna, utilizzando questa operazione con `versions` la sottorisorsa elenca i metadati di tutte le versioni degli oggetti nel bucket.

Operazione	Implementazione
PutBucketCors	Imposta la configurazione CORS per un bucket in modo che il bucket possa gestire le richieste cross-origin. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni Web client di un dominio di accedere alle risorse di un dominio diverso. Si supponga, ad esempio, di utilizzare un bucket S3 denominato `images` per memorizzare le immagini. Impostando la configurazione CORS per `images` bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito web `http://www.example.com`.
PutBucketEncryption	Consente di impostare lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è attivata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati.StorageGRID supporta la crittografia lato server con le chiavi gestite da StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare `SSEAlgorithm` parametro a. `AES256`e non utilizzare `KMSMasterKeyID` parametro. La configurazione della crittografia predefinita del bucket viene ignorata se la richiesta di caricamento degli oggetti specifica già la crittografia, ovvero se la richiesta include `x-amz-server-side-encryption-*` intestazione della richiesta).
PutBucketLifecycleConfiguration (Precedentemente denominato ciclo di vita bucket PUT)	Crea una nuova configurazione del ciclo di vita per il bucket o sostituisce una configurazione del ciclo di vita esistente. StorageGRID supporta fino a 1,000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML: • Scadenza (giorni, data, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtro (prefisso, tag) • Stato • ID StorageGRID non supporta queste azioni: • AbortIncompleteMultipartUpload • Transizione Vedere "Creare la configurazione del ciclo di vita S3". Per comprendere come l'azione di scadenza in un ciclo di vita del bucket interagisce con le istruzioni di posizionamento ILM, vedere "Come ILM opera per tutta la vita di un oggetto". **Nota**: La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.

Operazione	Implementazione

PutBucketNotificationConfiguration
 	
(Precedentemente denominata notifica bucket PUT)
	Configura le notifiche per il bucket utilizzando l'XML di configurazione delle notifiche incluso nel corpo della richiesta. È necessario conoscere i seguenti dettagli di implementazione:
	
	• StorageGRID supporta gli argomenti di Amazon Simple Notification Service (Amazon SNS) o Kafka come destinazioni. Gli endpoint SQS (Simple Queue Service) o Amazon Lambda non sono supportati.
	• La destinazione delle notifiche deve essere specificata come URN di un endpoint StorageGRID. Gli endpoint possono essere creati utilizzando il tenant Manager o l'API di gestione tenant.
	
	L'endpoint deve esistere perché la configurazione della notifica abbia esito positivo. Se l'endpoint non esiste, un `400 Bad Request` viene restituito un errore con il codice `InvalidArgument`.
	
	• Non è possibile configurare una notifica per i seguenti tipi di evento. Questi tipi di evento sono **non** supportati.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ad eccezione del fatto che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente:
	◦ **EventSource**
	
	`sgws:s3`
	
	◦ **AwsRegion**
	
	non incluso
	
	◦ **x-amz-id-2**
	
	non incluso
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	Imposta il criterio associato al bucket. Vedere "Utilizza policy di accesso a bucket e gruppi".

Operazione	Implementazione
PutBucketReplication	Configura "Replica di StorageGRID CloudMirror" Per il bucket che utilizza l'XML di configurazione della replica fornito nel corpo della richiesta. Per la replica di CloudMirror, è necessario conoscere i seguenti dettagli di implementazione: • StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo di `Filter` Per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per ulteriori informazioni, vedere "Guida utente di Amazon Simple Storage Service: Configurazione della replica". • La replica del bucket può essere configurata su bucket con versione o senza versione. • È possibile specificare un bucket di destinazione diverso in ciascuna regola dell'XML di configurazione della replica. Un bucket di origine può replicare in più di un bucket di destinazione. • I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID, come specificato in Gestione tenant o nell'API di gestione tenant. Vedere "Configurare la replica di CloudMirror". L'endpoint deve esistere per il successo della configurazione della replica. Se l'endpoint non esiste, la richiesta fallisce come a. `400 Bad Request`. Il messaggio di errore indica: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Non è necessario specificare un `Role` Nel file XML di configurazione. Questo valore non viene utilizzato da StorageGRID e verrà ignorato se inviato. • Se si omette la classe di storage dall'XML di configurazione, StorageGRID utilizza `STANDARD` classe di storage per impostazione predefinita. • Se si elimina un oggetto dal bucket di origine o si elimina lo stesso bucket di origine, il comportamento della replica tra regioni è il seguente: ◦ Se si elimina l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non viene replicato e non viene inviata alcuna notifica. ◦ Se elimini l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento standard di eliminazione di Amazon S3 per V1 della replica tra regioni.

Operazione	Implementazione
PutBucketTagging	Utilizza `tagging` sottorisorsa per aggiungere o aggiornare un set di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni: • StorageGRID e Amazon S3 supportano fino a 50 tag per ciascun bucket. • Le etichette associate a un bucket devono avere chiavi tag univoche. Una chiave tag può contenere fino a 128 caratteri Unicode. • I valori dei tag possono contenere fino a 256 caratteri Unicode. • Chiave e valori distinguono tra maiuscole e minuscole. **Attenzione**: Se per questo bucket è impostato un tag di criterio ILM non predefinito, verrà visualizzato un `NTAP-SG-ILM-BUCKET-TAG` tag bucket a cui è stato assegnato un valore. Assicurarsi che il `NTAP-SG-ILM-BUCKET-TAG` Il tag bucket è incluso con il valore assegnato in tutte le richieste PutBucketTagging. Non modificare o rimuovere questo tag. **Nota**: Questa operazione sovrascriverà tutti i tag correnti già presenti nel bucket. Se qualsiasi tag esistente viene omesso dal set, tali tag verranno rimossi per il bucket.
PutBucketVersioning	Utilizza `versioning` sottorisorsa per impostare lo stato di versione di un bucket esistente. È possibile impostare lo stato di versione con uno dei seguenti valori: • Enabled (attivato): Attiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID di versione univoco. • Suspended (sospeso): Disattiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID versione `null`.
PutObjectLockConfiguration	Configura o rimuove la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito. Se il periodo di conservazione predefinito viene modificato, la data di conservazione delle versioni degli oggetti esistenti rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3" per informazioni dettagliate.

Operazioni sugli oggetti

Operazioni sugli oggetti

Questa sezione descrive come il sistema StorageGRID implementa le operazioni API REST S3 per gli oggetti.

Le seguenti condizioni si applicano a tutte le operazioni a oggetti:

- StorageGRID "valori di coerenza" sono supportate da tutte le operazioni sugli oggetti, ad eccezione di quanto segue:

    - GetObjectAcl
    - `OPTIONS /`
    - PutObjectLegalHold
    - PutObjectRetention
    - SelectObjectContent
- Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.
- Tutti gli oggetti in un bucket StorageGRID sono di proprietà del proprietario del bucket, inclusi gli oggetti creati da un utente anonimo o da un altro account.
- Impossibile accedere agli oggetti dati acquisiti nel sistema StorageGRID tramite Swift tramite S3.

Nella tabella seguente viene descritto il modo in cui StorageGRID implementa le operazioni degli oggetti API REST S3.

Operazione	Implementazione
DeleteObject (Elimina oggetto)	Autenticazione multifattore (MFA) e intestazione della risposta `x-amz-mfa` non sono supportati. Durante l'elaborazione di una richiesta DeleteObject, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni memorizzate. Se l'esito è positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio, perché una posizione è temporaneamente non disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito. **Versione** Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare `versionId` sottorisorsa. L'utilizzo di questa sottorisorsa elimina in modo permanente la versione. Se il `versionId` corrisponde a un indicatore di eliminazione, l'intestazione della risposta `x-amz-delete-marker` viene restituito impostato su `true`. • Se un oggetto viene eliminato senza `versionId` sottorisorsa su un bucket abilitato alla versione, si ottiene la generazione di un indicatore di eliminazione. Il `versionId` per il contrassegno di eliminazione viene restituito utilizzando `x-amz-version-id` intestazione della risposta e la `x-amz-delete-marker` l'intestazione della risposta viene restituita impostata su `true`. • Se un oggetto viene eliminato senza `versionId` sottorisorsa su un bucket sospeso della versione, si ottiene una cancellazione permanente di una versione 'null' già esistente o di un marker di eliminazione 'null' e la generazione di un nuovo marker di eliminazione 'null'. Il `x-amz-delete-marker` l'intestazione della risposta viene restituita impostata su `true`. **Nota**: In alcuni casi, per un oggetto potrebbero esistere più contrassegni di eliminazione. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3" Per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.
DeleteObjects (Precedentemente denominato ELIMINA più oggetti)	Autenticazione multifattore (MFA) e intestazione della risposta `x-amz-mfa` non sono supportati. È possibile eliminare più oggetti nello stesso messaggio di richiesta. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3" Per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.

Operazione	Implementazione
DeleteObjectTagging	Utilizza `tagging` sottorisorsa per rimuovere tutti i tag da un oggetto. **Versione** Se il `versionId` il parametro query non è specificato nella richiesta, l'operazione elimina tutti i tag dalla versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con `x-amz-delete-marker` intestazione risposta impostata su `true`.
GetObject	"GetObject"
GetObjectAcl	Se vengono fornite le credenziali di accesso necessarie per l'account, l'operazione restituisce una risposta positiva e l'ID, il DisplayName e l'autorizzazione del proprietario dell'oggetto, indicando che il proprietario dispone dell'accesso completo all'oggetto.
GetObjectLegalHold	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
GetObjectRetention	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
GetObjectTagging	Utilizza `tagging` sottorisorsa per restituire tutti i tag per un oggetto. **Versione** Se il `versionId` il parametro query non è specificato nella richiesta, l'operazione restituisce tutti i tag della versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con `x-amz-delete-marker` intestazione risposta impostata su `true`.
HeadObject (oggetto intestazione)	"HeadObject (oggetto intestazione)"
RestoreObject	"RestoreObject"
PutObject	"PutObject"
Oggetto CopyObject (Precedentemente denominato oggetto PUT - Copia)	"Oggetto CopyObject"
PutObjectLegalHold	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
PutObjectRetention	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

Operazione	Implementazione
PutObjectTagging	Utilizza `tagging` sottorisorsa per aggiungere un set di tag a un oggetto esistente. **Limiti tag oggetto** È possibile aggiungere tag a nuovi oggetti durante il caricamento oppure aggiungerli a oggetti esistenti. StorageGRID e Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori di tag possono contenere fino a 256 caratteri Unicode. Chiave e valori distinguono tra maiuscole e minuscole. **Aggiornamenti dei tag e comportamento di acquisizione** Quando si utilizza PutObjectTagging per aggiornare i tag di un oggetto, StorageGRID non acquisisce nuovamente l'oggetto. Ciò significa che l'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background. Ciò significa che se la regola ILM utilizza l'opzione Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto. **Risoluzione dei conflitti** Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione. **Versione** Se il `versionId` il parametro query non è specificato nella richiesta, l'operazione aggiunge tag alla versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con `x-amz-delete-marker` intestazione risposta impostata su `true`.
SelectObjectContent	"SelectObjectContent"

USA S3 Select

StorageGRID supporta le seguenti condizioni, tipi di dati e operatori di Amazon S3 Select per "Comando SelectObjectContent".

Gli elementi non elencati non sono supportati.

Per la sintassi, vedere "SelectObjectContent". Per ulteriori informazioni su S3 Select, vedere "Documentazione AWS per S3 Select".

Solo gli account tenant con S3 Select abilitato possono eseguire query SelectObjectContent. Vedere "Considerazioni e requisiti per l'utilizzo di S3 Select".

Clausole

- SELEZIONARE l'elenco
- CLAUSOLA FROM
- Clausola WHERE
- Clausola di LIMITAZIONE

Tipi di dati

- bool
- intero
- stringa
- fluttuare
- decimale, numerico
- data e ora

Operatori

Operatori logici

- E.
- NO
- OPPURE

Operatori di confronto

- <
- >
- ⇐
- >=
- =
- =
- <>
- !=
- TRA
- POLL

Operatori di corrispondenza dei modelli

- MI PIACE
- _
- %

Operatori unitari

- È NULL
- NON È NULL

Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

Funzioni di aggregazione

- MEDIA()
- CONTEGGIO(*)
- MAX()
- MIN()
- SOMMA()

Funzioni condizionali

- CASO
- COALESCE
- NULLIF

Funzioni di conversione

- CAST (per il tipo di dati supportato)

Funzioni di data

- DATA_ADD
- DATA_DIFF
- ESTRARRE
- TO_STRING
- TO_TIMESTAMP

- UTCNOW

Funzioni di stringa

- CHAR_LENGTH, CHARACTER_LENGTH
- ABBASSARE
- SOTTOSTRINGA
- TAGLIARE
- SUPERIORE

Utilizzare la crittografia lato server

La crittografia lato server consente di proteggere i dati a oggetti inattivi. StorageGRID crittografa i dati durante la scrittura dell'oggetto e li decrta quando si accede all'oggetto.

Se si desidera utilizzare la crittografia lato server, è possibile scegliere una delle due opzioni che si escludono a vicenda, in base alla modalità di gestione delle chiavi di crittografia:

- **SSE (crittografia lato server con chiavi gestite da StorageGRID)**: Quando si invia una richiesta S3 per memorizzare un oggetto, StorageGRID crittografa l'oggetto con una chiave univoca. Quando si invia una richiesta S3 per recuperare l'oggetto, StorageGRID utilizza la chiave memorizzata per decrittare l'oggetto.
- **SSE-C (crittografia lato server con chiavi fornite dal cliente)**: Quando si invia una richiesta S3 per memorizzare un oggetto, viene fornita la propria chiave di crittografia. Quando si recupera un oggetto, si fornisce la stessa chiave di crittografia come parte della richiesta. Se le due chiavi di crittografia corrispondono, l'oggetto viene decrittografato e vengono restituiti i dati dell'oggetto.

  Mentre StorageGRID gestisce tutte le operazioni di crittografia e decifratura degli oggetti, è necessario gestire le chiavi di crittografia fornite.

  > Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente.

  > Se un oggetto viene crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Utilizzare SSE

Per crittografare un oggetto con una chiave univoca gestita da StorageGRID, utilizzare la seguente intestazione di richiesta:

```
x-amz-server-side-encryption
```

L'intestazione della richiesta SSE è supportata dalle seguenti operazioni a oggetti:

- "PutObject"
- "Oggetto CopyObject"
- "CreateMultipartUpload"

Utilizzare SSE-C.

Per crittografare un oggetto con una chiave univoca gestita, vengono utilizzate tre intestazioni di richiesta:

Intestazione della richiesta	Descrizione
`x-amz-server-side -encryption-customer -algorithm`	Specificare l'algoritmo di crittografia. Il valore dell'intestazione deve essere `AES256`.
`x-amz-server-side -encryption-customer-key`	Specificare la chiave di crittografia che verrà utilizzata per crittografare o decrittare l'oggetto. Il valore della chiave deve essere 256 bit, con codifica base64.
`x-amz-server-side -encryption-customer-key -MD5`	Specificare il digest MD5 della chiave di crittografia in base a RFC 1321, utilizzato per garantire che la chiave di crittografia sia stata trasmessa senza errori. Il valore del digest MD5 deve essere a 128 bit con codifica base64.

Le intestazioni delle richieste SSE-C sono supportate dalle seguenti operazioni a oggetti:

- "GetObject"
- "HeadObject (oggetto intestazione)"
- "PutObject"
- "Oggetto CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Considerazioni sull'utilizzo della crittografia lato server con le chiavi fornite dal cliente (SSE-C)

Prima di utilizzare SSE-C, tenere presente quanto segue:

- È necessario utilizzare https.

> ⚠ StorageGRID rifiuta qualsiasi richiesta effettuata su http quando si utilizza SSE-C. Per motivi di sicurezza, è consigliabile considerare compromessa qualsiasi chiave inviata accidentalmente utilizzando http. Eliminare la chiave e ruotarla in base alle necessità.

- L'ETag nella risposta non è l'MD5 dei dati dell'oggetto.
- È necessario gestire il mapping delle chiavi di crittografia agli oggetti. StorageGRID non memorizza le chiavi di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia che fornisce per ciascun oggetto.
- Se il bucket è abilitato per la versione, ogni versione dell'oggetto deve disporre di una propria chiave di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia utilizzata per ciascuna versione dell'oggetto.
- Poiché si gestiscono le chiavi di crittografia sul lato client, è necessario gestire anche eventuali protezioni aggiuntive, come la rotazione delle chiavi, sul lato client.

Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente.

- Se la replica cross-grid o CloudMirror è configurata per il bucket, non è possibile acquisire oggetti SSE-C. L'operazione di acquisizione non riesce.

Informazioni correlate

"Manuale dell'utente di Amazon S3: Utilizzo della crittografia lato server con chiavi fornite dal cliente (SSE-C)"

Oggetto CopyObject

È possibile utilizzare la richiesta CopyObject S3 per creare una copia di un oggetto già memorizzato in S3. Un'operazione CopyObject è la stessa dell'esecuzione di GetObject seguito da PutObject.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se sono presenti oggetti di dimensioni superiori a 5 GiB, utilizzare "caricamento multiparte" invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).

Se è stato eseguito l'aggiornamento da StorageGRID 11,6 o versioni precedenti, l'avviso S3 PUT object size too large verrà attivato se si tenta di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11,7 o 11,8, l'avviso non verrà attivato in questo caso. Tuttavia, per allinearsi allo standard AWS S3, le versioni future di StorageGRID non supporteranno il caricamento di oggetti di dimensioni superiori a 5 GiB.

UTF-8 caratteri nei metadati dell'utente

Se una richiesta include valori UTF-8 (non escapati) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento di StorageGRID non è definito.

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 escapiti vengono trattati come caratteri ASCII:

- Le richieste hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 escapiti.
- StorageGRID non restituisce `x-amz-missing-meta` header se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Content-Type`

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente
- `x-amz-metadata-directive`: Il valore predefinito è `COPY`, che consente di copiare l'oggetto e i metadati associati.

  È possibile specificare `REPLACE` per sovrascrivere i metadati esistenti durante la copia dell'oggetto o per aggiornare i metadati dell'oggetto.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: Il valore predefinito è `COPY`, che consente di copiare l'oggetto e tutti i tag.

  È possibile specificare `REPLACE` per sovrascrivere i tag esistenti durante la copia dell'oggetto o per aggiornare i tag.

- Intestazioni della richiesta di blocco oggetti S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la modalità di versione dell'oggetto e mantenere la data fino alla data. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

- Intestazioni di richiesta SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Vedere Intestazioni di richiesta per la crittografia lato server

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `Cache-Control`

- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

Opzioni di classe storage

Il `x-amz-storage-class` L'intestazione della richiesta è supportata e influisce sul numero di copie degli oggetti create da StorageGRID se la regola ILM corrispondente utilizza il doppio commit o bilanciato "opzione di acquisizione".

- `STANDARD`

  (Impostazione predefinita) specifica un'operazione di ingest dual-commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced (bilanciamento) torna alla creazione di copie interinali.

- `REDUCED_REDUNDANCY`

  Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione di commit doppio o quando l'opzione di bilanciamento ritorna alla creazione di copie interinali.

  > Se si sta inserendo un oggetto in un bucket con il blocco oggetti S3 attivato, il `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Utilizzo di x-amz-copy-source in CopyObject

Se il bucket e la chiave di origine, specificati in `x-amz-copy-source` header, sono diversi dal bucket e dalla chiave di destinazione, una copia dei dati dell'oggetto di origine viene scritta nella destinazione.

Se l'origine e la destinazione corrispondono, e il `x-amz-metadata-directive` l'intestazione è specificata come `REPLACE`, i metadati dell'oggetto vengono aggiornati con i valori dei metadati forniti nella richiesta. In questo caso, StorageGRID non reinserisce l'oggetto. Questo ha due conseguenze importanti:

- Non è possibile utilizzare CopyObject per crittografare un oggetto esistente sul posto o per modificare la crittografia di un oggetto esistente sul posto. Se si fornisce `x-amz-server-side-encryption` o il `x-amz-server-side-encryption-customer-algorithm` Intestazione, StorageGRID rifiuta la richiesta e restituisce `XNotImplemented`.
- L'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background.

  Ciò significa che se la regola ILM utilizza l'opzione Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto.

Intestazioni di richiesta per la crittografia lato server

Se "usa crittografia lato server", le intestazioni di richiesta fornite dipendono dal fatto che l'oggetto di origine sia crittografato o meno e dal fatto che si intenda crittografare l'oggetto di destinazione.

- Se l'oggetto di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta CopyObject, in modo che l'oggetto possa essere decrittografato e quindi copiato:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key`: Specificare la chiave di crittografia fornita al momento della creazione dell'oggetto di origine.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 fornito al momento della creazione dell'oggetto di origine.
- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca che si fornisce e si gestisce, includere le seguenti tre intestazioni:
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Specificare una nuova chiave di crittografia per l'oggetto di destinazione.
  - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della nuova chiave di crittografia.

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni per "utilizzo della crittografia lato server".

- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca gestita da StorageGRID (SSE), includere questa intestazione nella richiesta CopyObject:
  - `x-amz-server-side-encryption`

> Il `server-side-encryption` impossibile aggiornare il valore dell'oggetto. Invece, fare una copia con un nuovo `server-side-encryption` valore utilizzando `x-amz-metadata-directive`: `REPLACE`.

Versione

Se il bucket di origine è configurato con la versione, è possibile utilizzare `x-amz-copy-source` intestazione per copiare l'ultima versione di un oggetto. Per copiare una versione specifica di un oggetto, è necessario specificare esplicitamente la versione da copiare utilizzando `versionId` sottorisorsa. Se il bucket di destinazione è configurato con la versione, la versione generata viene restituita in `x-amz-version-id` intestazione della risposta. Se il controllo delle versioni viene sospeso per il bucket di destinazione, allora `x-amz-version-id` restituisce un valore "nullo".

GetObject

È possibile utilizzare la richiesta GetObject S3 per recuperare un oggetto da un bucket S3.

Oggetti GetObject e multiparte

È possibile utilizzare `partNumber` parametro di richiesta per recuperare una parte specifica di un oggetto multiparte o segmentato. Il `x-amz-mp-parts-count` l'elemento response indica il numero di parti dell'oggetto.

È possibile impostare `partNumber` a 1 per oggetti segmentati/multiparte e oggetti non segmentati/non multiparte; tuttavia, `x-amz-mp-parts-count` l'elemento di risposta viene restituito solo per gli oggetti segmentati o multiparte.

UTF-8 caratteri nei metadati dell'utente

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati nei metadati definiti dall'utente. LE richieste GET per un oggetto con caratteri UTF-8 escapiti nei metadati definiti dall'utente non restituiscono `x-amz-missing-meta` intestazione se il nome o il valore della chiave include caratteri non stampabili.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`:

- `x-amz-website-redirect-location`

Versione

Se si seleziona `versionId` la sottorisorsa non viene specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "non trovato" con `x-amz-delete-marker` intestazione risposta impostata su `true`.

Intestazioni delle richieste per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)

Utilizzare tutte e tre le intestazioni se l'oggetto è crittografato con una chiave univoca fornita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.
- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia dell'oggetto.

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni in "Utilizzare la crittografia lato server".

Comportamento degli oggetti GetObject per Cloud Storage Pool

Se un oggetto è stato memorizzato in "Pool di cloud storage", Il comportamento di una richiesta GetObject dipende dallo stato dell'oggetto. Vedere "HeadObject (oggetto intestazione)" per ulteriori dettagli.

> Se un oggetto viene memorizzato in un Cloud Storage Pool e sulla griglia esistono anche una o più copie dell'oggetto, le richieste GetObject tenteranno di recuperare i dati dalla griglia, prima di recuperarli da Cloud Storage Pool.

Stato dell'oggetto	Comportamento di GetObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	`200 OK` Viene recuperata una copia dell'oggetto.
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	`200 OK` Viene recuperata una copia dell'oggetto.
Oggetto sottoposto a transizione in uno stato non recuperabile	`403 Forbidden`, `InvalidObjectState` Utilizzare un "RestoreObject" richiesta di ripristino dell'oggetto in uno stato recuperabile.
Oggetto in fase di ripristino da uno stato non recuperabile	`403 Forbidden`, `InvalidObjectState` Attendere il completamento della richiesta RestoreObject.
Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK` Viene recuperata una copia dell'oggetto.

Oggetti multiparte o segmentati in un pool di storage cloud

Se hai caricato un oggetto multiparte o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta GetObject potrebbe non essere restituita correttamente `200 OK` quando alcune parti dell'oggetto sono già state trasferite in uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

In questi casi:

- La richiesta GetObject potrebbe restituire alcuni dati ma interrompersi a metà del trasferimento.
- Potrebbe essere restituita una richiesta GetObject successiva `403 Forbidden`.

Replica GetObject e cross-grid

Se si utilizza "federazione di grid" e. "replica cross-grid" È abilitato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta GetObject. La risposta include lo specifico StorageGRID `x-ntap-sg-cgr-replication-status` intestazione della risposta, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• **SUCCESSO**: La replica è riuscita. • **PENDING**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.

Griglia	Stato della replica
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

StorageGRID non supporta `x-amz-replication-status` intestazione.

HeadObject (oggetto intestazione)

È possibile utilizzare la richiesta HeadObject S3 per recuperare i metadati da un oggetto senza restituire l'oggetto stesso. Se l'oggetto viene memorizzato in un Cloud Storage Pool, è possibile utilizzare HeadObject per determinare lo stato di transizione dell'oggetto.

Oggetti HeadObject e multiparte

È possibile utilizzare `partNumber` richiedi il parametro per recuperare i metadati per una parte specifica di un oggetto multiparte o segmentato. Il `x-amz-mp-parts-count` l'elemento response indica il numero di parti dell'oggetto.

È possibile impostare `partNumber` a 1 per oggetti segmentati/multiparte e oggetti non segmentati/non multiparte; tuttavia, `x-amz-mp-parts-count` l'elemento di risposta viene restituito solo per gli oggetti segmentati o multiparte.

UTF-8 caratteri nei metadati dell'utente

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati nei metadati definiti dall'utente. Le richieste HEAD per un oggetto con caratteri UTF-8 escapati nei metadati definiti dall'utente non restituiscono `x-amz-missing-meta` intestazione se il nome o il valore della chiave include caratteri non stampabili.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`:

- `x-amz-website-redirect-location`

Versione

Se si seleziona `versionId` la sottorisorsa non viene specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "non trovato" con `x-amz-delete-marker` intestazione risposta impostata su `true`.

Intestazioni delle richieste per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)

Utilizzare tutte e tre queste intestazioni se l'oggetto è crittografato con una chiave univoca fornita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.
- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia dell'oggetto.

Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni in "Utilizzare la crittografia lato server".

Risposte HeadObject per gli oggetti Cloud Storage Pool

Se l'oggetto è memorizzato in "Pool di cloud storage", vengono restituite le seguenti intestazioni di risposta:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Le intestazioni delle risposte forniscono informazioni sullo stato di un oggetto quando viene spostato in un Cloud Storage Pool, facoltativamente trasferito in uno stato non recuperabile e ripristinato.

Stato dell'oggetto	Risposta a HeadObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	`200 OK` (Non viene restituita alcuna intestazione di risposta speciale).

Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: Continuing-request="false", expiry-date="Sab, 23 luglio 20 2030 00:00:00:00 GMT"`
	
	Fino a quando l'oggetto non passa a uno stato non recuperabile, il valore per `expiry-date` è impostato su un periodo di tempo lontano in futuro. L'ora esatta della transizione non è controllata dal sistema StorageGRID.

L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche nella griglia	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: Continuing-request="false", expiry-date="Sab, 23 luglio 20 2030 00:00:00:00 GMT"`
	
	Il valore per `expiry-date` è impostato su un periodo di tempo lontano in futuro.
	
	Nota: Se la copia sulla griglia non è disponibile (ad esempio, un nodo di storage non è disponibile), è necessario eseguire una "RestoreObject" Richiesta di ripristino della copia dal Cloud Storage Pool prima di poter recuperare correttamente l'oggetto.

Stato dell'oggetto	Risposta a HeadObject

L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia nella griglia	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Oggetto in fase di ripristino da uno stato non recuperabile	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: continue-request="true"`

Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: Continuing-request="false", expiry-date="Sab, 23 luglio 20 2018 00:00:00:00 GMT"`
	
	Il `expiry-date` Indica quando l'oggetto nel Cloud Storage Pool verrà riportato in uno stato non recuperabile.

Oggetti multiparte o segmentati nel Cloud Storage Pool

Se hai caricato un oggetto multiparte o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta HeadObject potrebbe restituire erroneamente `x-amz-restore: Continue-request="false" quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

HeadObject e replica cross-grid

Se si utilizza "federazione di grid" e. "replica cross-grid" È abilitato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta HeadObject. La risposta include lo specifico StorageGRID `x-ntap-sg-cgr-replication-status` intestazione della risposta, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• **SUCCESSO**: La replica è riuscita. • **PENDING**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

> StorageGRID non supporta `x-amz-replication-status` intestazione.

PutObject

È possibile utilizzare la richiesta S3 PutObject per aggiungere un oggetto a un bucket.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se sono presenti oggetti di dimensioni superiori a 5 GiB, utilizzare "caricamento multiparte" invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).

> Se è stato eseguito l'aggiornamento da StorageGRID 11,6 o versioni precedenti, l'avviso S3 PUT object size too large verrà attivato se si tenta di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11,7 o 11,8, l'avviso non verrà attivato in questo caso. Tuttavia, per allinearsi allo standard AWS S3, le versioni future di StorageGRID non supporteranno il caricamento di oggetti di dimensioni superiori a 5 GiB.

Dimensione dei metadati dell'utente

Amazon S3 limita la dimensione dei metadati definiti dall'utente all'interno di ogni intestazione di richiesta PUT a 2 KB. StorageGRID limita i metadati dell'utente a 24 KiB. La dimensione dei metadati definiti dall'utente viene misurata prendendo la somma del numero di byte nella codifica UTF-8 di ogni chiave e valore.

UTF-8 caratteri nei metadati dell'utente

Se una richiesta include valori UTF-8 (non escapati) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento di StorageGRID non è definito.

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 escapiti vengono trattati come caratteri ASCII:

- Le richieste PutObject, CopyObject, GetObject e HeadObject hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 di escape.
- StorageGRID non restituisce `x-amz-missing-meta` header se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

Limiti tag oggetto

È possibile aggiungere tag a nuovi oggetti durante il caricamento oppure aggiungerli a oggetti esistenti. StorageGRID e Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori di tag possono contenere fino a 256 caratteri Unicode. Chiave e valori distinguono tra maiuscole e minuscole.

Proprietà degli oggetti

In StorageGRID, tutti gli oggetti sono di proprietà dell'account del proprietario del bucket, inclusi gli oggetti creati da un account non proprietario o da un utente anonimo.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  Quando si specifica `aws-chunked` per `Content-Encoding`StorageGRID non verifica i seguenti elementi:

  - StorageGRID non verifica `chunk-signature` rispetto ai dati del blocco.
  - StorageGRID non verifica il valore fornito `x-amz-decoded-content-length` rispetto all'oggetto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  La codifica di trasferimento chunked è supportata se `aws-chunked` viene utilizzata anche la firma del payload.

- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente.

  Quando si specifica la coppia nome-valore per i metadati definiti dall'utente, utilizzare questo formato generale:

  ```
  x-amz-meta-name: value
  ```

  Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano quando l'oggetto è stato creato. Ad esempio:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  Il valore per `creation-time` Viene valutato in secondi dal 1° gennaio 1970.

  > Una regola ILM non può utilizzare sia un **tempo di creazione definito dall'utente** per il tempo di riferimento che l'opzione di acquisizione bilanciata o rigorosa. Quando viene creata la regola ILM viene restituito un errore.

- `x-amz-tagging`
- Intestazioni di richiesta blocco oggetti S3

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

  Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la modalità di versione dell'oggetto e mantenere la data fino alla data. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

- Intestazioni di richiesta SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Vedere Intestazioni di richiesta per la crittografia lato server

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- Il `x-amz-acl` intestazione della richiesta non supportata.
- Il `x-amz-website-redirect-location` l'intestazione della richiesta non è supportata e restituisce `XNotImplemented`.

Opzioni di classe storage

Il `x-amz-storage-class` l'intestazione della richiesta è supportata. Il valore inviato per `x-amz-storage-class` Influisce sul modo in cui StorageGRID protegge i dati degli oggetti durante l'acquisizione e non sul numero di copie persistenti dell'oggetto memorizzate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto acquisito utilizza l'opzione di acquisizione rigorosa, l' `x-amz-storage-class` l'intestazione non ha alcun effetto.

È possibile utilizzare i seguenti valori per `x-amz-storage-class`:

- `STANDARD` (Impostazione predefinita)
  - **Doppio commit**: Se la regola ILM specifica l'opzione doppio commit per il comportamento di Ingest, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita in un nodo di storage diverso (doppio commit). Quando viene valutato ILM, StorageGRID determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento della regola. In caso contrario, potrebbe essere necessario creare nuove copie degli oggetti in posizioni diverse e eliminare le copie intermedie iniziali.
  - **Balanced**: Se la regola ILM specifica l'opzione Balanced (bilanciamento) e StorageGRID non può eseguire immediatamente tutte le copie specificate nella regola, StorageGRID esegue due copie intermedie su nodi di storage diversi.

    Se StorageGRID è in grado di creare immediatamente tutte le copie degli oggetti specificate nella regola ILM (posizionamento sincrono), l' `x-amz-storage-class` l'intestazione non ha alcun effetto.

- `REDUCED_REDUNDANCY`
  - **Commit doppio**: Se la regola ILM specifica l'opzione commit doppio per il comportamento di Ingest, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (commit singolo).
  - **Balanced**: Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto.
    Il `REDUCED_REDUNDANCY` L'opzione è preferibile quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso, utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia di un oggetto extra per ogni operazione di acquisizione.

  Utilizzando il `REDUCED_REDUNDANCY` l'opzione non è consigliata in altre circostanze. `REDUCED_REDUNDANCY` aumenta il rischio di perdita dei dati degli oggetti durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.

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

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

> Se si sta inserendo un oggetto in un bucket con il blocco oggetti S3 attivato, il `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto con crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE**: Utilizzare la seguente intestazione se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca che si fornisce e si gestisce.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per il nuovo oggetto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.

Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni per "utilizzo della crittografia lato server".

Se un oggetto viene crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Versione

Se il controllo delle versioni è attivato per un bucket, viene visualizzato un valore univoco `versionId` viene generato automaticamente per la versione dell'oggetto memorizzato. Questo `versionId` viene inoltre restituito nella risposta utilizzando `x-amz-version-id` intestazione della risposta.

Se il controllo delle versioni è sospeso, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` se esiste già una versione nulla, questa verrà sovrascritta.

Calcoli della firma per l'intestazione autorizzazione

Quando si utilizza `Authorization` Header per autenticare le richieste, StorageGRID differisce da AWS nei seguenti modi:

- StorageGRID non richiede `host` intestazioni da includere in `CanonicalHeaders`.
- StorageGRID non richiede `Content-Type` da includere in `CanonicalHeaders`.
- StorageGRID non richiede `x-amz-*` intestazioni da includere in `CanonicalHeaders`.

Come Best practice generale, includere sempre queste intestazioni all'interno di `CanonicalHeaders` Per verificare che siano state verificate, tuttavia, se si escludono queste intestazioni, StorageGRID non restituisce alcun errore.

Per ulteriori informazioni, fare riferimento a. "Calcoli della firma per l'intestazione dell'autorizzazione: Trasferimento del payload in un singolo chunk (firma AWS versione 4)".

Informazioni correlate

"Gestire gli oggetti con ILM"

RestoreObject

È possibile utilizzare la richiesta S3 RestoreObject per ripristinare un oggetto memorizzato in un Cloud Storage Pool.

Tipo di richiesta supportato

StorageGRID supporta solo le richieste RestoreObject per ripristinare un oggetto. Non supporta `SELECT` tipo di ripristino. Selezionare Requests Return `XNotImplemented`.

Versione

Facoltativamente, specificare `versionId` per ripristinare una versione specifica di un oggetto in un bucket con versione. Se non si specifica `versionId`, viene ripristinata la versione più recente dell'oggetto

Comportamento di RestoreObject negli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in "Pool di cloud storage", Una richiesta RestoreObject ha il seguente comportamento, in base allo stato dell'oggetto. Vedere "HeadObject (oggetto intestazione)" per ulteriori dettagli.

> Se un oggetto viene memorizzato in un Cloud Storage Pool ed esistono anche una o più copie dell'oggetto nella griglia, non è necessario ripristinarlo inviando una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto non presente in un pool di storage cloud	`403 Forbidden`, `InvalidObjectState`
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	`200 OK` Non vengono apportate modifiche. **Nota**: Prima che un oggetto sia stato spostato in uno stato non recuperabile, non è possibile modificarne lo stato `expiry-date`.
Oggetto sottoposto a transizione in uno stato non recuperabile	`202 Accepted` Ripristina una copia recuperabile dell'oggetto nel Cloud Storage Pool per il numero di giorni specificato nel corpo della richiesta. Al termine di questo periodo, l'oggetto viene riportato in uno stato non recuperabile. In alternativa, utilizzare `Tier` elemento request per determinare il tempo necessario per il completamento del processo di ripristino (`Expedited`, `Standard`, o. `Bulk`). Se non si specifica `Tier`, il `Standard` viene utilizzato il tier. **Importante**: Se un oggetto è stato spostato in S3 Glacier Deep Archive o il Cloud Storage Pool utilizza lo storage Azure Blob, non è possibile ripristinarlo utilizzando `Expedited` tier. Viene visualizzato il seguente errore `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class`.
Oggetto in fase di ripristino da uno stato non recuperabile	`409 Conflict`, `RestoreAlreadyInProgress`
Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK` **Nota:** se un oggetto è stato ripristinato a uno stato recuperabile, è possibile modificarne lo stato `expiry-date` Riemettendo la richiesta RestoreObject con un nuovo valore per `Days`. La data di ripristino viene aggiornata in relazione all'ora della richiesta.

SelectObjectContent

È possibile utilizzare la richiesta S3 SelectObjectContent per filtrare il contenuto di un

oggetto S3 in base a una semplice istruzione SQL.

Per ulteriori informazioni, vedere "Riferimento API Amazon Simple Storage Service: SelectObjectContent".

Prima di iniziare

- L'account tenant dispone dell'autorizzazione S3 Select.
- Lo hai fatto `s3:GetObject` autorizzazione per l'oggetto che si desidera sottoporre a query.
- L'oggetto che si desidera sottoporre a query deve essere in uno dei seguenti formati:
  - **CSV**. Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
  - **Parquet**. Requisiti aggiuntivi per gli oggetti in parquet:
    - S3 Select supporta solo la compressione colonnare con GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti parquet.
    - S3 Select non supporta l'output parquet. Specificare il formato di output come CSV o JSON.
    - La dimensione massima del gruppo di righe non compresso è di 512 MB.
    - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
    - Non è possibile utilizzare TIPI logici INTERVAL, JSON, LIST, TIME o UUID.
- L'espressione SQL ha una lunghezza massima di 256 KB.
- Qualsiasi record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

Esempio di sintassi per le richieste CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Esempio di sintassi della richiesta di parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Esempio di query SQL

Questa query ottiene il nome dello stato, 2010 popolazioni, 2015 popolazioni stimate e la percentuale di cambiamento rispetto ai dati del censimento degli Stati Uniti. I record nel file che non sono stati vengono ignorati.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Le prime righe del file da interrogare, `SUB-EST2020_ALL.csv`, ad esempio:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Esempio di utilizzo di AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Le prime righe del file di output, `changes.csv`, ad esempio:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Esempio di utilizzo di AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Le prime righe del file di output, Changes.csv, sono le seguenti:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operazioni per caricamenti multiparte

Operazioni per upload multiparte: Panoramica

Questa sezione descrive come StorageGRID supporta le operazioni per gli upload di più parti.

Le seguenti condizioni e note si applicano a tutte le operazioni di caricamento multiparte:

- Non si devono superare i 1.000 caricamenti simultanei di più parti in un singolo bucket, poiché i risultati delle query ListMultipartUploads per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID applica i limiti di dimensione AWS per le parti multicpart. I client S3 devono seguire queste linee guida:
  - Ciascuna parte di un caricamento multiparte deve essere compresa tra 5 MiB (5,242,880 byte) e 5 GiB (5,368,709,120 byte).
  - L'ultima parte può essere inferiore a 5 MiB (5,242,880 byte).
  - In generale, le dimensioni delle parti devono essere il più grandi possibile. Ad esempio, utilizzare le dimensioni delle parti di 5 GiB per un oggetto 100 GiB. Poiché ogni parte è considerata un oggetto unico, l'utilizzo di parti di grandi dimensioni riduce l'overhead dei metadati StorageGRID.
  - Per gli oggetti di dimensioni inferiori a 5 GiB, prendere in considerazione l'utilizzo di un caricamento non multiparte.
- ILM viene valutato per ogni parte di un oggetto multiparte nel momento in cui viene acquisito e per l'oggetto nel suo complesso al termine del caricamento multiparte, se la regola ILM utilizza il bilanciato o il rigoroso "opzione di acquisizione". Devi essere consapevole di come questo influisca sul posizionamento di oggetti e parti:
  - Se ILM cambia mentre è in corso un caricamento multiparte S3, alcune parti dell'oggetto potrebbero

non soddisfare i requisiti ILM correnti al termine del caricamento multiparte. Qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e spostata nella posizione corretta in un secondo momento.

  - Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più grandi sono memorizzati a DC1 GB mentre tutti gli oggetti più piccoli sono memorizzati a DC2 GB, ogni parte da 1 GB di un caricamento multiparte in 10 parti viene memorizzata a DC2 GB al momento dell'acquisizione. Tuttavia, quando ILM viene valutato per l'oggetto nel suo complesso, tutte le parti dell'oggetto vengono spostate in DC1.

- Tutte le operazioni di caricamento multiparte supportano StorageGRID "valori di coerenza".
- Quando un oggetto viene acquisito utilizzando il caricamento multiparte, la "Soglia di segmentazione degli oggetti (1 GiB)" non è applicato.
- Se necessario, è possibile utilizzare "crittografia lato server" con upload multiparte. Per utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID), è necessario includere `x-amz-server-side-encryption` Intestazione della richiesta solo nella richiesta CreateMultipartUpload. Per utilizzare SSE-C (crittografia lato server con chiavi fornite dal cliente), specificare le stesse tre intestazioni di richiesta della chiave di crittografia nella richiesta CreateMultipartUpload e in ogni richiesta UploadPart successiva.

Operazione	Implementazione
AbortMultipartUpload	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
CompleteMultipartUpload	Vedere "CompleteMultipartUpload"
CreateMultipartUpload (Precedentemente denominato Initiate Multipart Upload)	Vedere "CreateMultipartUpload"
ListMultipartUploads	Vedere "ListMultipartUploads"
ListParts	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
UploadPart	Vedere "UploadPart"
UploadPartCopy	Vedere "UploadPartCopy"

CompleteMultipartUpload

L'operazione CompleteMultipartUpload completa il caricamento multiparte di un oggetto assemblando le parti caricate in precedenza.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Intestazioni delle richieste

Il `x-amz-storage-class` L'intestazione della richiesta è supportata e influisce sul numero di copie degli oggetti create da StorageGRID se la regola ILM corrispondente specifica Dual Commit o Balanced "opzione di acquisizione".

- `STANDARD`

  (Impostazione predefinita) specifica un'operazione di ingest dual-commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced (bilanciamento) torna alla creazione di copie interinali.

- `REDUCED_REDUNDANCY`

  Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione di commit doppio o quando l'opzione di bilanciamento ritorna alla creazione di copie interinali.

  > Se si sta inserendo un oggetto in un bucket con il blocco oggetti S3 attivato, il `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

> Se un caricamento multiparte non viene completato entro 15 giorni, l'operazione viene contrassegnata come inattiva e tutti i dati associati vengono cancellati dal sistema.

> Il `ETag` Il valore restituito non è una somma MD5 dei dati, ma segue l'implementazione dell'API Amazon S3 di `ETag` valore per oggetti multiparte.

Versione

Questa operazione completa un caricamento multiparte. Se il controllo delle versioni è attivato per un bucket, la versione dell'oggetto viene creata al termine del caricamento multiparte.

Se il controllo delle versioni è attivato per un bucket, viene visualizzato un valore univoco `versionId` viene generato automaticamente per la versione dell'oggetto memorizzato. Questo `versionId` viene inoltre restituito nella risposta utilizzando `x-amz-version-id` intestazione della risposta.

Se il controllo delle versioni è sospeso, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` se esiste già una versione nulla, questa verrà sovrascritta.

Quando il controllo delle versioni è attivato per un bucket, il completamento di un caricamento multiparte crea sempre una nuova versione, anche se ci sono caricamenti multipli simultanei completati sulla stessa chiave a oggetti. Quando il controllo delle versioni non è abilitato per un bucket, è possibile avviare un caricamento multiparte e fare in modo che un altro caricamento multiparte venga avviato e completato prima sulla stessa chiave a oggetti. Nei bucket senza versione, il caricamento multiparte che completa l'ultimo ha la precedenza.

Replica, notifica o notifica dei metadati non riuscite

Se il bucket in cui si verifica il caricamento multiparte è configurato per un servizio di piattaforma, il caricamento multiparte riesce anche se l'azione di replica o notifica associata non riesce.

In questo caso, viene generato un allarme in Grid Manager on Total Events (SMTT). L'ultimo evento visualizza il messaggio "Impossibile pubblicare le notifiche per la chiave bucket-nameobject" per l'ultimo oggetto la cui notifica non è riuscita. (Per visualizzare questo messaggio, selezionare **NODES** > ***Storage Node*** > **Events**. Visualizza ultimo evento nella parte superiore della tabella.) I messaggi degli eventi sono elencati anche nella `/var/local/log/bycast-err.log`.

Un tenant può attivare la replica o la notifica non riuscita aggiornando i metadati o i tag dell'oggetto. Un tenant può reinviare i valori esistenti per evitare modifiche indesiderate.

CreateMultipartUpload

L'operazione CreateMultipartUpload (precedentemente denominata Initiate Multipart Upload) avvia un caricamento multiparte per un oggetto e restituisce un ID di caricamento.

Il `x-amz-storage-class` l'intestazione della richiesta è supportata. Il valore inviato per `x-amz-storage-class` Influisce sul modo in cui StorageGRID protegge i dati degli oggetti durante l'acquisizione e non sul numero di copie persistenti dell'oggetto memorizzate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto acquisito utilizza Strict "opzione di acquisizione", il `x-amz-storage-class` l'intestazione non ha alcun effetto.

È possibile utilizzare i seguenti valori per `x-amz-storage-class`:

- `STANDARD` (Impostazione predefinita)
  - **Dual Commit**: Se la regola ILM specifica l'opzione di acquisizione Dual Commit, non appena un oggetto viene acquisito una seconda copia di tale oggetto viene creata e distribuita in un nodo di archiviazione diverso (dual commit). Quando viene valutato ILM, StorageGRID determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento della regola. In caso contrario, potrebbe essere necessario creare nuove copie degli oggetti in posizioni diverse e eliminare le copie intermedie iniziali.
  - **Balanced**: Se la regola ILM specifica l'opzione Balanced (bilanciamento) e StorageGRID non può eseguire immediatamente tutte le copie specificate nella regola, StorageGRID esegue due copie intermedie su nodi di storage diversi.

    Se StorageGRID è in grado di creare immediatamente tutte le copie degli oggetti specificate nella regola ILM (posizionamento sincrono), l' `x-amz-storage-class` l'intestazione non ha alcun effetto.
- `REDUCED_REDUNDANCY`

- **Dual Commit**: Se la regola ILM specifica l'opzione Dual Commit, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (Single Commit).
- **Balanced**: Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto.
  Il `REDUCED_REDUNDANCY` L'opzione è preferibile quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso, utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia di un oggetto extra per ogni operazione di acquisizione.

Utilizzando il `REDUCED_REDUNDANCY` l'opzione non è consigliata in altre circostanze. `REDUCED_REDUNDANCY` aumenta il rischio di perdita dei dati degli oggetti durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.

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

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

> Se si sta inserendo un oggetto in un bucket con il blocco oggetti S3 attivato, il `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Sono supportate le seguenti intestazioni di richiesta:

- `Content-Type`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente

  Quando si specifica la coppia nome-valore per i metadati definiti dall'utente, utilizzare questo formato generale:

  ```
  x-amz-meta-_name_: `value`
  ```

  Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano quando l'oggetto è stato creato. Ad esempio:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  Il valore per `creation-time` Viene valutato in secondi dal 1° gennaio 1970.

Aggiunta `creation-time` Poiché i metadati definiti dall'utente non sono consentiti se si aggiunge un oggetto a un bucket che ha abilitato la conformità legacy. Viene restituito un errore.

- Intestazioni della richiesta di blocco oggetti S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la versione dell'oggetto che resta aggiornata.

"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

- Intestazioni di richiesta SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Intestazioni di richiesta per la crittografia lato server

Per informazioni su come StorageGRID gestisce i caratteri UTF-8, vedere "PutObject".

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto multiparte con crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE**: Utilizzare la seguente intestazione nella richiesta CreateMultipartUpload se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID. Non specificare questa intestazione in nessuna delle richieste UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilizzare tutte e tre le intestazioni nella richiesta CreateMultipartUpload (e in ogni richiesta UploadPart successiva) se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per il nuovo oggetto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.

Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni per "utilizzo della crittografia lato server".

Intestazioni di richiesta non supportate

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`

- `x-amz-website-redirect-location`

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

ListMultipartUploads

L'operazione ListMultipartUploads elenca i caricamenti multiparte in corso per un bucket.

Sono supportati i seguenti parametri di richiesta:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

UploadPart

L'operazione UploadPart carica una parte in un upload multiparte per un oggetto.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Content-Length`

- `Content-MD5`

Intestazioni di richiesta per la crittografia lato server

Se è stata specificata la crittografia SSE-C per la richiesta CreateMultipartUpload, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.
- `x-amz-server-side-encryption-customer-key`: Specificare la stessa chiave di crittografia fornita nella richiesta CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare lo stesso digest MD5 fornito nella richiesta CreateMultipartUpload.

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni in "Utilizzare la crittografia lato server".

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

UploadPartCopy

L'operazione UploadPartCopy carica una parte di un oggetto copiando i dati da un oggetto esistente come origine dati.

L'operazione UploadPartCopy viene implementata con tutto il comportamento dell'API REST Amazon S3. Soggetto a modifiche senza preavviso.

Questa richiesta legge e scrive i dati dell'oggetto specificati in `x-amz-copy-source-range` Nel sistema StorageGRID.

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Intestazioni di richiesta per la crittografia lato server

Se è stata specificata la crittografia SSE-C per la richiesta CreateMultipartUpload, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.

- `x-amz-server-side-encryption-customer-key`: Specificare la stessa chiave di crittografia fornita nella richiesta CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare lo stesso digest MD5 fornito nella richiesta CreateMultipartUpload.

Se l'oggetto di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta UploadPartCopy, in modo che l'oggetto possa essere decrittografato e quindi copiato:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Specificare la chiave di crittografia fornita al momento della creazione dell'oggetto di origine.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 fornito al momento della creazione dell'oggetto di origine.

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni in "Utilizzare la crittografia lato server".

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

Risposte agli errori

Il sistema StorageGRID supporta tutte le risposte di errore standard dell'API REST S3 applicabili. Inoltre, l'implementazione di StorageGRID aggiunge diverse risposte personalizzate.

Codici di errore S3 API supportati

Nome	Stato HTTP
Accesso negato	403 proibita
BadDigest	400 richiesta errata
BucketAlreadyExists	409 conflitto
BucketNotEmpty	409 conflitto
IncompleteBody	400 richiesta errata
InternalError	500 errore interno del server

Nome	Stato HTTP
InvalidAccessKeyId	403 proibita
Documento invalidato	400 richiesta errata
InvalidBucketName	400 richiesta errata
InvalidBucketState	409 conflitto
InvalidDigest	400 richiesta errata
InvalidEncryptionAlgorithmError	400 richiesta errata
InvalidPart	400 richiesta errata
InvalidPartOrder	400 richiesta errata
InvalidRange	416 intervallo richiesto non riscontrabile
InvalidRequest	400 richiesta errata
InvalidStorageClass	400 richiesta errata
InvalidTag	400 richiesta errata
InvalidURI	400 richiesta errata
KeyTooLong	400 richiesta errata
MalformedXML	400 richiesta errata
MetadataTooLarge	400 richiesta errata
MethodNon consentito	405 metodo non consentito
MissingContentLength	411 lunghezza richiesta
MissingRequestBodyError	400 richiesta errata
MissingSecurityHeader	400 richiesta errata
NoSuchBucket	404 non trovato
NoSuchKey	404 non trovato

Nome	Stato HTTP
NoSuchUpload	404 non trovato
Non soddisfatto	501 non implementato
NoSuchBucketPolicy	404 non trovato
ObjectLockConfigurationNotFoundError	404 non trovato
PrecondizioneFailed	412 precondizione non riuscita
RequestTimeTooSkewed	403 proibita
ServiceUnavailable (Servizio non disponibile)	503 Servizio non disponibile
SignatureDoesNotMatch	403 proibita
TooManyBucket	400 richiesta errata
UserKeyMustBeSpecified	400 richiesta errata

Codici di errore personalizzati StorageGRID

Nome	Descrizione	Stato HTTP
XBucketLifecycleNotAllowed	La configurazione del ciclo di vita del bucket non è consentita in un bucket compatibile legacy	400 richiesta errata
XBucketPolicyParseException	Impossibile analizzare JSON policy bucket ricevuta.	400 richiesta errata
XComplianceConflict	Operazione negata a causa delle impostazioni di conformità legacy.	403 proibita
XComplianceRiduciRedundancyProibita	La ridondanza ridotta non è consentita nel bucket compatibile legacy	400 richiesta errata
XMaxBucketPolicyLengthExceed	La policy supera la lunghezza massima consentita della policy bucket.	400 richiesta errata
XMissingInternalRequestHeader	Manca un'intestazione di una richiesta interna.	400 richiesta errata
Conformità XNoSuchBucketCompliance	Nel bucket specificato non è attivata la compliance legacy.	404 non trovato

Nome	Descrizione	Stato HTTP
XNotAcceptable (XNotAccettabile)	La richiesta contiene una o più intestazioni di accettazione che non possono essere soddisfatte.	406 non accettabile
XNotImplemented	La richiesta fornita implica funzionalità non implementate.	501 non implementato

Operazioni personalizzate di StorageGRID

Operazioni personalizzate di StorageGRID: Panoramica

Il sistema StorageGRID supporta operazioni personalizzate che vengono aggiunte all'API REST S3.

Nella tabella seguente sono elencate le operazioni personalizzate supportate da StorageGRID.

Operazione	Descrizione
"COERENZA del bucket"	Restituisce la coerenza applicata a un determinato bucket.
"METTI la coerenza del bucket"	Imposta la coerenza applicata a un particolare bucket.
"OTTIENI l'ultimo tempo di accesso a bucket"	Restituisce se gli ultimi aggiornamenti dell'ora di accesso sono attivati o disattivati per un bucket specifico.
"TEMPO ULTIMO accesso bucket"	Consente di attivare o disattivare gli ultimi aggiornamenti dell'orario di accesso per un determinato bucket.
"ELIMINA la configurazione di notifica dei metadati del bucket"	Elimina l'XML di configurazione della notifica dei metadati associato a un bucket specifico.
"OTTIENI la configurazione della notifica dei metadati del bucket"	Restituisce l'XML di configurazione della notifica dei metadati associato a un bucket specifico.
"INSERIRE la configurazione della notifica dei metadati del bucket"	Configura il servizio di notifica dei metadati per un bucket.
"OTTIENI l'utilizzo dello storage"	Indica la quantità totale di spazio di archiviazione utilizzato da un account e per ciascun bucket associato all'account.
"Obsoleto: CreateBucket con impostazioni di conformità"	Obsoleto e non supportato: Non è più possibile creare nuovi bucket con Compliance abilitata.
"Obsoleto: OTTIENI la compliance del bucket"	Obsoleto ma supportato: Restituisce le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.

Operazione	Descrizione
"Obsoleto: METTI la compliance del bucket"	Obsoleto ma supportato: Consente di modificare le impostazioni di conformità per un bucket compatibile esistente.

COERENZA del bucket

La richiesta di coerenza GET Bucket consente di determinare la coerenza applicata a un determinato bucket.

La coerenza predefinita è impostata per garantire la lettura dopo scrittura per gli oggetti appena creati.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketConsistency o essere root dell'account.

Esempio di richiesta

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Risposta

Nella risposta XML, `<Consistency>` restituisce uno dei seguenti valori:

Coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
forte-globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
read-after-new-write	(Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
disponibile	Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Esempio di risposta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-new-write</Consistency>
```

Informazioni correlate

"Valori di coerenza"

METTI la coerenza del bucket

La richiesta di coerenza PUT bucket consente di specificare la coerenza da applicare alle operazioni eseguite su un bucket.

La coerenza predefinita è impostata per garantire la lettura dopo scrittura per gli oggetti appena creati.

Prima di iniziare

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:PutBucketConsistency o essere root dell'account.

Richiesta

Il `x-ntap-sg-consistency` il parametro deve contenere uno dei seguenti valori:

Coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
forte-globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
read-after-new-write	(Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.

Coerenza	Descrizione
disponibile	Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Nota: in generale, si dovrebbe usare la coerenza "Read-after-new-write". Se le richieste non funzionano correttamente, modificare il comportamento del client dell'applicazione, se possibile. In alternativa, configurare il client per specificare la coerenza per ogni richiesta API. Impostare la consistenza a livello del bucket solo come ultima risorsa.

Esempio di richiesta

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informazioni correlate

"Valori di coerenza"

OTTIENI l'ultimo tempo di accesso a bucket

La richiesta GET bucket last access time (OTTIENI bucket ultimo accesso) consente di determinare se gli ultimi aggiornamenti dell'orario di accesso sono attivati o disattivati per i singoli bucket.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketLastAccessTime o essere root dell'account.

Esempio di richiesta

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Questo esempio mostra che gli ultimi aggiornamenti dell'ora di accesso sono attivati per il bucket.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

TEMPO ULTIMO accesso bucket

La richiesta PUT bucket Last access time consente di attivare o disattivare gli ultimi aggiornamenti del tempo di accesso per i singoli bucket. La disattivazione degli ultimi aggiornamenti dell'orario di accesso migliora le prestazioni ed è l'impostazione predefinita per tutti i bucket creati con la versione 10.3.0 o successiva.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:PutBucketLastAccessTime per un bucket o essere root dell'account.

> A partire dalla versione 10.3 di StorageGRID, gli aggiornamenti all'ultimo tempo di accesso sono disattivati per impostazione predefinita per tutti i nuovi bucket. Se si dispone di bucket creati utilizzando una versione precedente di StorageGRID e si desidera che corrispondano al nuovo comportamento predefinito, è necessario disattivare esplicitamente gli ultimi aggiornamenti del tempo di accesso per ciascuno di questi bucket precedenti. È possibile attivare o disattivare gli aggiornamenti per l'ora dell'ultimo accesso utilizzando la richiesta PUT Bucket last access time o dalla pagina dei dettagli di un bucket in Tenant Manager. Vedere "Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso".

Se gli ultimi aggiornamenti dell'ora di accesso sono disattivati per un bucket, alle operazioni sul bucket viene applicato il seguente comportamento:

- Le richieste GetObject, GetObjectAcl, GetObjectTagging e HeadObject non aggiornano l'ora dell'ultimo accesso. L'oggetto non viene aggiunto alle code per la valutazione ILM (Information Lifecycle Management).
- Le richieste CopyObject e PutObjectTagging che aggiornano solo i metadati aggiornano anche l'ora dell'ultimo accesso. L'oggetto viene aggiunto alle code per la valutazione ILM.
- Se gli aggiornamenti dell'ora dell'ultimo accesso sono disattivati per il bucket di origine, le richieste CopyObject non aggiornano l'ora dell'ultimo accesso per il bucket di origine. L'oggetto copiato non viene aggiunto alle code per la valutazione ILM del bucket di origine. Tuttavia, per la destinazione, le richieste CopyObject aggiornano sempre l'ora dell'ultimo accesso. La copia dell'oggetto viene aggiunta alle code per la valutazione ILM.
- CompleteMultipartUpload richiede l'aggiornamento dell'ora di ultimo accesso. L'oggetto completato viene aggiunto alle code per la valutazione ILM.

Richiedi esempi

In questo esempio viene attivato l'ultimo tempo di accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Questo esempio disattiva l'ultimo tempo di accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

ELIMINA la configurazione di notifica dei metadati del bucket

La richiesta di configurazione DELLA notifica dei metadati DEL bucket DELETE consente di disattivare il servizio di integrazione della ricerca per i singoli bucket eliminando il file XML di configurazione.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:DeleteBucketMetadataNotification per un bucket o essere root dell'account.

Esempio di richiesta

Questo esempio mostra la disattivazione del servizio di integrazione della ricerca per un bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

OTTIENI la configurazione della notifica dei metadati del bucket

La richiesta DI configurazione DELLA notifica dei metadati GET Bucket consente di recuperare l'XML di configurazione utilizzato per configurare l'integrazione della ricerca per i singoli bucket.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketMetadataNotification o essere root dell'account.

Esempio di richiesta

Questa richiesta recupera la configurazione di notifica dei metadati per il bucket denominato `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Risposta

Il corpo della risposta include la configurazione della notifica dei metadati per il bucket. La configurazione della notifica dei metadati consente di determinare la configurazione del bucket per l'integrazione della ricerca. Ciò consente di determinare quali oggetti vengono indicizzati e a quali endpoint vengono inviati i metadati degli oggetti.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Ogni configurazione di notifica dei metadati include una o più regole. Ogni regola specifica gli oggetti a cui si applica e la destinazione in cui StorageGRID deve inviare i metadati degli oggetti. Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfiguration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi della regola.	Sì

Nome	Descrizione	Obbligatorio
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato. Le regole con prefissi sovrapposti vengono rifiutate. Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola. Incluso nell'elemento Rule.	No
Stato	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì

Nome	Descrizione	Obbligatorio
Urna	URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • `es` deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel form `domain-name/myindex/mytype`. Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404. L'urn è incluso nell'elemento Destination.	Sì

Esempio di risposta

L'XML incluso tra `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tag mostra come è configurata l'integrazione con un endpoint di integrazione della ricerca per il bucket. In questo esempio, i metadati degli oggetti vengono inviati a un indice Elasticsearch denominato `current` e digitare named `2017` Che è ospitato in un dominio AWS denominato `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informazioni correlate

"Utilizzare un account tenant"

INSERIRE la configurazione della notifica dei metadati del bucket

La richiesta di configurazione DELLA notifica dei metadati PUT bucket consente di attivare il servizio di integrazione della ricerca per i singoli bucket. L'XML di configurazione della notifica dei metadati fornito nel corpo della richiesta specifica gli oggetti i cui metadati vengono inviati all'indice di ricerca di destinazione.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:PutBucketMetadataNotification per un bucket o essere account root.

Richiesta

La richiesta deve includere la configurazione della notifica dei metadati nel corpo della richiesta. Ogni configurazione di notifica dei metadati include una o più regole. Ogni regola specifica gli oggetti a cui si applica e la destinazione in cui StorageGRID deve inviare i metadati degli oggetti.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, è possibile inviare metadati per oggetti con il prefisso `/images` a una destinazione e agli oggetti con il prefisso `/videos` a un altro.

Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, una configurazione che includeva una regola per per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2` non sarebbe consentito.

Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID. L'endpoint deve

esistere quando viene inviata la configurazione della notifica dei metadati, oppure la richiesta non riesce come a. `400 Bad Request`. Il messaggio di errore indica: `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN`.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

La tabella descrive gli elementi contenuti nel file XML di configurazione per la notifica dei metadati.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfiguration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi della regola.	Sì
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato. Le regole con prefissi sovrapposti vengono rifiutate. Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola. Incluso nell'elemento Rule.	No

Nome	Descrizione	Obbligatorio
Stato	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì
Urna	URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • `es` deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel form `domain-name/myindex/mytype`. Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404. L'urn è incluso nell'elemento Destination.	Sì

Richiedi esempi

Questo esempio mostra come abilitare l'integrazione della ricerca per un bucket. In questo esempio, i metadati degli oggetti per tutti gli oggetti vengono inviati alla stessa destinazione.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

In questo esempio, i metadati degli oggetti per gli oggetti che corrispondono al prefisso `/images` viene inviato a una destinazione, mentre i metadati degli oggetti per gli oggetti che corrispondono al prefisso `/videos` viene inviato a una seconda destinazione.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON generato dal servizio di integrazione della ricerca

Quando si attiva il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato all'endpoint di destinazione ogni volta che vengono aggiunti, aggiornati o cancellati metadati o tag dell'oggetto.

Questo esempio mostra un esempio di JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. Il `test` bucket non è configurato, quindi il `versionId` tag vuoto.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadati degli oggetti inclusi nelle notifiche dei metadati

La tabella elenca tutti i campi inclusi nel documento JSON che viene inviato all'endpoint di destinazione quando è attivata l'integrazione della ricerca.

Il nome del documento include il nome del bucket, il nome dell'oggetto e l'ID della versione, se presente.

Tipo	Nome dell'elemento	Descrizione
Informazioni su bucket e oggetti	bucket	Nome del bucket
Informazioni su bucket e oggetti	chiave	Nome chiave oggetto
Informazioni su bucket e oggetti	ID versione	Versione oggetto, per gli oggetti nei bucket con versione
Informazioni su bucket e oggetti	regione	Area bucket, ad esempio `us-east-1`
Metadati di sistema	dimensione	Dimensione dell'oggetto (in byte) come visibile a un client HTTP
Metadati di sistema	md5	Hash di oggetto
Metadati dell'utente	metadati *`key:value`*	Tutti i metadati dell'utente per l'oggetto, come coppie chiave-valore

Tipo	Nome dell'elemento	Descrizione
Tag	tag *key:value*	Tutti i tag di oggetto definiti per l'oggetto, come coppie chiave-valore

> Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Prima di configurare il servizio di integrazione della ricerca, è necessario attivare le mappature dinamiche dei campi sull'indice. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Informazioni correlate

"Utilizzare un account tenant"

OTTIENI la richiesta di utilizzo dello storage

La richiesta GET Storage Usage indica la quantità totale di storage in uso da un account e per ciascun bucket associato all'account.

La quantità di spazio di archiviazione utilizzata da un account e dai relativi bucket può essere ottenuta mediante una richiesta ListBuckets modificata con `x-ntap-sg-usage` parametro di query. L'utilizzo dello storage bucket viene monitorato separatamente dalle richieste DI PUT ed ELIMINAZIONE elaborate dal sistema. Potrebbe verificarsi un ritardo prima che i valori di utilizzo corrispondano ai valori previsti in base all'elaborazione delle richieste, in particolare se il sistema è sottoposto a un carico pesante.

Per impostazione predefinita, StorageGRID tenta di recuperare le informazioni sull'utilizzo utilizzando una coerenza forte-globale. Se non è possibile ottenere una forte coerenza globale, StorageGRID tenta di recuperare le informazioni sull'utilizzo con una forte coerenza del sito.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:ListAllMyBucket o essere root dell'account.

Esempio di richiesta

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Questo esempio mostra un account con quattro oggetti e 12 byte di dati in due bucket. Ogni bucket contiene due oggetti e sei byte di dati.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Versione

Ogni versione dell'oggetto memorizzata contribuirà a. `ObjectCount` e. `DataBytes` valori nella risposta. I contrassegni di eliminazione non vengono aggiunti a `ObjectCount` totale.

Informazioni correlate

"Valori di coerenza"

Richieste bucket obsolete per conformità legacy

Richieste bucket obsolete per conformità legacy

Potrebbe essere necessario utilizzare l'API REST di StorageGRID S3 per gestire i bucket creati utilizzando la funzionalità di conformità legacy.

Funzionalità di compliance obsoleta

La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3.

Se in precedenza è stata attivata l'impostazione di conformità globale, l'impostazione di blocco oggetti S3 globale viene attivata in StorageGRID 11.6. Non è più possibile creare nuovi bucket con la conformità abilitata; tuttavia, se necessario, è possibile utilizzare l'API REST di StorageGRID S3 per gestire qualsiasi bucket compatibile esistente.

- "Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
- "Gestire gli oggetti con ILM"
- "Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"

Richieste di conformità obsolete:

- "Deprecato - CONSENTE DI APPORTARE modifiche alla richiesta di conformità al bucket"

  L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML opzionale di PUT bucket Requests per creare un bucket conforme.

- "Obsoleto - CONFORMITÀ bucket"

  La richiesta DI compliance GET Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.

- "Deprecato - METTERE la compliance del bucket"

  La richiesta DI compliance DEL bucket PUT è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket compatibile esistente. Ad esempio, è possibile mettere un bucket esistente in attesa legale o aumentarne il periodo di conservazione.

Obsoleto: CreateBucket richiede modifiche per la conformità

L'elemento XML SGCompliance è obsoleto. In precedenza, è possibile includere questo elemento personalizzato StorageGRID nel corpo di richiesta XML opzionale delle richieste CreateBucket per creare un bucket conforme.

> La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3. Per ulteriori informazioni, vedere quanto segue:
>
> - "Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
> - "Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"

Non è più possibile creare nuovi bucket con Compliance abilitata. Se si tenta di utilizzare le modifiche della richiesta CreateBucket per la conformità per creare un nuovo bucket conforme, viene visualizzato il seguente messaggio di errore:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Deprecato: OTTIENI una richiesta di conformità bucket

La richiesta DI compliance GET Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.

> La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3. Per ulteriori informazioni, vedere quanto segue:
>
> - "Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
> - "Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketCompliance o essere root dell'account.

Esempio di richiesta

Questa richiesta di esempio consente di determinare le impostazioni di conformità per il bucket denominato `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Nella risposta XML, `<SGCompliance>` elenca le impostazioni di compliance in vigore per il bucket. Questa risposta di esempio mostra le impostazioni di compliance per un bucket in cui ciascun oggetto verrà conservato per un anno (525,600 minuti), a partire da quando l'oggetto viene acquisito nella griglia. Attualmente non esiste un blocco legale in questo bucket. Ogni oggetto verrà automaticamente cancellato dopo un anno.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrizione
RetentionPeriodMinutes	La durata del periodo di conservazione per gli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene acquisito nella griglia.
LegalHold	• Vero: Questo bucket è attualmente sotto una stretta legale. Gli oggetti in questo bucket non possono essere cancellati fino a quando non viene revocata la conservazione a fini giudiziari, anche se il periodo di conservazione è scaduto. • Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.
Eliminazione automatica	• Vero: Gli oggetti in questo bucket verranno cancellati automaticamente allo scadere del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale. • Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.

Risposte agli errori

Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è `404 Not Found`, Con un codice di errore S3 di `XNoSuchBucketCompliance`.

Deprecato: INSERIRE la richiesta di conformità del bucket

La richiesta DI compliance DEL bucket PUT è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket compatibile esistente. Ad esempio, è possibile mettere un bucket esistente in attesa legale o aumentarne il periodo di conservazione.

La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3. Per ulteriori informazioni, vedere quanto segue:

- "Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
- "Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:PutBucketCompliance o essere root dell'account.

È necessario specificare un valore per ogni campo delle impostazioni di compliance quando si invia una richiesta DI compliance PUT bucket.

Esempio di richiesta

Questa richiesta di esempio modifica le impostazioni di compliance per il bucket denominato `mybucket`. In questo esempio, gli oggetti in `mybucket` verrà ora conservato per due anni (1,051,200 minuti) invece di un anno, a partire dal momento in cui l'oggetto viene acquisito nella griglia. Questo bucket non ha alcuna tenuta legale. Ogni oggetto verrà automaticamente cancellato dopo due anni.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrizione
RetentionPeriodMinutes	La durata del periodo di conservazione per gli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene acquisito nella griglia. **Importante** quando si specifica un nuovo valore per RetentionPeriodMinutes, è necessario specificare un valore uguale o superiore al periodo di conservazione corrente del bucket. Una volta impostato il periodo di conservazione del bucket, non è possibile diminuire tale valore, ma solo aumentarlo.

Nome	Descrizione
LegalHold	• Vero: Questo bucket è attualmente sotto una stretta legale. Gli oggetti in questo bucket non possono essere cancellati fino a quando non viene revocata la conservazione a fini giudiziari, anche se il periodo di conservazione è scaduto. • Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.
Eliminazione automatica	• Vero: Gli oggetti in questo bucket verranno cancellati automaticamente allo scadere del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale. • Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.

Coerenza per le impostazioni di conformità

Quando aggiorni le impostazioni di compliance per un bucket S3 con una richiesta DI compliance PUT bucket, StorageGRID tenta di aggiornare i metadati del bucket nella griglia. Per impostazione predefinita, StorageGRID utilizza la coerenza **strong-Global** per garantire che tutti i siti dei data center e tutti i nodi di storage che contengono i metadati del bucket abbiano coerenza di lettura dopo scrittura per le impostazioni di conformità modificate.

Se StorageGRID non riesce a raggiungere la coerenza **strong-Global** perché un sito di data center o più nodi di archiviazione in un sito non sono disponibili, il codice di stato HTTP per la risposta è `503 Service Unavailable.`

Se si riceve questa risposta, è necessario contattare l'amministratore del grid per assicurarsi che i servizi di storage richiesti siano resi disponibili il prima possibile. Se l'amministratore della griglia non è in grado di rendere disponibile una quantità sufficiente di nodi di archiviazione in ogni sito, il supporto tecnico potrebbe richiedere di riprovare la richiesta non riuscita forzando la coerenza **strong-Site**.

> Non forzare mai la coerenza **strong-site** per la conformità del bucket PUT a meno che non sia stato richiesto dal supporto tecnico e a meno che non si capiscano le potenziali conseguenze dell'utilizzo di questo livello.

Quando la coerenza viene ridotta a **strong-Site**, StorageGRID garantisce che le impostazioni di conformità aggiornate abbiano coerenza di lettura dopo scrittura solo per le richieste client all'interno di un sito. Ciò significa che il sistema StorageGRID potrebbe disporre temporaneamente di più impostazioni incoerenti per questo bucket fino a quando non saranno disponibili tutti i siti e i nodi di storage. Le impostazioni incoerenti possono causare comportamenti imprevisti e indesiderati. Ad esempio, se si colloca un bucket in una conservazione legale e si forza una minore coerenza, le precedenti impostazioni di conformità del bucket (ovvero, blocco legale) potrebbero continuare a essere attive in alcuni data center. Di conseguenza, gli oggetti che si ritiene siano in stato di conservazione a fini giudiziari potrebbero essere eliminati allo scadere del periodo di conservazione, dall'utente o mediante eliminazione automatica, se attivata.

Per forzare l'uso della coerenza **strong-Site**, riemettere la richiesta di conformità PUT Bucket e includere il `Consistency-Control` Intestazione della richiesta HTTP, come segue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Risposte agli errori

- Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è `404 Not Found`.
- Se `RetentionPeriodMinutes` Se la richiesta è inferiore al periodo di conservazione corrente del bucket, il codice di stato HTTP è `400 Bad Request`.

Informazioni correlate

"Deprecato: APPORTARE modifiche alla richiesta di conformità al bucket"

Policy di accesso a bucket e gruppi

Utilizza policy di accesso a bucket e gruppi

StorageGRID utilizza il linguaggio delle policy di Amazon Web Services (AWS) per consentire ai tenant S3 di controllare l'accesso ai bucket e agli oggetti all'interno di tali bucket. Il sistema StorageGRID implementa un sottoinsieme del linguaggio dei criteri delle API REST S3. I criteri di accesso per l'API S3 sono scritti in JSON.

Panoramica dei criteri di accesso

StorageGRID supporta due tipi di policy di accesso.

- **Criteri bucket**, che sono gestiti utilizzando le operazioni API GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy S3. Le policy del bucket sono collegate ai bucket, quindi sono configurate per controllare l'accesso degli utenti nell'account del proprietario del bucket o altri account al bucket e agli oggetti in esso contenuti. Una policy di bucket si applica a un solo bucket ed eventualmente a più gruppi.
- **Criteri di gruppo**, configurati utilizzando l'API di gestione tenant Manager o tenant. I criteri di gruppo sono associati a un gruppo dell'account, quindi sono configurati per consentire a tale gruppo di accedere a risorse specifiche di proprietà di tale account. Una policy di gruppo si applica a un solo gruppo e possibilmente a più bucket.

> Non vi è alcuna differenza di priorità tra le policy di gruppo e quelle di bucket.

Le policy di gruppo e bucket di StorageGRID seguono una grammatica specifica definita da Amazon. All'interno di ogni policy è presente una serie di dichiarazioni di policy, ciascuna delle quali contiene i seguenti elementi:

- ID dichiarazione (Sid) (opzionale)
- Effetto
- Principal/NotPrincipal
- Risorsa/NotResource
- Azione/Notazione
- Condizione (opzionale)

Le istruzioni dei criteri vengono create utilizzando questa struttura per specificare le autorizzazioni: Grant <Effect> per consentire/negare a <Principal> di eseguire <Action> su <Resource> quando viene applicato <Condition>.

Ciascun elemento di policy viene utilizzato per una funzione specifica:

Elemento	Descrizione
SID	L'elemento Sid è opzionale. Il Sid deve essere utilizzato solo come descrizione per l'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID.
Effetto	Utilizzare l'elemento Effect per stabilire se le operazioni specificate sono consentite o rifiutate. È necessario identificare le operazioni consentite (o negate) su bucket o oggetti utilizzando le parole chiave dell'elemento Action supportate.
Principal/NotPrincipal	È possibile consentire a utenti, gruppi e account di accedere a risorse specifiche ed eseguire azioni specifiche. Se nella richiesta non è inclusa alcuna firma S3, l'accesso anonimo è consentito specificando il carattere jolly (*) come principale. Per impostazione predefinita, solo l'account root ha accesso alle risorse di proprietà dell'account. È sufficiente specificare l'elemento Principal in una policy bucket. Per i criteri di gruppo, il gruppo a cui è associato il criterio è l'elemento Principal implicito.
Risorsa/NotResource	L'elemento Resource identifica bucket e oggetti. Puoi consentire o negare le autorizzazioni per bucket e oggetti utilizzando il nome risorsa Amazon (ARN) per identificare la risorsa.
Azione/Notazione	Gli elementi Action e Effect sono i due componenti delle autorizzazioni. Quando un gruppo richiede una risorsa, gli viene concesso o negato l'accesso alla risorsa. L'accesso viene negato a meno che non si assegnino specificamente autorizzazioni, ma è possibile utilizzare la funzione di negazione esplicita per ignorare un'autorizzazione concessa da un altro criterio.
Condizione	L'elemento Condition è opzionale. Le condizioni consentono di creare espressioni per determinare quando applicare un criterio.

Nell'elemento Action, è possibile utilizzare il carattere jolly (*) per specificare tutte le operazioni o un sottoinsieme di operazioni. Ad esempio, questa azione corrisponde a permessi come s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

Nell'elemento Resource, è possibile utilizzare i caratteri jolly (**) e (?). Mentre l'asterisco (**) corrisponde a 0 o più caratteri, il punto interrogativo (?) corrisponde a qualsiasi singolo carattere.

Nell'elemento Principal, i caratteri jolly non sono supportati, ad eccezione dell'impostazione dell'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, impostare il carattere jolly (*) come valore Principal.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

Nell'esempio seguente, l'istruzione utilizza gli elementi Effect, Principal, Action e Resource. Questo esempio mostra un'istruzione completa di policy bucket che utilizza l'effetto "allow" per assegnare i Principal, il gruppo di amministrazione `federated-group/admin` e il gruppo finanziario `federated-group/finance`, Autorizzazioni per eseguire l'azione `s3:ListBucket` sul bucket denominato `mybucket` E l'azione `s3:GetObject` su tutti gli oggetti all'interno del bucket.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

Il criterio bucket ha un limite di dimensione di 20,480 byte e il criterio di gruppo ha un limite di dimensione di 5,120 byte.

Coerenza delle policy

Per impostazione predefinita, gli aggiornamenti apportati ai criteri di gruppo sono coerenti. Quando un criterio di gruppo diventa coerente, le modifiche possono richiedere altri 15 minuti, a causa della memorizzazione nella cache dei criteri. Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri bucket sono fortemente coerenti.

Come richiesto, è possibile modificare le garanzie di coerenza per gli aggiornamenti delle policy bucket. Ad esempio, è possibile rendere disponibile una modifica a un criterio bucket in caso di fuori servizio di un sito.

In questo caso, è possibile impostare `Consistency-Control` Nella richiesta PutBucketPolicy oppure è possibile utilizzare la richiesta di coerenza PUT Bucket. Quando un criterio bucket diventa coerente, le modifiche possono richiedere altri 8 secondi per diventare effettive, a causa del caching delle policy.

> Se si imposta la coerenza su un valore diverso per risolvere una situazione temporanea, assicurarsi di riportare l'impostazione del livello del bucket al valore originale al termine dell'operazione. In caso contrario, tutte le richieste bucket future utilizzeranno l'impostazione modificata.

Utilizzare ARN nelle dichiarazioni delle policy

Nelle dichiarazioni delle policy, l'ARN viene utilizzato negli elementi Principal e Resource.

- Utilizzare questa sintassi per specificare la risorsa S3 ARN:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilizzare questa sintassi per specificare l'ARN della risorsa di identità (utenti e gruppi):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Altre considerazioni:

- È possibile utilizzare l'asterisco (*) come carattere jolly per far corrispondere zero o più caratteri all'interno della chiave oggetto.
- I caratteri internazionali, che possono essere specificati nella chiave oggetto, devono essere codificati utilizzando JSON UTF-8 o le sequenze di escape JSON. La codifica in percentuale non è supportata.

  "Sintassi URN RFC 2141"

  Il corpo della richiesta HTTP per l'operazione PutBucketPolicy deve essere codificato con charset=UTF-8.

Specificare le risorse in un criterio

Nelle istruzioni policy, è possibile utilizzare l'elemento Resource per specificare il bucket o l'oggetto per cui le autorizzazioni sono consentite o negate.

- Ogni dichiarazione di policy richiede un elemento Resource. In un criterio, le risorse sono indicate dall'elemento `Resource`, o in alternativa, `NotResource` per l'esclusione.
- Specificare le risorse con un ARN di risorsa S3. Ad esempio:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- È inoltre possibile utilizzare le variabili dei criteri all'interno della chiave a oggetti. Ad esempio:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- Il valore della risorsa può specificare un bucket che non esiste ancora quando viene creata una policy di gruppo.

Specificare le entità in un criterio

Utilizzare l'elemento Principal per identificare l'account utente, gruppo o tenant a cui è consentito/negato l'accesso alla risorsa dall'istruzione policy.

- Ogni dichiarazione di policy in una policy bucket deve includere un elemento Principal. Le dichiarazioni di policy in una policy di gruppo non necessitano dell'elemento Principal perché il gruppo è considerato il principale.
- In un criterio, i principal sono indicati dall'elemento "Principal" o in alternativa "NotPrincipal" per l'esclusione.
- Le identità basate sull'account devono essere specificate utilizzando un ID o un ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- In questo esempio viene utilizzato l'ID account tenant 27233906934684427525, che include l'account root e tutti gli utenti dell'account:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- È possibile specificare solo l'account root:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- È possibile specificare un utente federato specifico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- È possibile specificare uno specifico gruppo federated ("Manager"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- È possibile specificare un'entità anonima:

```
"Principal": "*"
```

- Per evitare ambiguità, è possibile utilizzare l'UUID utente invece del nome utente:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Ad esempio, supponiamo che Alex lasci l'organizzazione e il nome utente `Alex` viene cancellato. Se un nuovo Alex entra a far parte dell'organizzazione e viene assegnato lo stesso `Alex` nome utente, il nuovo utente potrebbe ereditare involontariamente le autorizzazioni concesse all'utente originale.

- Il valore principale può specificare un nome utente/gruppo che non esiste ancora quando viene creata una policy bucket.

Specificare le autorizzazioni in un criterio

In un criterio, l'elemento Action viene utilizzato per consentire/negare le autorizzazioni a una risorsa. È possibile specificare una serie di autorizzazioni in un criterio, indicate dall'elemento "Action" o, in alternativa, "NotAction" per l'esclusione. Ciascuno di questi elementi viene associato a specifiche operazioni REST API S3.

Le tabelle elencano le autorizzazioni applicabili ai bucket e le autorizzazioni applicabili agli oggetti.

> Amazon S3 ora utilizza l'autorizzazione S3:PutReplicationConfiguration per entrambe le azioni PutBucketReplication e DeleteBucketReplication. StorageGRID utilizza autorizzazioni separate per ciascuna azione, che corrispondono alla specifica originale di Amazon S3.

> Un'eliminazione viene eseguita quando si utilizza un put per sovrascrivere un valore esistente.

Autorizzazioni applicabili ai bucket

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:CreateBucket	CreateBucket	Sì. **Nota**: Utilizzare solo nei criteri di gruppo.
s3:Deletebucket	DeleteBucket	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:DeleteBucketMetadataNotification	ELIMINA la configurazione di notifica dei metadati del bucket	Sì
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBucketReplication	Sì, separare le autorizzazioni per PUT ed DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	OTTIENI compliance bucket (obsoleta)	Sì
s3:GetBucketConsistency	COERENZA del bucket	Sì
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	OTTIENI l'ultimo tempo di accesso a bucket	Sì
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	OTTIENI la configurazione della notifica dei metadati del bucket	Sì
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:ListAllMyBucket	• ListBucket • OTTIENI l'utilizzo dello storage	Sì, per OTTIENI utilizzo storage. **Nota**: Utilizzare solo nei criteri di gruppo.
s3:ListBucket	• ListObjects (oggetti elenco) • HeadBucket • RestoreObject	
s3:ListBucketMultipartUploads	• ListMultipartUploads • RestoreObject	
s3:ListBucketVersions	SCARICA le versioni di bucket	
s3:PutBucketCompliance	METTERE la compliance del bucket (obsoleta)	Sì
s3:PutBucketConsistency	METTI la coerenza del bucket	Sì
s3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:PutBucketLastAccessTime	TEMPO ULTIMO accesso bucket	Sì
s3:PutBucketMetadataNotification	INSERIRE la configurazione della notifica dei metadati del bucket	Sì
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	• CreateBucket con `x-amz-bucket-object-lock-enabled: true` Intestazione della richiesta (richiede anche l'autorizzazione s3:CreateBucket) • PutObjectLockConfiguration	
s3:PutBucketPolicy	PutBucketPolicy	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:PutBucketTagging	• DeleteBucketTagging† • PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	Sì, separare le autorizzazioni per PUT ed DELETE

Autorizzazioni applicabili agli oggetti

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:AbortMultipartUpload	• AbortMultipartUpload • RestoreObject	
s3:BypassGovernanceRetention	• DeleteObject (Elimina oggetto) • DeleteObjects • PutObjectRetention	
s3:DeleteObject	• DeleteObject (Elimina oggetto) • DeleteObjects • RestoreObject	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (una versione specifica dell'oggetto)	
s3:DeleteObjectVersion	DeleteObject (una versione specifica dell'oggetto)	
s3:GetObject	• GetObject • HeadObject (oggetto intestazione) • RestoreObject • SelectObjectContent	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (una versione specifica dell'oggetto)	
s3:GetObjectVersion	GetObject (una versione specifica dell'oggetto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• PutObject • Oggetto CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (una versione specifica dell'oggetto)	
s3:PutOverwriteObject	• PutObject • Oggetto CopyObject • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload	Sì
s3:RestoreObject (Riavvia oggetto)	RestoreObject	

Utilizza l'autorizzazione PutOverwriteObject

l'autorizzazione s3:PutOverwriteObject è un'autorizzazione StorageGRID personalizzata che si applica alle operazioni che creano o aggiornano oggetti. L'impostazione di questa autorizzazione determina se il client può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o il tagging degli oggetti S3.

Le impostazioni possibili per questa autorizzazione includono:

- **Allow**: Il client può sovrascrivere un oggetto. Questa è l'impostazione predefinita.
- **Nega**: Il client non può sovrascrivere un oggetto. Se impostata su Nega, l'autorizzazione PutOverwriteObject funziona come segue:
  - Se un oggetto esistente viene trovato nello stesso percorso:
    - I dati dell'oggetto, i metadati definiti dall'utente o il tag S3 non possono essere sovrascritti.
    - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
    - Se è attivata la versione S3, l'impostazione Nega impedisce alle operazioni PutObjectTagging o DeleteObjectTagging di modificare il TagSet per un oggetto e le relative versioni non correnti.
  - Se non viene trovato un oggetto esistente, questa autorizzazione non ha effetto.
- Quando questa autorizzazione non è presente, l'effetto è lo stesso di se Allow è stato impostato.

> Se il criterio S3 corrente consente la sovrascrittura e l'autorizzazione PutOverwriteObject è impostata su Nega, il client non può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o il tagging degli oggetti. Inoltre, se la casella di controllo **Impedisci modifica client** è selezionata (**CONFIGURAZIONE** > **Impostazioni di sicurezza** > **rete e oggetti**), tale impostazione sovrascrive l'impostazione dell'autorizzazione PutOverwriteObject.

Specificare le condizioni in un criterio

Le condizioni definiscono quando una policy sarà in vigore. Le condizioni sono costituite da operatori e coppie chiave-valore.

Le condizioni utilizzano coppie chiave-valore per la valutazione. Un elemento Condition può contenere più condizioni e ciascuna condizione può contenere più coppie chiave-valore. Il blocco Condition utilizza il seguente formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

Nell'esempio seguente, la condizione ipaddress utilizza la chiave SourceIp Condition.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operatori delle condizioni supportati

Gli operatori delle condizioni sono classificati come segue:

- Stringa
- Numerico
- Booleano
- Indirizzo IP
- Controllo nullo

Condizionare gli operatori	Descrizione
StringEquals	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole).
StringNotEquals	Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole).
StringEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora maiuscole/minuscole).
StringNotEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza negata (ignora maiuscole/minuscole).
StringLike	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole). Possono includere * e ? caratteri jolly.
StringNotLike	Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole). Possono includere * e ? caratteri jolly.
Valori numerici Equals	Confronta una chiave con un valore numerico in base alla corrispondenza esatta.
NumericNotEquals	Confronta una chiave con un valore numerico in base alla corrispondenza negata.
NumericGreaterThan	Confronta un tasto con un valore numerico basato sulla corrispondenza "maggiore di".
NumericGreaterThanEquals	Confronta una chiave con un valore numerico basato sulla corrispondenza "maggiore o uguale".
NumericLessThan	Confronta una chiave con un valore numerico basato sulla corrispondenza "minore di".

Condizionare gli operatori	Descrizione
NumericLessThanEquals	Confronta una chiave con un valore numerico basato sulla corrispondenza "minore di o uguale".
Bool	Confronta una chiave con un valore booleano basato sulla corrispondenza "true o false".
Indirizzo IP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP.
NotIpAddress	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata.
Nullo	Controlla se è presente una chiave di condizione nel contesto della richiesta corrente.

Chiavi di condizione supportate

Tasti Condition	Azioni	Descrizione
aws: SourceIp	Operatori IP	Viene confrontato con l'indirizzo IP da cui è stata inviata la richiesta. Può essere utilizzato per operazioni bucket o a oggetti. **Nota:** se la richiesta S3 è stata inviata tramite il servizio Load Balancer sui nodi Admin e Gateway, viene confrontato con l'indirizzo IP a monte del servizio Load Balancer. **Nota**: Se si utilizza un bilanciamento del carico non trasparente di terze parti, questo viene confrontato con l'indirizzo IP del bilanciamento del carico. Qualsiasi `X-Forwarded-For` l'intestazione verrà ignorata perché la sua validità non può essere accertata.
aws:nome utente	Risorsa/identità	Viene confrontato con il nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni bucket o a oggetti.
s3:delimitatore	s3:ListBucket e. s3:autorizzazioni ListBucketVersions	Verrà eseguito un confronto con il parametro delimitatore specificato in una richiesta ListObjects o ListObjectVersions.

Tasti Condition	Azioni	Descrizione
S3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging S3:PutObjectAcl s3:PutObjectTagging S3:PutObjectVersionAcl s3:PutObjectVersionTagging	Richiede che l'oggetto esistente abbia la chiave e il valore tag specifici.
s3: tasti max	s3:ListBucket e. s3:autorizzazioni ListBucketVersions	Verrà eseguito un confronto con il parametro max-keys specificato in una richiesta ListObjects o ListObjectVersions.
s3:giorni-rimanenti-conservazione-blocco-oggetto	s3:PutObject	Viene confrontato con la data di conservazione specificata in `x-amz-object-lock-retain-until-date` intestazione della richiesta o calcolata dal periodo di conservazione predefinito del bucket per assicurarsi che questi valori rientrino nell'intervallo consentito per le seguenti richieste: • PutObject • Oggetto CopyObject • CreateMultipartUpload
s3:giorni-rimanenti-conservazione-blocco-oggetto	s3:PutObjectRetention	Viene confrontato con la data di scadenza specificata nella richiesta PutObjectRetention per garantire che rientri nell'intervallo consentito.

Tasti Condition	Azioni	Descrizione
s3:prefisso	s3:ListBucket e. s3:autorizzazioni ListBucketVersions	Verrà eseguito un confronto con il parametro prefix specificato in una richiesta ListObjects o ListObjectVersions.
S3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Richiede una chiave e un valore tag specifici quando la richiesta dell'oggetto include il tagging.

Specificare le variabili in un criterio

È possibile utilizzare le variabili nei criteri per popolare le informazioni sui criteri quando sono disponibili. È possibile utilizzare le variabili dei criteri in `Resource` confronto tra elementi e stringhe in `Condition` elemento.

In questo esempio, la variabile `${aws:username}` Fa parte dell'elemento Resource:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In questo esempio, la variabile `${aws:username}` fa parte del valore della condizione nel blocco condition:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variabile	Descrizione
`${aws:SourceIp}`	Utilizza la chiave SourceIp come variabile fornita.
`${aws:username}`	Utilizza la chiave Username come variabile fornita.
`${s3:prefix}`	Utilizza la chiave di prefisso specifica del servizio come variabile fornita.
`${s3:max-keys}`	Utilizza la chiave max-keys specifica del servizio come variabile fornita.
`${*}`	Carattere speciale. Utilizza il carattere come carattere * letterale.

Variabile	Descrizione
`${?}`	Carattere speciale. Utilizza il carattere come letterale ? carattere.
`${$}`	Carattere speciale. Utilizza il carattere come carattere letterale.

Creare policy che richiedono una gestione speciale

A volte un criterio può concedere autorizzazioni pericolose per la sicurezza o pericolose per operazioni continue, come il blocco dell'utente root dell'account. L'implementazione dell'API REST di StorageGRID S3 è meno restrittiva durante la convalida delle policy rispetto ad Amazon, ma altrettanto rigorosa durante la valutazione delle policy.

Descrizione della policy	Tipo di policy	Comportamento di Amazon	Comportamento di StorageGRID
Negare automaticamente le autorizzazioni all'account root	Bucket	Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del bucket S3	Stesso
Negare automaticamente le autorizzazioni all'utente/gruppo	Gruppo	Valido e applicato	Stesso
Consenti a un gruppo di account esterno qualsiasi autorizzazione	Bucket	Principal non valido	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio
Consentire a un account root esterno o a un utente qualsiasi autorizzazione	Bucket	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio	Stesso
Consenti a tutti i permessi per tutte le azioni	Bucket	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) per l'account root esterno e gli utenti	Stesso

Descrizione della policy	Tipo di policy	Comportamento di Amazon	Comportamento di StorageGRID
Negare a Everyone le autorizzazioni per tutte le azioni	Bucket	Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del bucket S3	Stesso
Principal è un utente o un gruppo inesistente	Bucket	Principal non valido	Valido
La risorsa è un bucket S3 inesistente	Gruppo	Valido	Stesso
Principal è un gruppo locale	Bucket	Principal non valido	Valido
Il criterio concede a un account non proprietario (inclusi gli account anonimi) le autorizzazioni per l'inserimento degli oggetti.	Bucket	Valido. Gli oggetti sono di proprietà dell'account creatore e la policy bucket non si applica. L'account creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL a oggetti.	Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la policy bucket.

Protezione WORM (Write-Once-Read-Many)

È possibile creare bucket WORM (write-once-Read-many) per proteggere i dati, i metadati degli oggetti definiti dall'utente e il tagging degli oggetti S3. I bucket WORM vengono configurati in modo da consentire la creazione di nuovi oggetti e impedire la sovrascrittura o l'eliminazione del contenuto esistente. Utilizzare uno degli approcci descritti di seguito.

Per garantire che le sovrascritture vengano sempre negate, è possibile:

- Da Grid Manager, selezionare **CONFIGURATION** > **Security** > **Security settings** > **Network and Objects**, quindi selezionare la casella di controllo **Impedisci modifica client**.
- Applicare le seguenti regole e criteri S3:
  - Aggiungere un'operazione di NEGAZIONE PutOverwriteObject al criterio S3.
  - Aggiungere un'operazione di NEGAZIONE DeleteObject al criterio S3.
  - Aggiungere un'operazione PutObject ALLOW al criterio S3.

> L'impostazione di DeleteObject su NEGA in un criterio S3 non impedisce a ILM di eliminare oggetti quando esiste una regola come "zero copie dopo 30 giorni".

> Anche quando tutte queste regole e policy vengono applicate, non si proteggono dalle scritture simultanee (vedi situazione A). Si proteggono dalle sovrascritture sequenziali completate (vedere situazione B).

Situazione A: Scritture simultanee (non protette)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situazione B: Sovrascritture sequenziali completate (con protezione)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informazioni correlate

- "Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID"
- "Esempio di policy bucket"
- "Criteri di gruppo di esempio"
- "Gestire gli oggetti con ILM"
- "Utilizzare un account tenant"

Esempio di policy bucket

Utilizza gli esempi di questa sezione per creare policy di accesso StorageGRID per i bucket.

I criteri del bucket specificano le autorizzazioni di accesso per il bucket a cui è associata la policy. I criteri del bucket vengono configurati utilizzando l'API S3 PutBucketPolicy. Vedere "Operazioni sui bucket".

È possibile configurare un criterio bucket utilizzando l'interfaccia CLI AWS seguendo il seguente comando:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Esempio: Consentire a tutti l'accesso in sola lettura a un bucket

In questo esempio, a tutti, incluso anonimo, è consentito elencare gli oggetti nel bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket. Tutte le altre operazioni verranno negate. Si noti che questo criterio potrebbe non essere particolarmente utile perché nessuno, ad eccezione dell'account root, dispone delle autorizzazioni di scrittura nel bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Esempio: Consentire a tutti gli utenti di un account l'accesso completo e a tutti gli utenti di un altro account l'accesso in sola lettura a un bucket

In questo esempio, a tutti gli utenti di un account specificato è consentito l'accesso completo a un bucket, mentre a tutti gli utenti di un altro account specificato è consentito solo elencare il bucket ed eseguire operazioni GetObject sugli oggetti nel bucket che iniziano con `shared/` prefisso chiave oggetto.

> In StorageGRID, gli oggetti creati da un account non proprietario (inclusi gli account anonimi) sono di proprietà dell'account proprietario del bucket. La policy bucket si applica a questi oggetti.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Esempio: Consentire a tutti l'accesso in sola lettura a un bucket e l'accesso completo per gruppo specificato

In questo esempio, a tutti, incluso anonimo, è consentito elencare il bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket, mentre solo gli utenti appartengono al gruppo `Marketing` nell'account specificato è consentito l'accesso completo.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Esempio: Consentire a tutti l'accesso in lettura e scrittura a un bucket se il client si trova nell'intervallo IP

In questo esempio, Everyone, incluso l'anonimato, è autorizzato a elencare il bucket ed eseguire qualsiasi operazione oggetto su tutti gli oggetti nel bucket, a condizione che le richieste provengano da un intervallo IP specificato (da 54.240.143.0 a 54.240.143.255, eccetto 54.240.143.188). Tutte le altre operazioni verranno rifiutate e tutte le richieste al di fuori dell'intervallo IP verranno rifiutate.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Esempio: Consentire l'accesso completo a un bucket esclusivamente da un utente federato specificato

In questo esempio, all'utente federato Alex è consentito l'accesso completo a `examplebucket` bucket e i suoi oggetti. A tutti gli altri utenti, tra cui 'root', vengono esplicitamente negate tutte le operazioni. Si noti tuttavia che a 'root' non vengono mai negate le autorizzazioni per put/get/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Esempio: Autorizzazione PutOverwriteObject

In questo esempio, il `Deny` Effect per PutOverwriteObject e DeleteObject garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e il tagging degli oggetti S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Criteri di gruppo di esempio

Utilizzare gli esempi di questa sezione per creare criteri di accesso StorageGRID per i gruppi.

I criteri di gruppo specificano le autorizzazioni di accesso per il gruppo a cui è associato il criterio. Non c'è `Principal` elemento nel criterio perché è implicito. I criteri di gruppo vengono configurati utilizzando il tenant Manager o l'API.

Esempio: Impostare i criteri di gruppo utilizzando Tenant Manager

Quando si aggiunge o si modifica un gruppo in Tenant Manager, è possibile selezionare una policy di gruppo per determinare quali autorizzazioni di accesso S3 avranno i membri di questo gruppo. Vedere "Creare gruppi per un tenant S3".

- **Nessun accesso S3**: Opzione predefinita. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non sia concesso con una policy bucket. Se si seleziona questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
- **Accesso di sola lettura**: Gli utenti di questo gruppo hanno accesso di sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile modificare questa stringa.
- **Accesso completo**: Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo ad accesso completo. Impossibile modificare questa stringa.
- **Ransomware Mitigation**: Questa policy di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti.

  Gli utenti di tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono eseguire l'override di questa policy di gruppo. Limitare l'autorizzazione Manage All bucket (Gestisci tutti i bucket) agli utenti attendibili e utilizzare l'autenticazione multifattore (MFA), se disponibile.

- **Personalizzato**: Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

Esempio: Consentire l'accesso completo del gruppo a tutti i bucket

In questo esempio, a tutti i membri del gruppo è consentito l'accesso completo a tutti i bucket di proprietà dell'account tenant, a meno che non sia esplicitamente negato dalla policy bucket.

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

Esempio: Consentire l'accesso di gruppo in sola lettura a tutti i bucket

In questo esempio, tutti i membri del gruppo hanno accesso in sola lettura alle risorse S3, a meno che non sia esplicitamente negato dalla policy del bucket. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Esempio: Consenti ai membri del gruppo di accedere completamente solo alla loro "cartella" in un bucket

In questo esempio, i membri del gruppo possono solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato. Tenere presente che le autorizzazioni di accesso da altre policy di gruppo e la policy del bucket devono essere prese in considerazione quando si determina la privacy di queste cartelle.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Operazioni S3 registrate nei registri di audit

I messaggi di audit vengono generati dai servizi StorageGRID e memorizzati in file di log di testo. È possibile rivedere i messaggi di audit specifici per S3 nel registro di audit per ottenere dettagli sulle operazioni di bucket e oggetti.

Operazioni bucket registrate nei registri di audit

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- HeadBucket
- ListObjects (oggetti elenco)
- ListObjectVersions
- METTI la compliance del bucket
- PutBucketTagging
- PutBucketVersioning

Operazioni a oggetti registrate nei registri di audit

- CompleteMultipartUpload
- Oggetto CopyObject
- DeleteObject (Elimina oggetto)
- GetObject
- HeadObject (oggetto intestazione)
- PutObject
- RestoreObject
- SelectObject (oggetto)
- UploadPart (quando una regola ILM utilizza un'acquisizione bilanciata o rigorosa)
- UploadPartCopy (quando una regola ILM utilizza l'acquisizione bilanciata o rigorosa)

Informazioni correlate

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

USA API REST di Swift (obsoleto)

USA Swift REST API: Panoramica

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

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

StorageGRID supporta le seguenti versioni specifiche di Swift e HTTP.

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

Informazioni correlate

"OpenStack: API dello storage a oggetti"

Cronologia del supporto delle API Swift in StorageGRID

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

Rilasciare	Commenti
11,8	
11,7	Il supporto per le applicazioni client Swift è stato obsoleto e verrà rimosso in una release futura.
11,6	Modifiche editoriali minori.
11,5	Eliminata la debole consistenza. Verrà invece utilizzata la coerenza disponibile.
11,4	Aggiunto supporto per TLS 1.3. Aggiunta descrizione dell'interrelazione tra ILM e coerenza.
11,3	Aggiornate le operazioni PUT object per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono all'acquisizione (le opzioni bilanciate e rigide per il comportamento di Ingest). Aggiunta descrizione delle connessioni client che utilizzano endpoint di bilanciamento del carico o gruppi ad alta disponibilità. Le crittografia TLS 1.1 non sono più supportate.
11,2	Modifiche editoriali minori al documento.
11,1	Aggiunto supporto per l'utilizzo di HTTP per connessioni client Swift ai nodi grid. Aggiornate le definizioni dei valori di coerenza.
11,0	Aggiunto supporto per 1,000 container per ciascun account tenant.
10,3	Aggiornamenti amministrativi e correzioni del documento. Rimosse le sezioni per la configurazione dei certificati server personalizzati.
10,2	Supporto iniziale dell'API Swift da parte del sistema StorageGRID. La versione attualmente supportata è OpenStack Swift Object Storage API v1.

Come StorageGRID implementa l'API di Swift REST

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

Gestione rapida degli oggetti

Una volta acquisiti gli oggetti Swift nel sistema StorageGRID, questi vengono gestiti dalle regole ILM

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

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

Richieste client in conflitto

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

Garanzie e controlli di coerenza

Per impostazione predefinita, StorageGRID fornisce coerenza di lettura dopo scrittura per gli oggetti appena creati ed eventuale coerenza per gli aggiornamenti degli oggetti e le operazioni HEAD. Qualsiasi "OTTIENI" a seguito di un completamento riuscito "IN PRIMO PIANO" sarà in grado di leggere i dati appena scritti. Le sovrascritture degli oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni sono coerenti. Le sovrascritture in genere richiedono secondi o minuti per la propagazione, ma possono richiedere fino a 15 giorni.

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

Raccomandazioni per l'implementazione di Swift REST API

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

Raccomandazioni per la gestione di oggetti inesistenti

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

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

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

Raccomandazioni per i nomi degli oggetti

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

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

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

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

Invece di questo formato:

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

Raccomandazioni per "letture di gamma"

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

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

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

Verifica della configurazione delle API REST Swift

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

Prima di iniziare

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

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

A proposito di questa attività

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

questi comandi.

Fasi

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

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

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

2. Inserire un oggetto nel contenitore:

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

3. Ottenere il container per verificare l'oggetto:

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

4. Eliminare l'oggetto:

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

5. Eliminare il contenitore:

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

Operazioni supportate da Swift REST API

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

Operazioni supportate in StorageGRID

Sono supportate le seguenti operazioni API Swift:

- "Operazioni dell'account"
- "Operazioni container"
- "Operazioni a oggetti"

Intestazioni di risposta comuni per tutte le operazioni

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

Informazioni correlate

"OpenStack: API dello storage a oggetti"

Endpoint API Swift supportati

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

URL info

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

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

Nella richiesta:

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

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

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

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

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

URL di autenticazione

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

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

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

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

X-Auth-Key: Password
```

Nelle intestazioni della richiesta:

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

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

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

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

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

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

X-Auth-Token: token

X-Storage-Token: token
```

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

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

URL dello storage

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

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

[/container][/object]

X-Auth-Token: token
```

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

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

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

Informazioni correlate

"Configurare gli account e le connessioni del tenant"

"Operazioni dell'account"

"Operazioni container"

"Operazioni a oggetti"

Operazioni dell'account

Le seguenti operazioni API Swift vengono eseguite sugli account.

OTTIENI un account

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

È necessario il seguente parametro di richiesta:

- `Account`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

I seguenti parametri di query di richiesta supportati sono facoltativi:

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

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

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

Conto PRINCIPALE

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

È necessario il seguente parametro di richiesta:

- `Account`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

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

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

- `X-Trans-Id`

Informazioni correlate

"Operazioni rapide monitorate nei registri di audit"

Operazioni container

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

ELIMINA contenitore

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

Sono richiesti i seguenti parametri di richiesta:

- `Account`
- `Container`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

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

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

OTTIENI container

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

Sono richiesti i seguenti parametri di richiesta:

- `Account`
- `Container`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

I seguenti parametri di query di richiesta supportati sono facoltativi:

- `Delimiter`
- `End_marker`
- `Format`

- `Limit`
- `Marker`
- `Path`
- `Prefix`

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

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

CONTENITORE DI TESTA

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

Sono richiesti i seguenti parametri di richiesta:

- `Account`
- `Container`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

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

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

METTI container

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

Sono richiesti i seguenti parametri di richiesta:

- `Account`
- `Container`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

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

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

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

Informazioni correlate

"Monitorare e controllare le operazioni"

Operazioni a oggetti

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

ELIMINA oggetto

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

Sono richiesti i seguenti parametri di richiesta:

- `Account`
- `Container`
- `Object`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

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

- `Content-Length`
- `Content-Type`
- `Date`

- `X-Trans-Id`

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

Per ulteriori informazioni, vedere "Modalità di eliminazione degli oggetti".

OTTIENI oggetto

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

Sono richiesti i seguenti parametri di richiesta:

- `Account`
- `Container`
- `Object`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

Le seguenti intestazioni di richiesta sono opzionali:

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

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

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

- `X-Trans-Id`

Oggetto TESTA

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

Sono richiesti i seguenti parametri di richiesta:

- `Account`
- `Container`
- `Object`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

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

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

METTI oggetto

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

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

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

Sono richiesti i seguenti parametri di richiesta:

- `Account`
- `Container`
- `Object`

È richiesta la seguente intestazione di richiesta:

- `X-Auth-Token`

Le seguenti intestazioni di richiesta sono opzionali:

- `Content-Disposition`
- `Content-Encoding`

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

- `Transfer-Encoding`

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

- `Content-Length`

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

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

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

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

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

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

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

- `X-Storage-Class: reduced_redundancy`

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

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

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

  Utilizzando il `reduced_redundancy` l'intestazione non è consigliata in altre circostanze perché aumenta il rischio di perdita dei dati dell'oggetto durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.

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

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

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

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

Richiesta DI OPZIONI

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

Metodo DI OPZIONI

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

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

È necessario il seguente parametro di richiesta:

- `Account`

I seguenti parametri di richiesta sono facoltativi:

- `Container`
- `Object`

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1,1 204 Nessun contenuto". Le OPZIONI richieste all'URL di storage non richiedono l'esistenza della destinazione.

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

Informazioni correlate

"Endpoint API Swift supportati"

Risposte agli errori alle operazioni API di Swift

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

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

Nome errore Swift	Stato HTTP
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadataValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadataTooLarge	400 richiesta errata
Accesso negato	403 proibita
ContainerNotEmpty, ContainerAlreadyExists	409 conflitto
InternalError	500 errore interno del server
InvalidRange	416 intervallo richiesto non riscontrabile

Nome errore Swift	Stato HTTP
MethodNon consentito	405 metodo non consentito
MissingContentLength	411 lunghezza richiesta
Non trovato	404 non trovato
Non soddisfatto	501 non implementato
PrecondizioneFailed	412 precondizione non riuscita
ResourceNotFound	404 non trovato
Non autorizzato	401 non autorizzato
UnprocessableEntity	422 entità non elaborabile

Operazioni API Swift REST di StorageGRID

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

OTTENERE una richiesta di coerenza dei container

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

Richiesta

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

Esempio di richiesta

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

Risposta

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

Esempio di risposta

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

INVIO di una richiesta di coerenza del container

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

Richiesta

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

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

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

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

Esempio di interazione tra le regole di coerenza e ILM

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

- **ILM rule**: Creare due copie di oggetti, una nel sito locale e una in un sito remoto. Viene selezionato il comportamento rigoroso dell'acquisizione.

- **: "Strong-Global" (i metadati degli oggetti vengono immediatamente distribuiti a tutti i siti).

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

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

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

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

Esempio di richiesta

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

Risposta

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

Esempio di risposta

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

Operazioni rapide monitorate nei registri di audit

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

Operazioni dell'account

- "OTTIENI un account"
- "Conto PRINCIPALE"

Operazioni container

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

Operazioni a oggetti

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

Informazioni correlate

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

Monitorare e risolvere i problemi di un sistema StorageGRID

Monitorare il sistema StorageGRID

Monitorare un sistema StorageGRID: Panoramica

Monitorare regolarmente il sistema StorageGRID per assicurarsi che funzioni come previsto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

> Per modificare le unità per i valori di storage visualizzati in Grid Manager, selezionare il menu a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User preferences** (Preferenze utente).

A proposito di questa attività

Queste istruzioni descrivono come:

- "Visualizzare e gestire la dashboard"
- "Visualizzare la pagina nodi"
- "Monitorare regolarmente questi aspetti del sistema:"
  - "Stato del sistema"
  - "Capacità dello storage"
  - "Gestione del ciclo di vita delle informazioni"
  - "Risorse di rete e di sistema"
  - "Attività del tenant"
  - "Operazioni di bilanciamento del carico"
  - "Connessioni a federazione di griglie"
  - "Capacità di archiviazione"
- "Gestire gli avvisi e gli allarmi legacy"
- "Visualizzare i file di registro"
- "Configurare i messaggi di audit e le destinazioni dei log"
- "Utilizzare un server syslog esterno" per raccogliere le informazioni di controllo
- "Utilizzare SNMP per il monitoraggio"
- "Ottenere ulteriori dati StorageGRID", comprese le metriche e la diagnostica

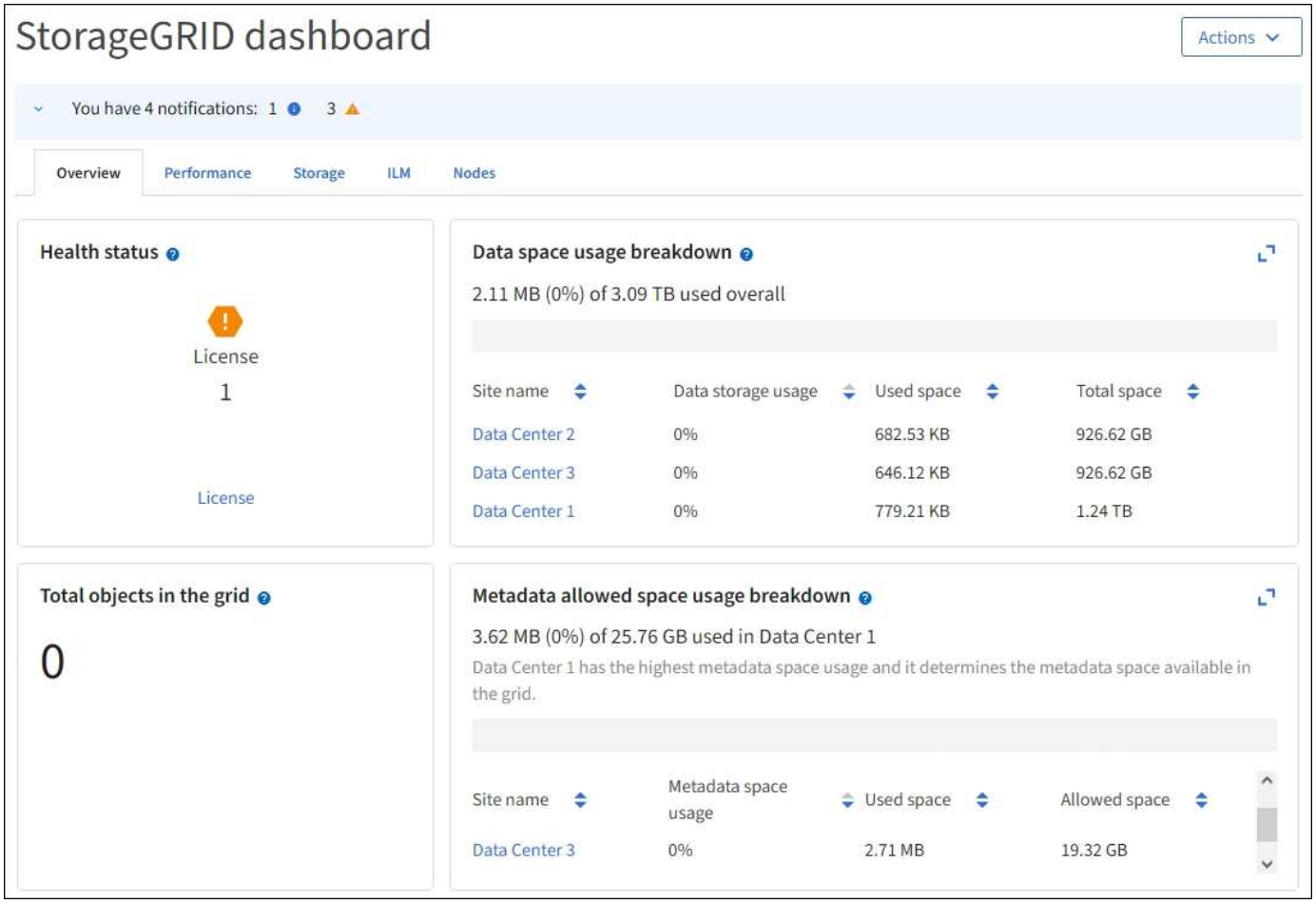
Visualizzare e gestire la dashboard

È possibile utilizzare la dashboard per monitorare le attività del sistema in un colpo

d’occhio. È possibile creare dashboard personalizzati per monitorare l’implementazione di StorageGRID.

Per modificare le unità per i valori di storage visualizzati in Grid Manager, selezionare il menu a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User preferences** (Preferenze utente).

Il dashboard potrebbe essere diverso a seconda della configurazione del sistema.



Visualizza la dashboard

La dashboard è costituita da schede che contengono informazioni specifiche sul sistema StorageGRID. Ciascuna scheda contiene le categorie di informazioni visualizzate sulle schede.

È possibile utilizzare la dashboard fornita con il sistema così com’è. Inoltre, è possibile creare dashboard personalizzati contenenti solo schede e schede rilevanti per il monitoraggio dell’implementazione di StorageGRID.

Le schede della dashboard fornite dal sistema contengono schede con i seguenti tipi di informazioni:

Scheda sulla dashboard fornita dal sistema	Contiene
Panoramica	Informazioni generali sulla griglia, ad esempio avvisi attivi, utilizzo dello spazio e oggetti totali nella griglia.

Scheda sulla dashboard fornita dal sistema	Contiene
Performance	Utilizzo dello spazio, storage utilizzato nel tempo, operazioni S3 o Swift, durata della richiesta, tasso di errore.
Storage	Utilizzo delle quote dei tenant e dello spazio logico. Previsioni di utilizzo dello spazio per i dati e i metadati dell'utente.
ILM	Coda di gestione del ciclo di vita delle informazioni e tasso di valutazione.
Nodi	Utilizzo di CPU, dati e memoria per nodo. Operazioni S3 o Swift per nodo. Distribuzione da nodo a sito.

Alcune schede possono essere massimizzate per una visualizzazione più semplice. Selezionare l'icona Ingrandisci nell'angolo superiore destro della scheda. Per chiudere una scheda ingrandita, selezionare l'icona Riduci a icona Oppure selezionare **Chiudi**.

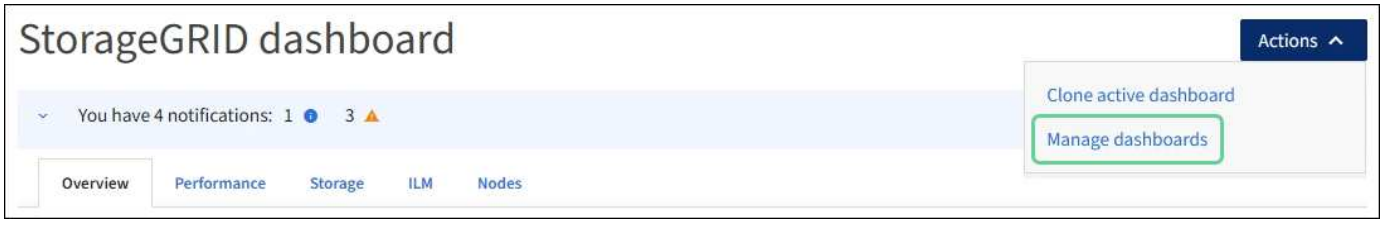
Gestire i dashboard

Se si dispone dell'accesso root (vedere "Autorizzazioni del gruppo di amministrazione"), è possibile eseguire le seguenti attività di gestione per i dashboard:

- Crea una dashboard personalizzata da zero. È possibile utilizzare dashboard personalizzati per controllare quali informazioni StorageGRID vengono visualizzate e come sono organizzate.
- Clonare una dashboard per creare dashboard personalizzati.
- Impostare una dashboard attiva per un utente. La dashboard attiva può essere la dashboard fornita dal sistema o una dashboard personalizzata.
- Impostare una dashboard predefinita, che è quella visualizzata da tutti gli utenti, a meno che non attivino la propria dashboard.
- Modificare il nome di una dashboard.
- Modificare una dashboard per aggiungere o rimuovere schede e schede. È possibile avere un minimo di 1 e un massimo di 20 schede.
- Rimuovere una dashboard.

Se si dispone di altre autorizzazioni oltre all'accesso root, è possibile impostare solo una dashboard attiva.

Per gestire i dashboard, selezionare **azioni** > **Gestisci dashboard**.



Configurare i dashboard

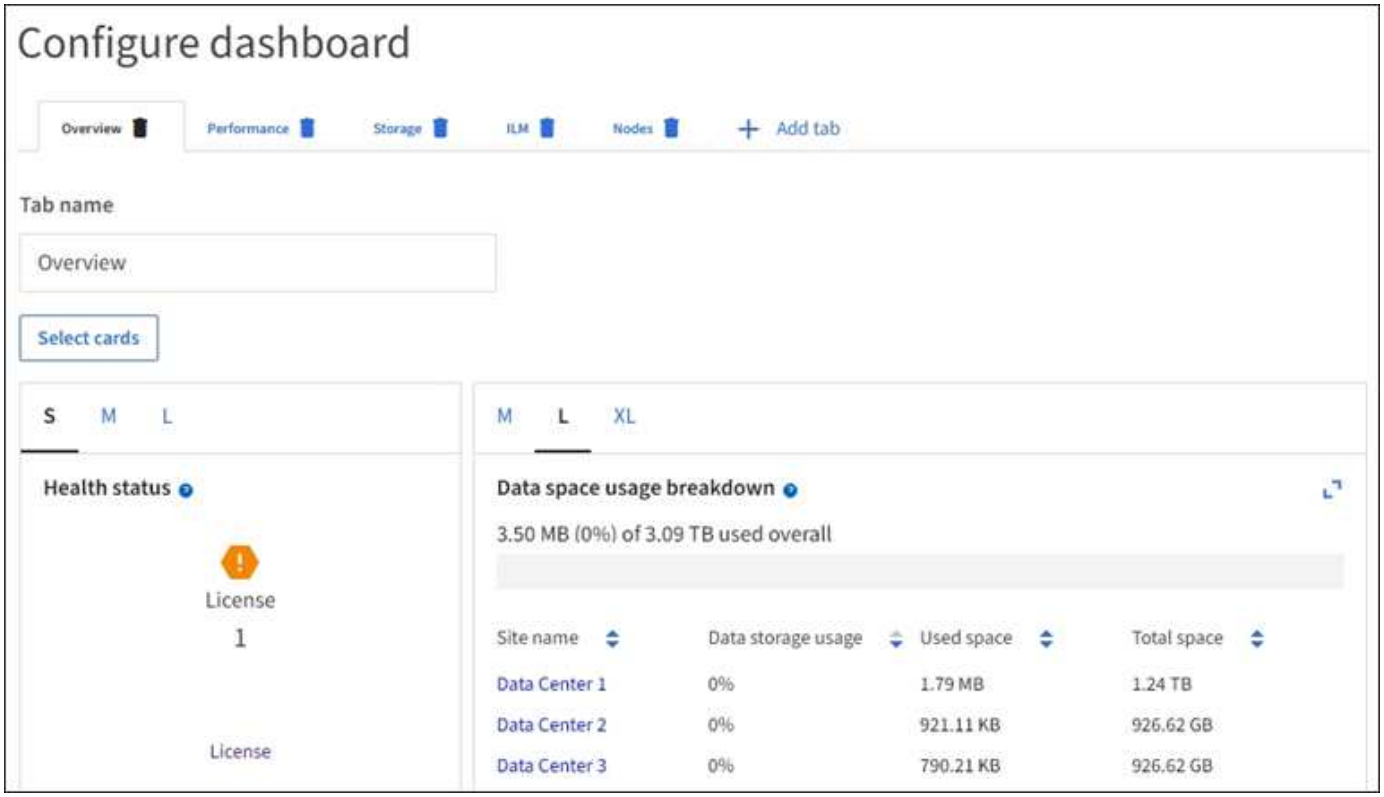
Per creare una nuova dashboard clonando la dashboard attiva, selezionare **azioni** > **Clona dashboard attiva**.

Per modificare o clonare una dashboard esistente, selezionare **azioni** > **Gestisci dashboard**.

La dashboard fornita dal sistema non può essere modificata o rimossa.

Durante la configurazione di una dashboard, è possibile:

- Aggiungere o rimuovere le schede
- Rinominare le schede e assegnarle nomi univoci
- Aggiungere, rimuovere o riorganizzare (trascinare) le schede per ciascuna scheda
- Selezionare le dimensioni delle singole schede selezionando **S**, **M**, **L** o **XL** nella parte superiore della scheda



Visualizzare la pagina nodi

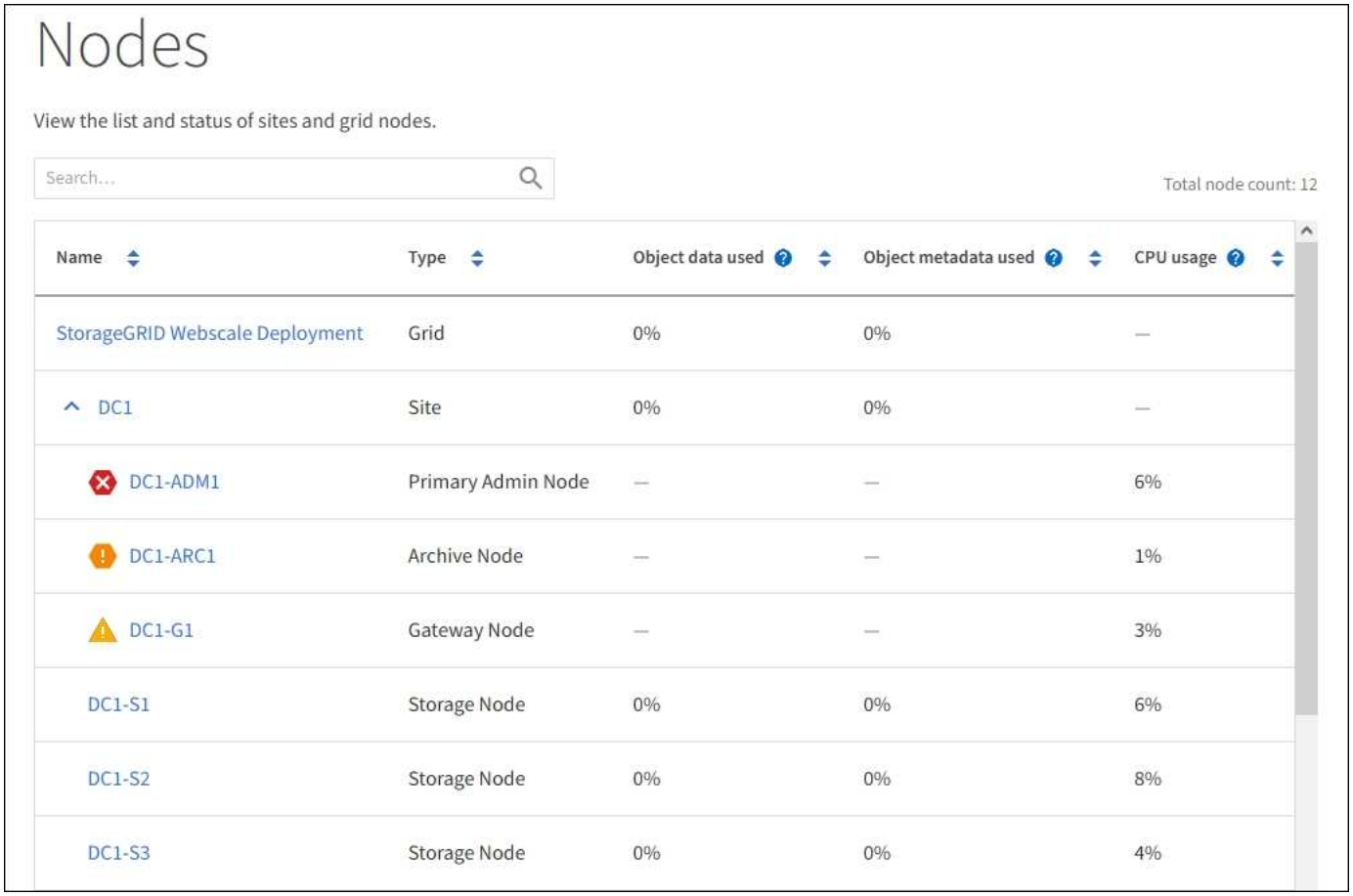
Visualizza la pagina nodi: Panoramica

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.

La tabella Nodes (nodi) elenca informazioni riepilogative per l'intera griglia, ciascun sito e ciascun nodo. Se un nodo è disconnesso o presenta 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.

Quando un nodo non è connesso alla griglia, ad esempio durante l'aggiornamento o uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della griglia. Dopo che un nodo si ricollega alla griglia, attendere alcuni minuti per consentire la stabilizzazione dei valori.

Per modificare le unità per i valori di storage visualizzati in Grid Manager, selezionare il menu a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User preferences** (Preferenze utente).



Icone di stato della connessione

Se un nodo viene disconnesso dalla griglia, accanto al nome del nodo viene visualizzata una delle seguenti icone.

Icona	Descrizione	Azione richiesta
	Non connesso - Sconosciuto Per un motivo sconosciuto, un nodo viene disconnesso o i servizi sul nodo vengono inaspettatamente disattivi. Ad esempio, un servizio sul nodo potrebbe essere stato arrestato o il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione dell'alimentazione o di un'interruzione imprevista. Potrebbe essere attivato anche l'avviso **Impossibile comunicare con il nodo**. Potrebbero essere attivi anche altri avvisi.	Richiede un'attenzione immediata. "Selezionare ciascun avviso" e seguire le azioni consigliate. Ad esempio, potrebbe essere necessario riavviare un servizio che ha arrestato o riavviato l'host per il nodo. **Nota**: 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 Per un motivo previsto, il nodo non è connesso alla rete. 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. In base al problema sottostante, questi nodi tornano spesso online senza alcun intervento.	Determinare se eventuali avvisi influiscono su questo nodo. Se sono attivi uno o più avvisi, "Selezionare ciascun avviso" e seguire le azioni consigliate.

Se un nodo è disconnesso dalla griglia, potrebbe essere presente 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.

Major: 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 esiste una condizione anomala che potrebbe influire sulla capacità di funzionamento del sistema se continua. È necessario monitorare e risolvere gli avvisi minori che non vengono risolti da soli per garantire che non causino problemi più gravi.

Visualizza i dettagli di un sistema, sito o nodo

Per filtrare le informazioni visualizzate nella tabella Nodes (nodi), inserire una stringa di ricerca nel campo **Search** (Ricerca). È possibile eseguire una ricerca in base al nome del sistema, al nome visualizzato o al tipo (ad esempio, immettere **gat** per individuare rapidamente tutti i nodi gateway).

Per visualizzare le informazioni relative a griglia, sito o nodo:

- Selezionare il nome della griglia per visualizzare un riepilogo aggregato delle statistiche per l'intero sistema 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.

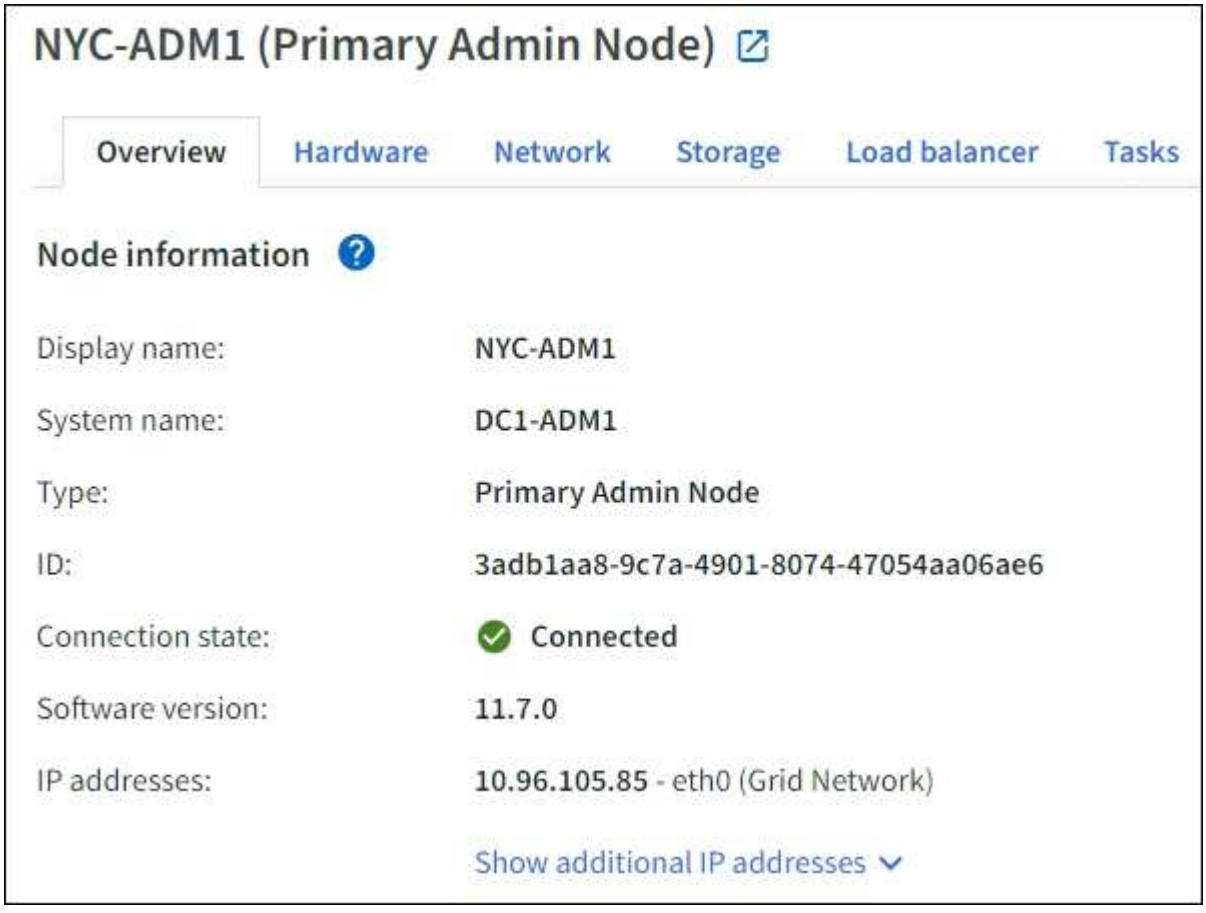
Visualizzare la scheda Panoramica

La scheda Panoramica fornisce informazioni di base su ciascun nodo. Inoltre, vengono visualizzati tutti gli avvisi che attualmente influiscono sul nodo.

Viene visualizzata la scheda Overview (Panoramica) per tutti i nodi.

Informazioni sul nodo

La sezione Node Information (informazioni nodo) della scheda Overview (Panoramica) elenca le informazioni di base sul nodo.



Le informazioni generali per un nodo includono quanto segue:

- **Nome visualizzato** (visualizzato solo se il nodo è stato rinominato): Il nome visualizzato corrente per il nodo. Utilizzare "Rinominare la griglia, i siti e i nodi" procedura per aggiornare questo valore.
- **Nome sistema**: Il nome immesso per il nodo durante l'installazione. I nomi di sistema vengono utilizzati per le operazioni StorageGRID interne e non possono essere modificati.
- **Type**: Il tipo di nodo — Admin Node, Primary Admin Node, Storage Node, Gateway Node o Archive Node.

> Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura. Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità.

- **ID**: Identificatore univoco del nodo, chiamato anche UUID.
- **Stato connessione**: Uno dei tre stati. Viene visualizzata l'icona dello stato più grave.
  - **Sconosciuto**: Per un motivo sconosciuto, il nodo non è connesso alla rete o uno o più servizi sono inaspettatamente fuori servizio. Ad esempio, la connessione di rete tra i nodi è stata persa, l'alimentazione è inattiva o un servizio è inattivo. 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).

  - **Amministrativamente inattivo**: 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.
  - **Connesso**: Il nodo è collegato alla rete.
- **Storage utilizzato**: Solo per nodi di storage.
  - **Dati oggetto**: Percentuale dello spazio utilizzabile totale per i dati oggetto che è stato utilizzato nel nodo di storage.
  - **Metadati oggetto**: Percentuale dello spazio totale consentito per i metadati oggetto utilizzati nel nodo di storage.
- **Versione software**: La versione di StorageGRID installata sul nodo.
- **Gruppi ha**: Solo per nodi Admin Node e Gateway. Viene visualizzato se un'interfaccia di rete sul nodo è inclusa in un gruppo ad alta disponibilità e se tale interfaccia è l'interfaccia primaria.
- **Indirizzi IP**: Gli indirizzi IP del nodo. Fare clic su **Show additional IP addresses** (Mostra indirizzi IP aggiuntivi) per visualizzare gli indirizzi IPv4 e IPv6 e le mappature dell'interfaccia del nodo.

Avvisi

La sezione Avvisi della scheda Panoramica elenca qualsiasi "avvisi che attualmente interessano questo nodo e che non sono stati tacitati". Selezionare il nome dell'avviso per visualizzare ulteriori dettagli e le azioni consigliate.

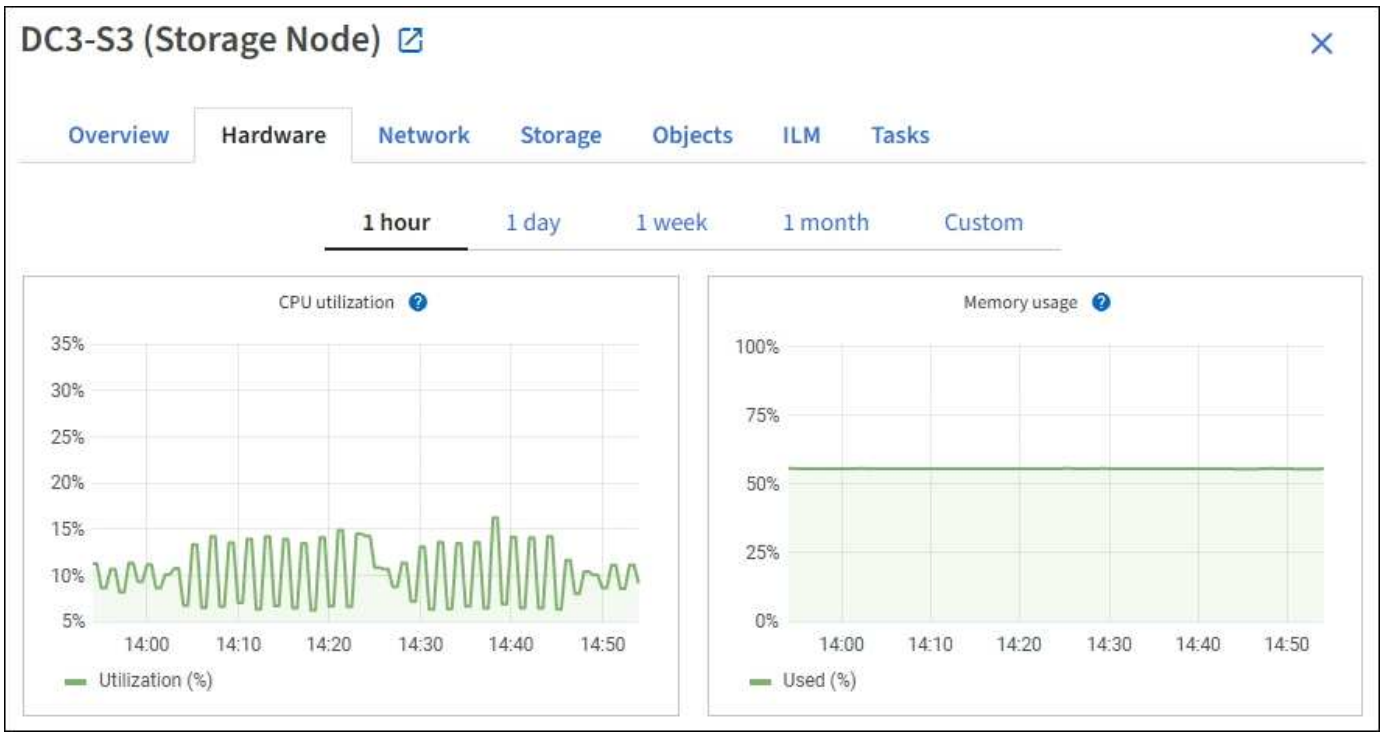
Sono inclusi anche gli avvisi per "stati di connessione del nodo".

Visualizzare la scheda hardware

La scheda hardware visualizza l'utilizzo della CPU e della memoria per ciascun nodo, oltre a informazioni aggiuntive sull'hardware delle appliance.

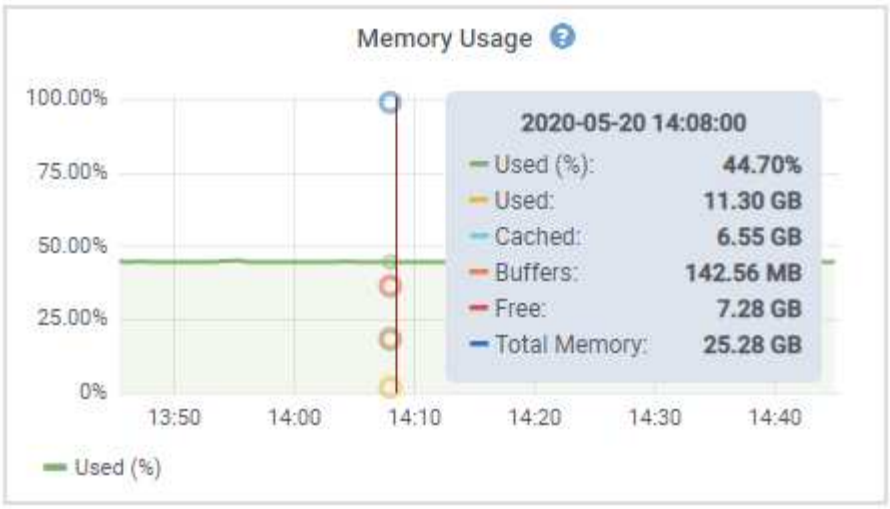
> Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere alle schermate di esempio di questa pagina.

Viene visualizzata la scheda hardware per tutti i nodi.



Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.

Per visualizzare i dettagli relativi all'utilizzo della CPU e della memoria, posizionare il cursore su ciascun grafico.



Se il nodo è un nodo appliance, questa scheda include anche una sezione con ulteriori informazioni sull'hardware dell'appliance.

Visualizza informazioni sui nodi di storage dell'appliance

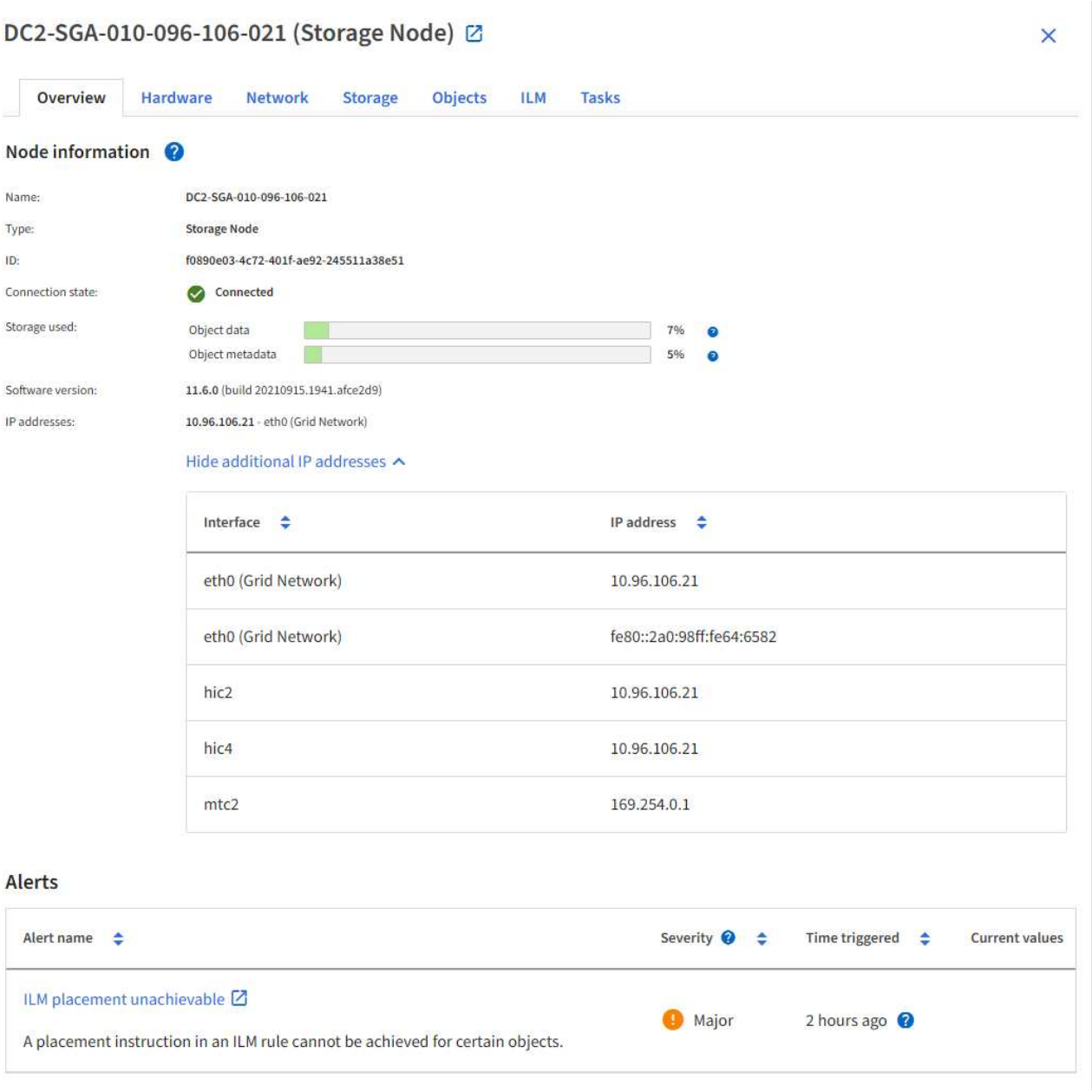
La pagina Nodes (nodi) elenca le informazioni sullo stato di salute del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ciascun nodo di storage dell'appliance. È inoltre possibile visualizzare memoria, hardware di storage, versione del firmware del controller, risorse di rete, interfacce di rete, indirizzi di rete e ricevere e trasmettere dati.

Fasi

1. Dalla pagina Nodes (nodi), selezionare un nodo di storage dell'appliance.
2. Selezionare **Panoramica**.

   La sezione Node information (informazioni nodo) della scheda Overview (Panoramica) visualizza informazioni riepilogative per il nodo, ad esempio il nome, il tipo, l'ID e lo stato di connessione del nodo. L'elenco degli indirizzi IP include il nome dell'interfaccia per ciascun indirizzo, come segue:

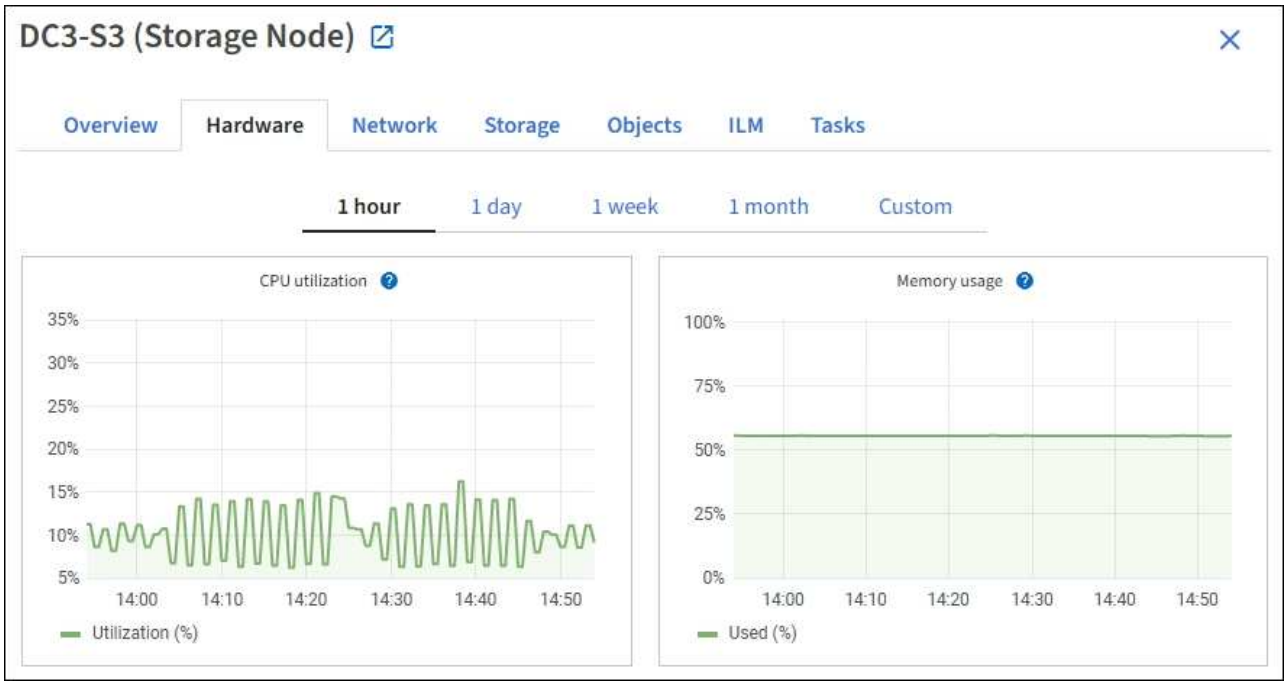
   - **eth**: Rete griglia, rete amministrativa o rete client.
   - **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate alla rete griglia StorageGRID (eth0) e alla rete client (eth2).
   - **mtc**: Una delle porte 1 GbE fisiche dell'appliance. Una o più interfacce mtc sono collegate per formare l'interfaccia di rete amministrativa StorageGRID (eth1). È possibile lasciare altre interfacce mtc disponibili per la connettività locale temporanea per un tecnico del data center.



La sezione Avvisi della scheda Panoramica visualizza gli avvisi attivi per il nodo.

3. Selezionare **hardware** per visualizzare ulteriori informazioni sull'appliance.

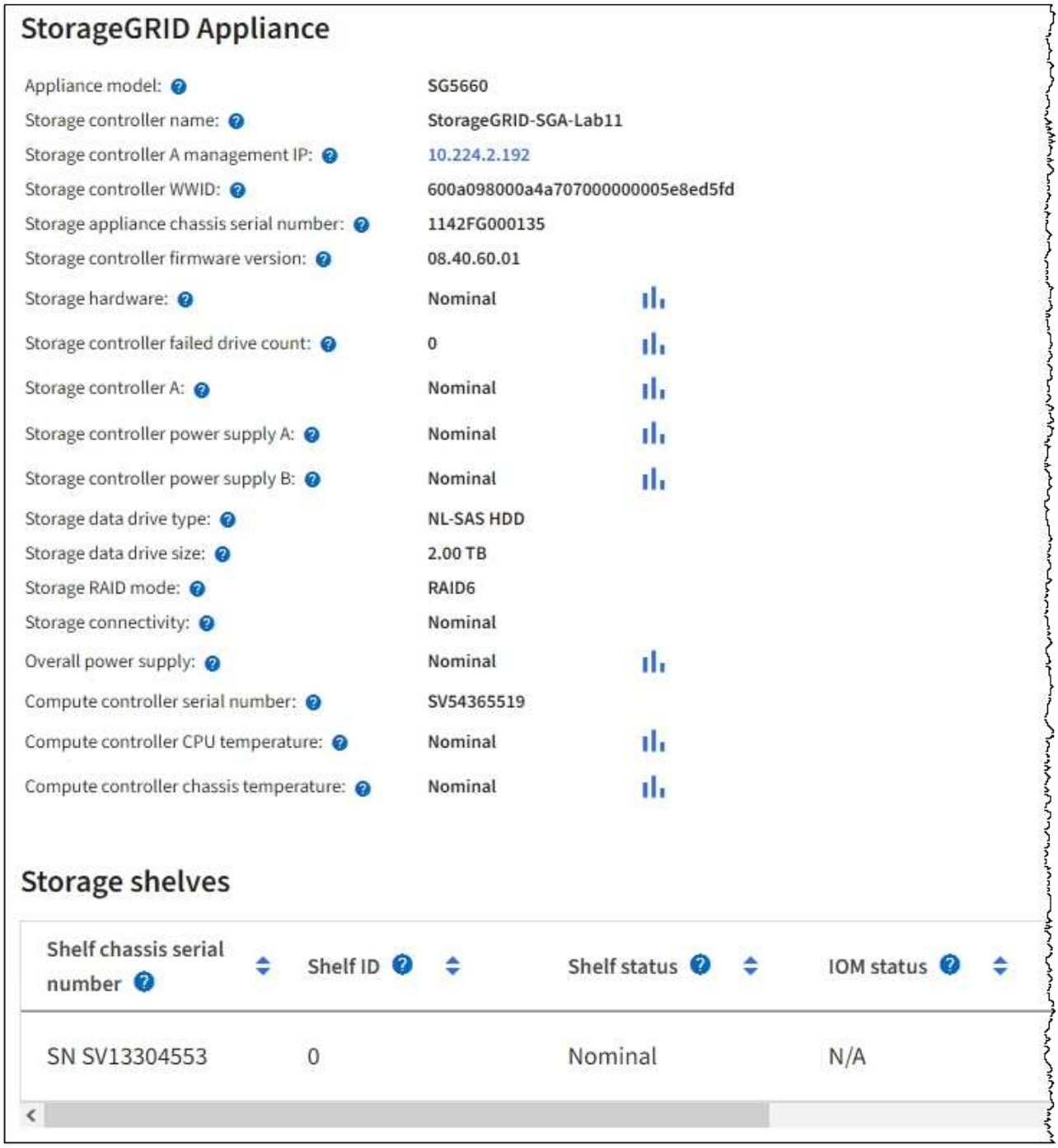
   a. Visualizzare i grafici relativi all'utilizzo della CPU e della memoria per determinare le percentuali di utilizzo della CPU e della memoria nel tempo. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.



b. Scorrere verso il basso per visualizzare la tabella dei componenti dell'appliance. Questa tabella contiene informazioni quali il nome del modello dell'appliance, i nomi dei controller, i numeri di serie e gli indirizzi IP e lo stato di ciascun componente.

> Alcuni campi, ad esempio Compute controller BMC IP e Compute hardware, vengono visualizzati solo per le appliance dotate di tale funzionalità.

I componenti per gli shelf di storage e gli shelf di espansione, se sono parte dell'installazione, vengono visualizzati in una tabella separata sotto la tabella dell'appliance.



Nella tabella Appliance	Descrizione
Modello di appliance	Il numero di modello di questo dispositivo StorageGRID mostrato in SANtricity OS.
Nome dello storage controller	Il nome dell'appliance StorageGRID visualizzato in SANtricity OS.
Storage controller A IP di gestione	Indirizzo IP per la porta di gestione 1 sul controller storage A. Questo IP viene utilizzato per accedere al sistema operativo SANtricity e risolvere i problemi di storage.

Nella tabella Appliance	Descrizione
IP di gestione dello storage controller B.	Indirizzo IP per la porta di gestione 1 sul controller di storage B. Questo IP viene utilizzato per accedere al sistema operativo SANtricity e risolvere i problemi di storage. Alcuni modelli di appliance non dispongono di un controller di storage B.
WWID dello storage controller	L'identificatore mondiale dello storage controller mostrato in SANtricity OS.
Numero di serie dello chassis dell'appliance di storage	Il numero di serie dello chassis dell'appliance.
Versione del firmware del controller di storage	La versione del firmware del controller di storage per l'appliance.
Hardware per lo storage	Lo stato generale dell'hardware del controller dello storage. Se Gestore di sistema di SANtricity riporta lo stato di intervento richiesto per l'hardware di storage, anche il sistema StorageGRID riporta questo valore. Se lo stato è "richiede attenzione", controllare prima lo storage controller utilizzando il sistema operativo SANtricity. Quindi, assicurarsi che non esistano altri allarmi applicabili al controller di calcolo.
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Controller dello storage A	Lo stato dello storage controller A.
Controller dello storage B	Lo stato dello storage controller B. Alcuni modelli di appliance non dispongono di un controller di storage B.
Alimentazione a del controller storage	Lo stato dell'alimentatore A per il controller dello storage.
Alimentazione controller storage B	Lo stato dell'alimentazione B del controller di storage.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato solido).
Dimensioni del disco per i dati di storage	Le dimensioni effettive di un'unità dati. **Nota**: Per i nodi con shelf di espansione, utilizzare Dimensioni del disco dati per ogni shelf invece. Le dimensioni effettive del disco potrebbero differire in base allo shelf.

Nella tabella Appliance	Descrizione
Storage RAID mode (modalità RAID storage)	La modalità RAID configurata per l'appliance.
Connettività dello storage	Lo stato di connettività dello storage.
Alimentatore generale	Lo stato di tutti gli alimentatori dell'apparecchio.
IP BMC del controller di calcolo	L'indirizzo IP della porta BMC (Baseboard Management Controller) nel controller di calcolo. Questo IP viene utilizzato per connettersi all'interfaccia BMC per monitorare e diagnosticare l'hardware dell'appliance. Questo campo non viene visualizzato per i modelli di appliance che non contengono un BMC.
Numero di serie del controller di calcolo	Il numero di serie del controller di calcolo.
Hardware di calcolo	Lo stato dell'hardware del controller di calcolo. Questo campo non viene visualizzato per i modelli di appliance che non dispongono di hardware di calcolo e storage separati.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di calcolo.
Temperatura dello chassis del controller di calcolo	Lo stato della temperatura del controller di calcolo.

+

Nella tabella Storage shelf	Descrizione
Numero di serie dello shelf chassis	Il numero di serie dello chassis dello shelf di storage.
ID shelf	L'identificativo numerico dello shelf di storage. • 99: Shelf dello storage controller • 0: Primo shelf di espansione • 1: Secondo shelf di espansione **Nota:** gli scaffali di espansione si applicano solo ai modelli SG6060 e SG6160.
Stato dello shelf	Lo stato generale dello shelf di storage.

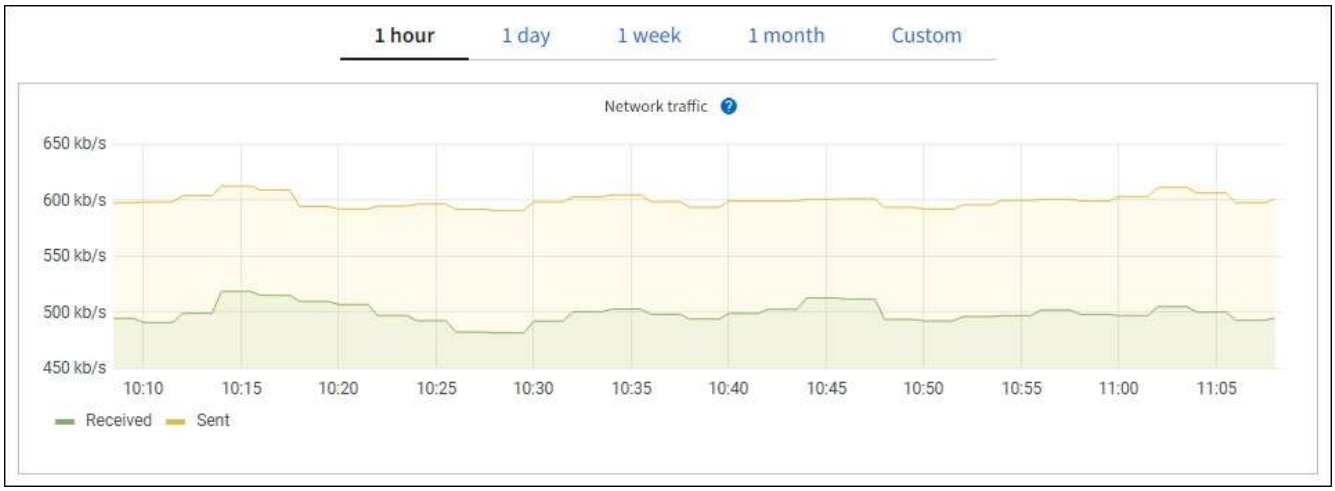
Nella tabella Storage shelf	Descrizione
Stato IOM	Lo stato dei moduli di input/output (IOM) in qualsiasi shelf di espansione. N/D se non si tratta di uno shelf di espansione.
Stato dell'alimentatore	Lo stato generale degli alimentatori per lo shelf di storage.
Stato del cassetto	Lo stato dei cassetti nello shelf di archiviazione. N/D se il ripiano non contiene cassetti.
Stato della ventola	Lo stato generale delle ventole di raffreddamento nello shelf di storage.
Slot per dischi	Il numero totale di slot per dischi nello shelf di storage.
Dischi dati	Il numero di dischi nello shelf di storage utilizzati per lo storage dei dati.
dimensione del disco dati	La dimensione effettiva di un'unità dati nello shelf di storage.
Dischi cache	Il numero di dischi nello shelf di storage utilizzati come cache.
Dimensione dell'unità cache	La dimensione dell'unità cache più piccola nello shelf di storage. Normalmente, le unità cache sono tutte delle stesse dimensioni.
Stato della configurazione	Lo stato di configurazione dello shelf di storage.

a. Verificare che tutti gli stati siano "nominale".

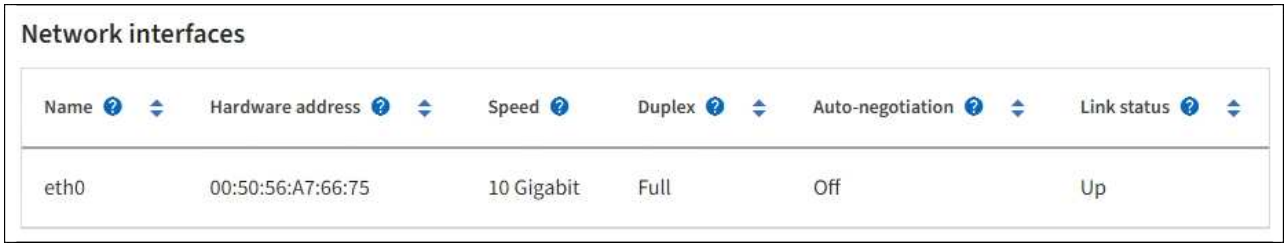
   Se uno stato non è "nominale", esaminare eventuali avvisi correnti. Puoi anche utilizzare Gestione di sistema di SANtricity per saperne di più su alcuni di questi valori hardware. Consultare le istruzioni per l'installazione e la manutenzione dell'apparecchio.

4. Selezionare **Network** per visualizzare le informazioni relative a ciascuna rete.

   Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo.



a. Consultare la sezione interfacce di rete.



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

Utilizzare la seguente tabella con i valori nella colonna **Speed** della tabella Network Interfaces (interfacce di rete) per determinare se le porte di rete 10/25-GbE dell'appliance sono state configurate per l'utilizzo della modalità Active/backup o LACP.

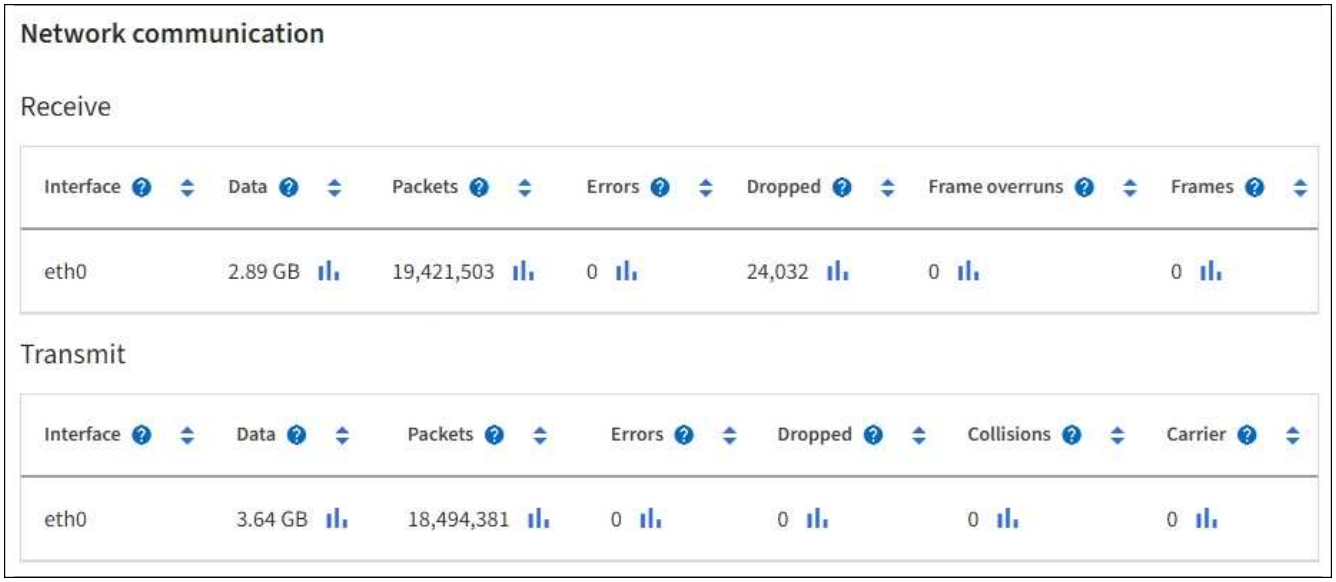
I valori mostrati nella tabella presuppongono che siano utilizzati tutti e quattro i collegamenti.

Modalità link	Modalità bond	Velocità di collegamento HIC singola (hic1, hic2, hic3, hic4)	Velocità rete client/griglia prevista (eth0,eth2)
Aggregato	LACP	25	100
Corretto	LACP	25	50
Corretto	Attivo/Backup	25	25
Aggregato	LACP	10	40
Corretto	LACP	10	20
Corretto	Attivo/Backup	10	10

Vedere "Configurare i collegamenti di rete" Per ulteriori informazioni sulla configurazione delle porte 10/25-GbE.

b. Consultare la sezione comunicazione di rete.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, nonché altre metriche di ricezione e trasmissione.



Network communication

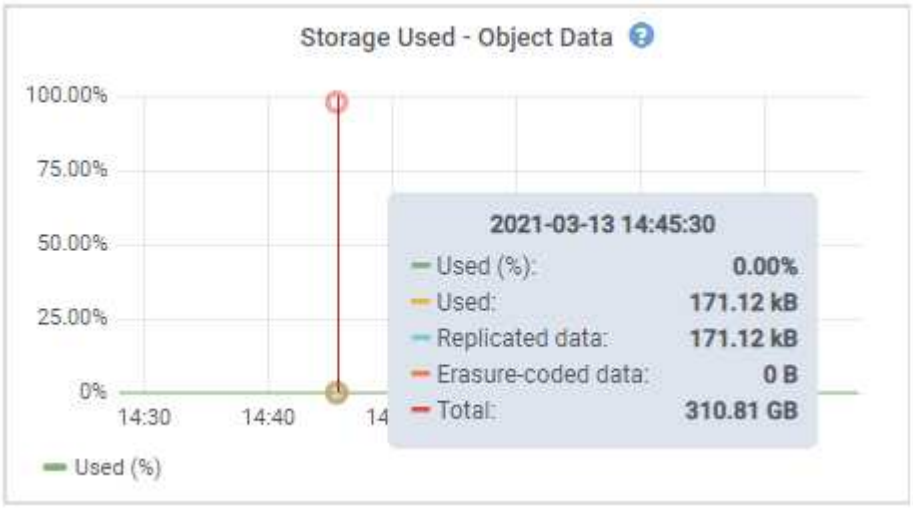
Receive

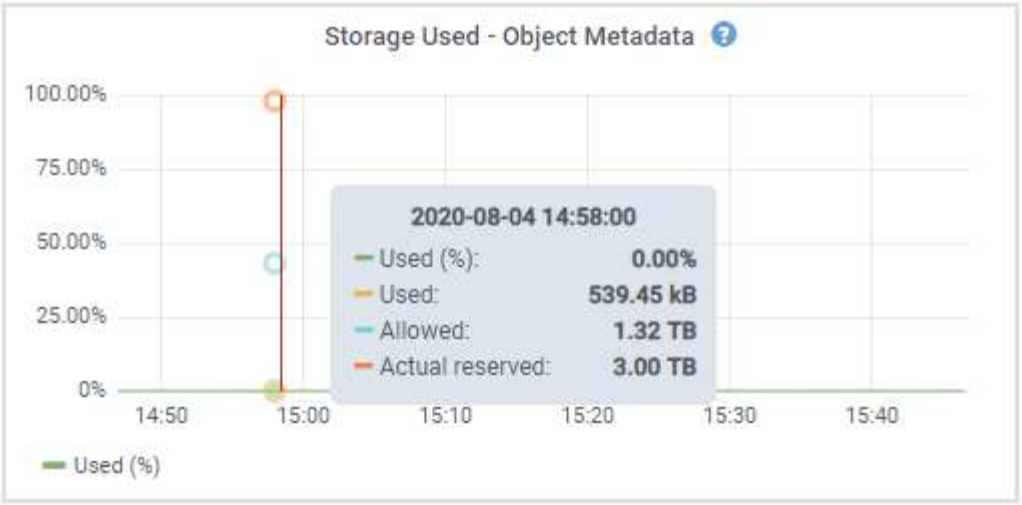
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

5. Selezionare **Storage** per visualizzare i grafici che mostrano le percentuali di storage utilizzate nel tempo per i dati degli oggetti e i metadati degli oggetti, nonché informazioni su dischi, volumi e archivi di oggetti.

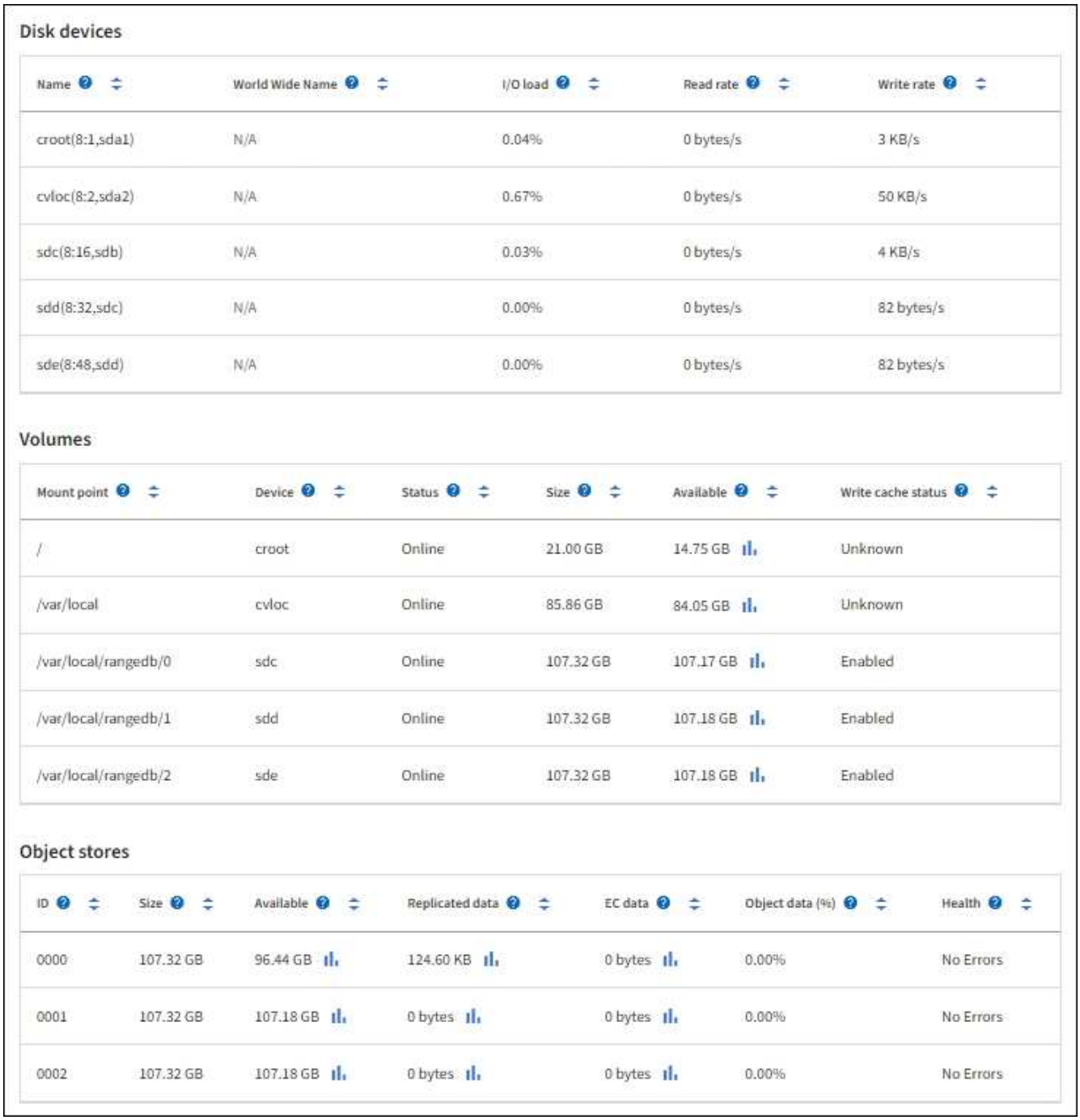




a. Scorrere verso il basso per visualizzare le quantità di storage disponibili per ciascun volume e archivio di oggetti.

   Il nome internazionale di ciascun disco corrisponde all'identificativo mondiale del volume (WWID) visualizzato quando si visualizzano le proprietà standard del volume in SANtricity OS (il software di gestione collegato al controller di storage dell'appliance).

   Per semplificare l'interpretazione delle statistiche di lettura e scrittura dei dischi relative ai punti di montaggio del volume, la prima parte del nome visualizzato nella colonna **Name** della tabella Disk Devices (periferiche disco) (ovvero *sdc*, *sdd*, *sde* e così via) corrisponde al valore visualizzato nella colonna **Device** della tabella Volumes (volumi).



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Visualizza informazioni sui nodi di amministrazione dell'appliance e sui nodi gateway

La pagina Nodes (nodi) elenca le informazioni sullo stato del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ogni appliance di servizi utilizzata come nodo di amministrazione o nodo gateway. È inoltre possibile visualizzare memoria, hardware di storage, risorse di rete, interfacce di rete, indirizzi di rete, e ricevere e trasmettere dati.

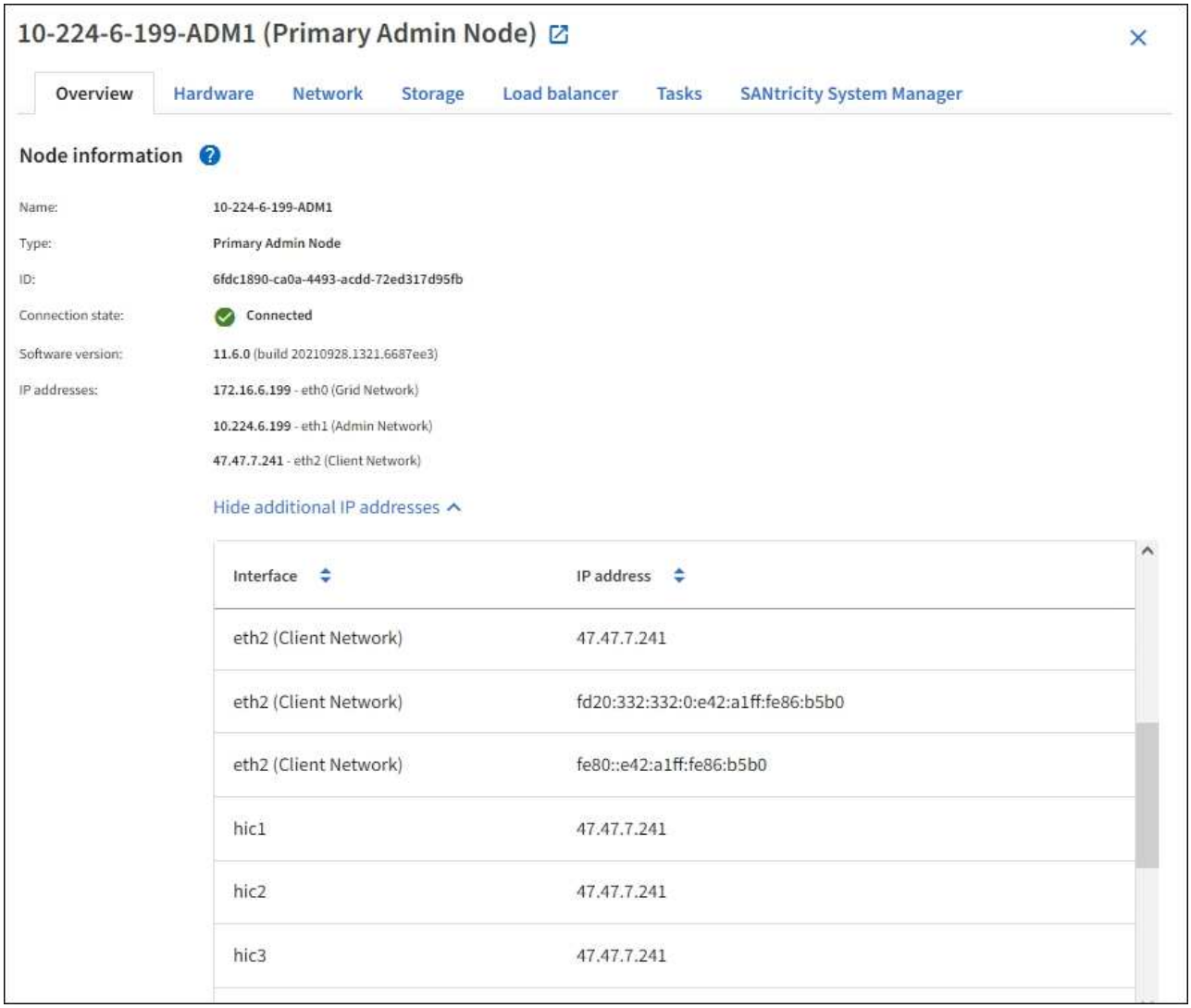
Fasi

1. Dalla pagina Nodes (nodi), selezionare un nodo Admin dell'appliance o un nodo Gateway dell'appliance.
2. Selezionare **Panoramica**.

   La sezione Node information (informazioni nodo) della scheda Overview (Panoramica) visualizza informazioni riepilogative per il nodo, ad esempio il nome, il tipo, l'ID e lo stato di connessione del nodo.

L’elenco degli indirizzi IP include il nome dell’interfaccia per ciascun indirizzo, come segue:

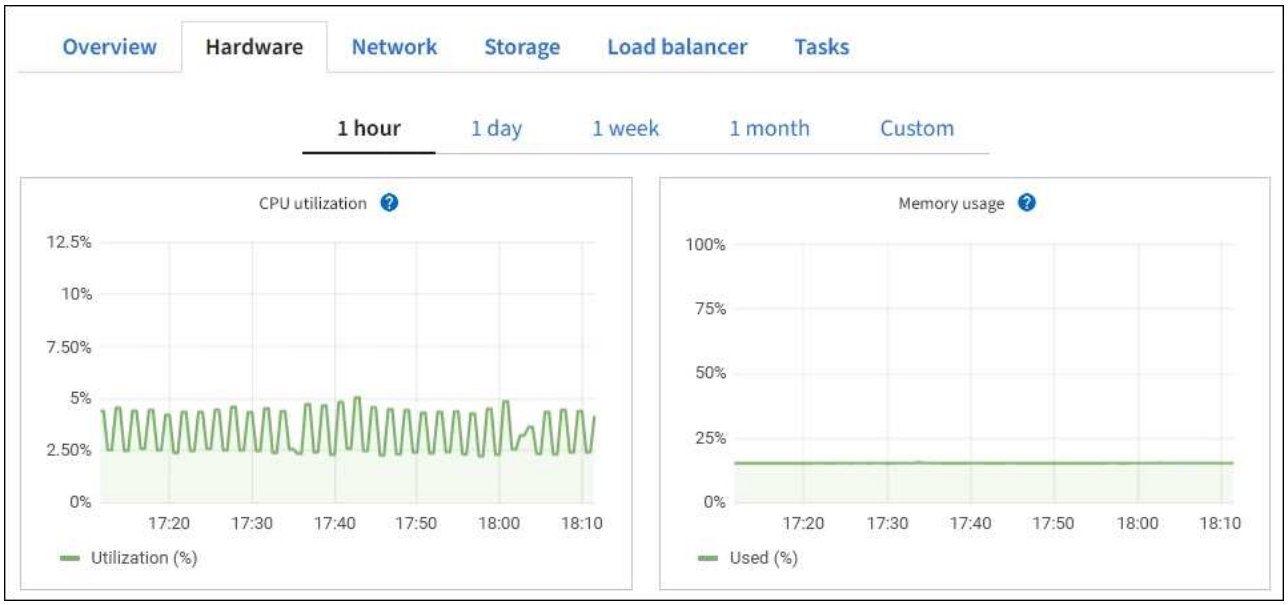
- **Adllb** e **adlli**: Visualizzato se si utilizza il bonding Active/backup per l’interfaccia di Admin Network
- **eth**: Rete griglia, rete amministrativa o rete client.
- **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell’appliance. Queste porte possono essere collegate tra loro e collegate alla rete griglia StorageGRID (eth0) e alla rete client (eth2).
- **mtc**: Una delle porte 1-GbE fisiche dell’appliance. Una o più interfacce mtc sono collegate per formare l’interfaccia Admin Network (eth1). È possibile lasciare altre interfacce mtc disponibili per la connettività locale temporanea per un tecnico del data center.



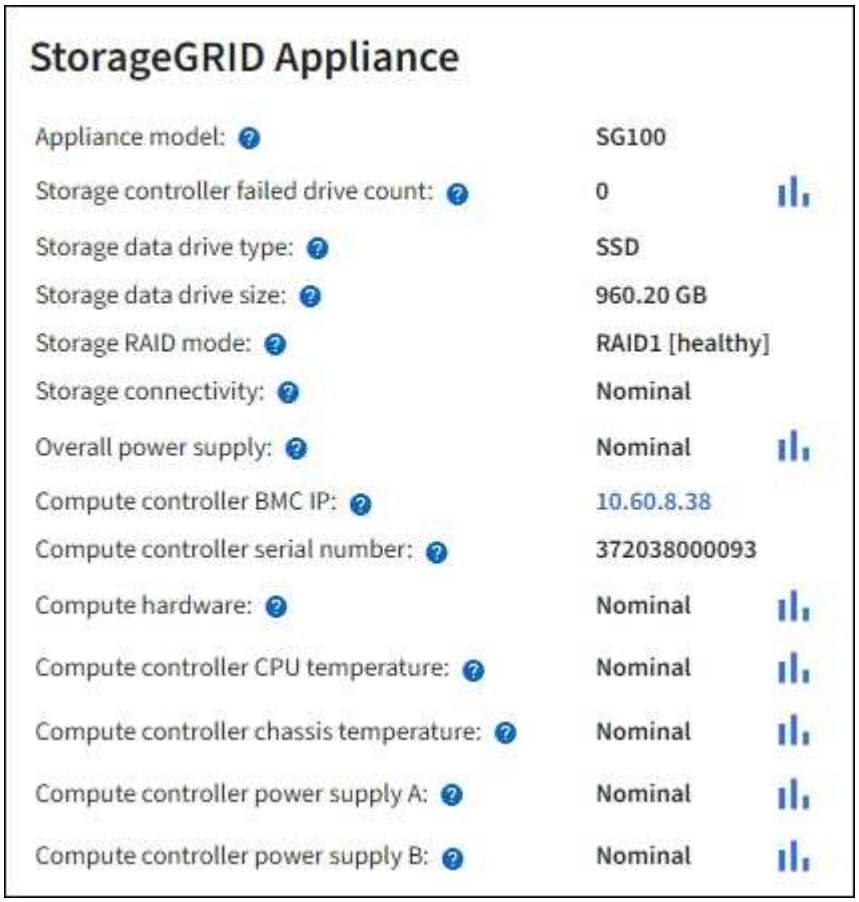
La sezione Avvisi della scheda Panoramica visualizza gli avvisi attivi per il nodo.

3. Selezionare **hardware** per visualizzare ulteriori informazioni sull’appliance.

   a. Visualizzare i grafici relativi all’utilizzo della CPU e della memoria per determinare le percentuali di utilizzo della CPU e della memoria nel tempo. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.



b. Scorrere verso il basso per visualizzare la tabella dei componenti dell'appliance. Questa tabella contiene informazioni come il nome del modello, il numero di serie, la versione del firmware del controller e lo stato di ciascun componente.



Nella tabella Appliance	Descrizione
Modello di appliance	Il numero di modello dell'appliance StorageGRID.

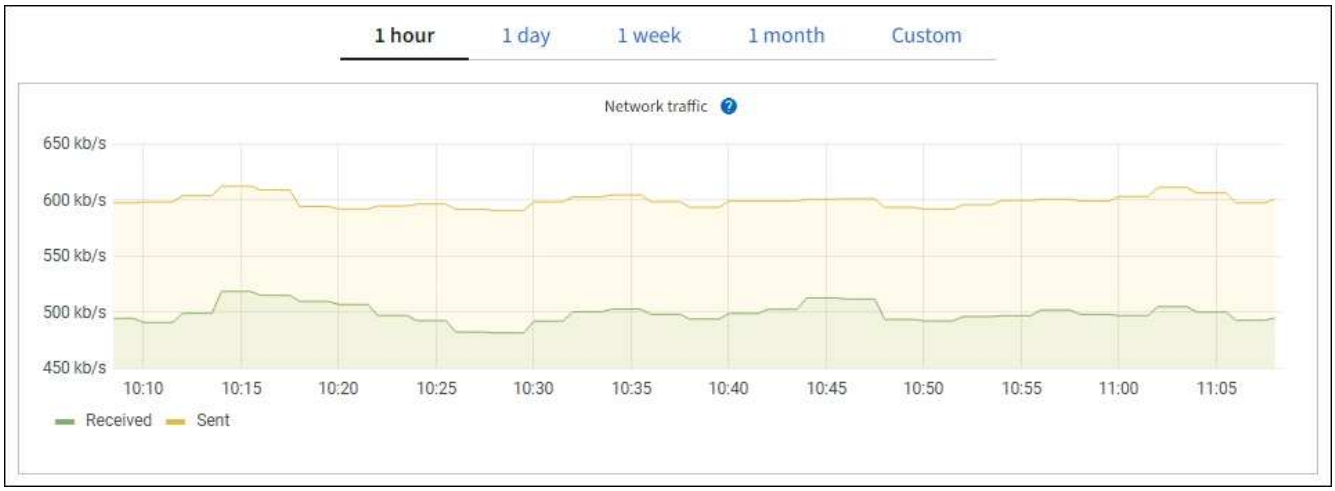
Nella tabella Appliance	Descrizione
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato solido).
Dimensioni del disco per i dati di storage	Le dimensioni effettive di un'unità dati.
Storage RAID mode (modalità RAID storage)	La modalità RAID per l'appliance.
Alimentatore generale	Lo stato di tutti gli alimentatori dell'apparecchio.
IP BMC del controller di calcolo	L'indirizzo IP della porta BMC (Baseboard Management Controller) nel controller di calcolo. È possibile utilizzare questo IP per connettersi all'interfaccia BMC per monitorare e diagnosticare l'hardware dell'appliance. Questo campo non viene visualizzato per i modelli di appliance che non contengono un BMC.
Numero di serie del controller di calcolo	Il numero di serie del controller di calcolo.
Hardware di calcolo	Lo stato dell'hardware del controller di calcolo.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di calcolo.
Temperatura dello chassis del controller di calcolo	Lo stato della temperatura del controller di calcolo.

a. Verificare che tutti gli stati siano "nominale".

   Se uno stato non è "nominale", esaminare eventuali avvisi correnti.

4. Selezionare **Network** per visualizzare le informazioni relative a ciascuna rete.

   Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo.



a. Consultare la sezione interfacce di rete.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up

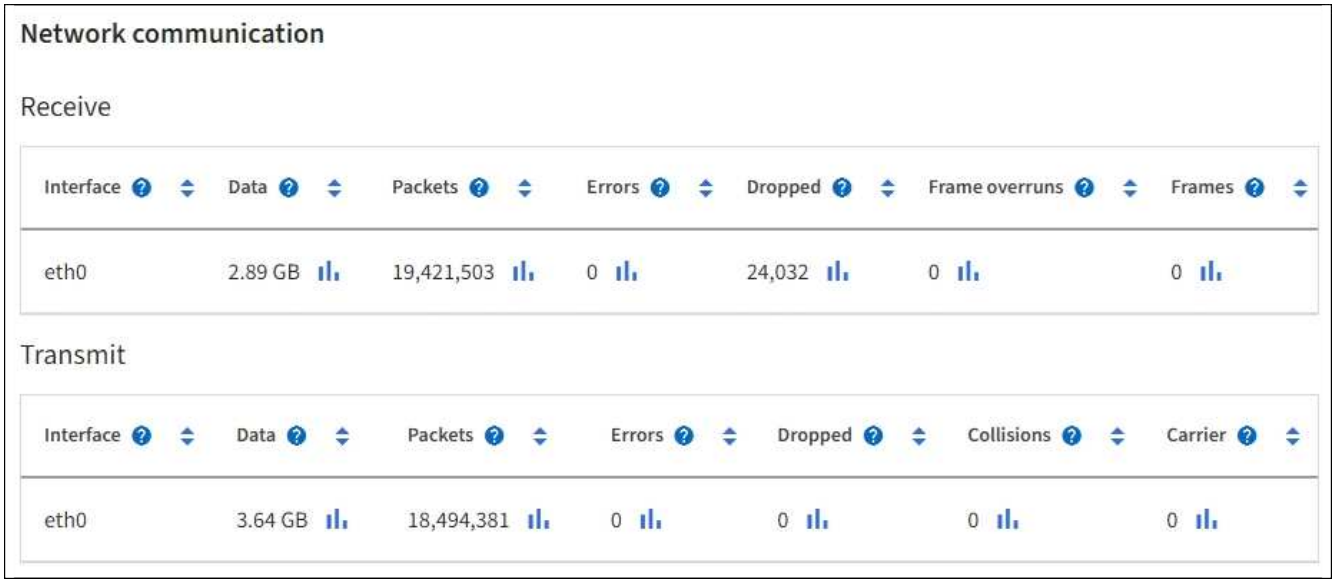
Utilizzare la seguente tabella con i valori nella colonna **Speed** della tabella Network Interfaces (interfacce di rete) per determinare se le quattro porte di rete 40/100-GbE dell'appliance sono state configurate per l'utilizzo della modalità Active/backup o LACP.

I valori mostrati nella tabella presuppongono che siano utilizzati tutti e quattro i collegamenti.

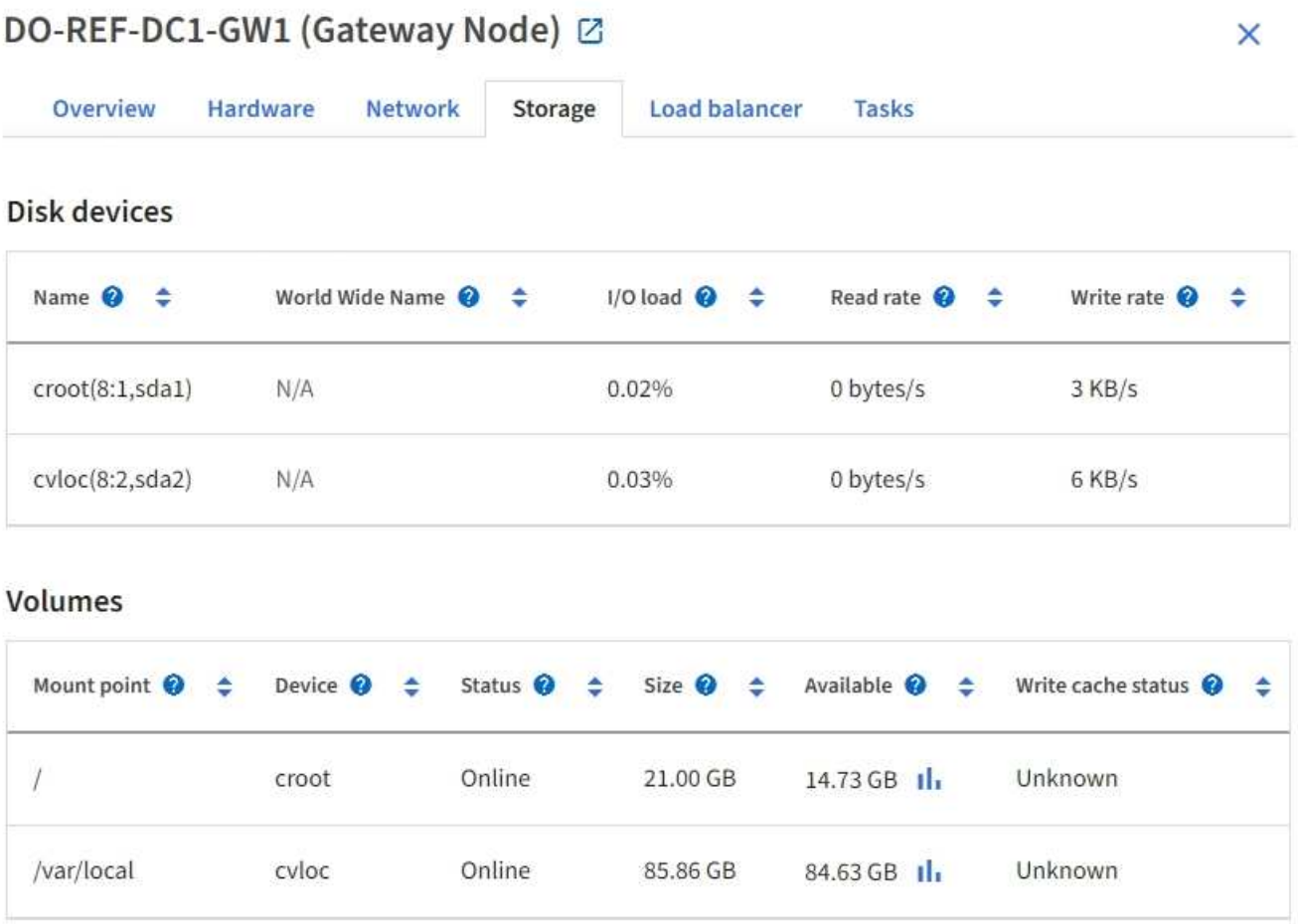
Modalità link	Modalità bond	Velocità di collegamento HIC singola (hic1, hic2, hic3, hic4)	Velocità rete client/griglia prevista (eth0, eth2)
Aggregato	LACP	100	400
Corretto	LACP	100	200
Corretto	Attivo/Backup	100	100
Aggregato	LACP	40	160
Corretto	LACP	40	80
Corretto	Attivo/Backup	40	40

b. Consultare la sezione comunicazione di rete.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, nonché altre metriche di ricezione e trasmissione.



5. Selezionare **Storage** per visualizzare le informazioni relative ai dischi e ai volumi sull'appliance di servizi.



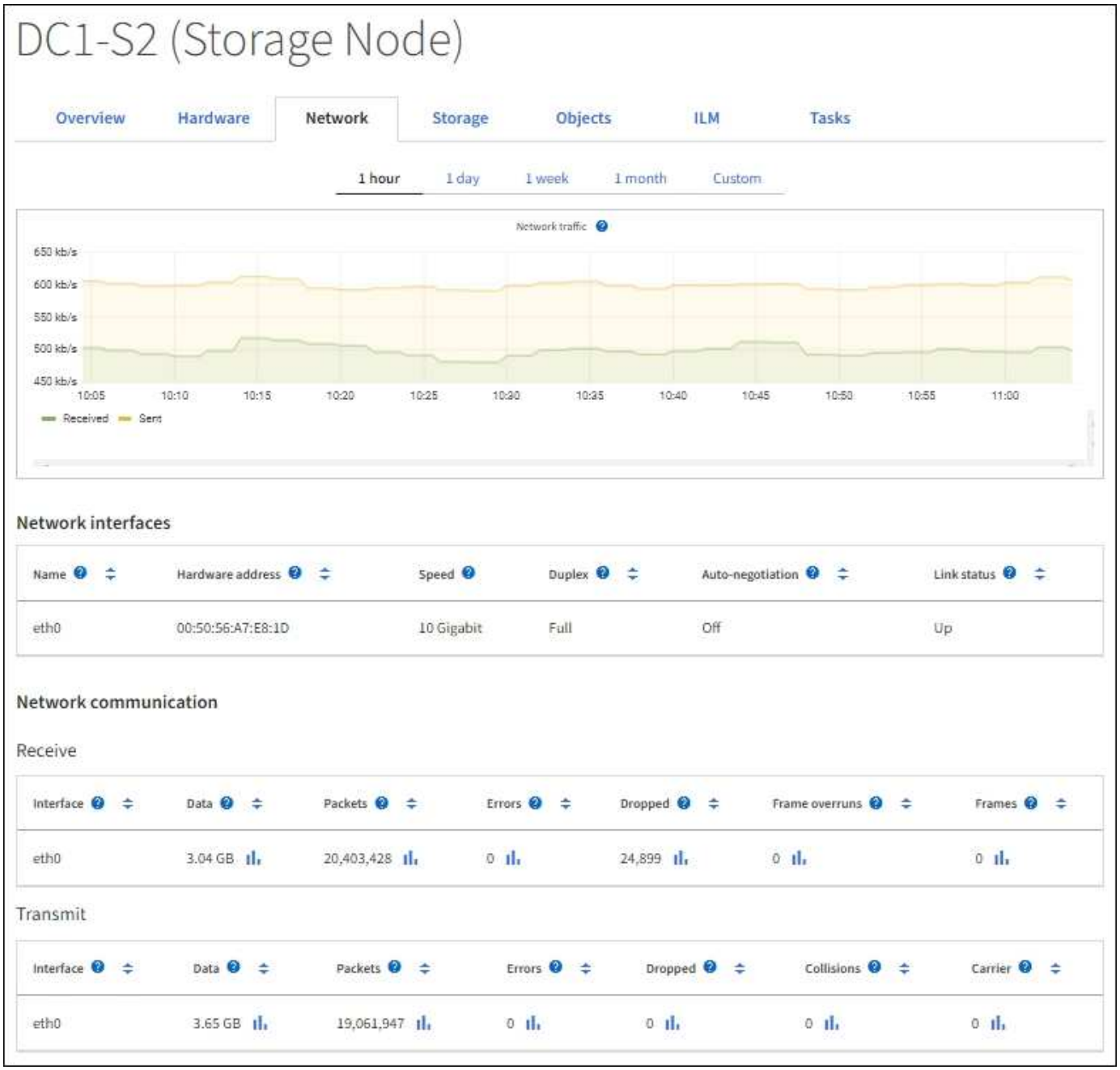
Visualizzare la scheda rete

La scheda Network (rete) visualizza un grafico che mostra il traffico di rete ricevuto e inviato attraverso tutte le interfacce di rete del nodo, del sito o della griglia.

Viene visualizzata la scheda Network (rete) per tutti i nodi, ciascun sito e l'intera griglia.

Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.

Per i nodi, la tabella interfacce di rete fornisce informazioni sulle porte di rete fisiche di ciascun nodo. La tabella delle comunicazioni di rete fornisce dettagli sulle operazioni di ricezione e trasmissione di ciascun nodo e sui contatori di guasti segnalati dai driver.



Informazioni correlate

"Monitorare le connessioni di rete e le performance"

Visualizzare la scheda Storage (archiviazione)

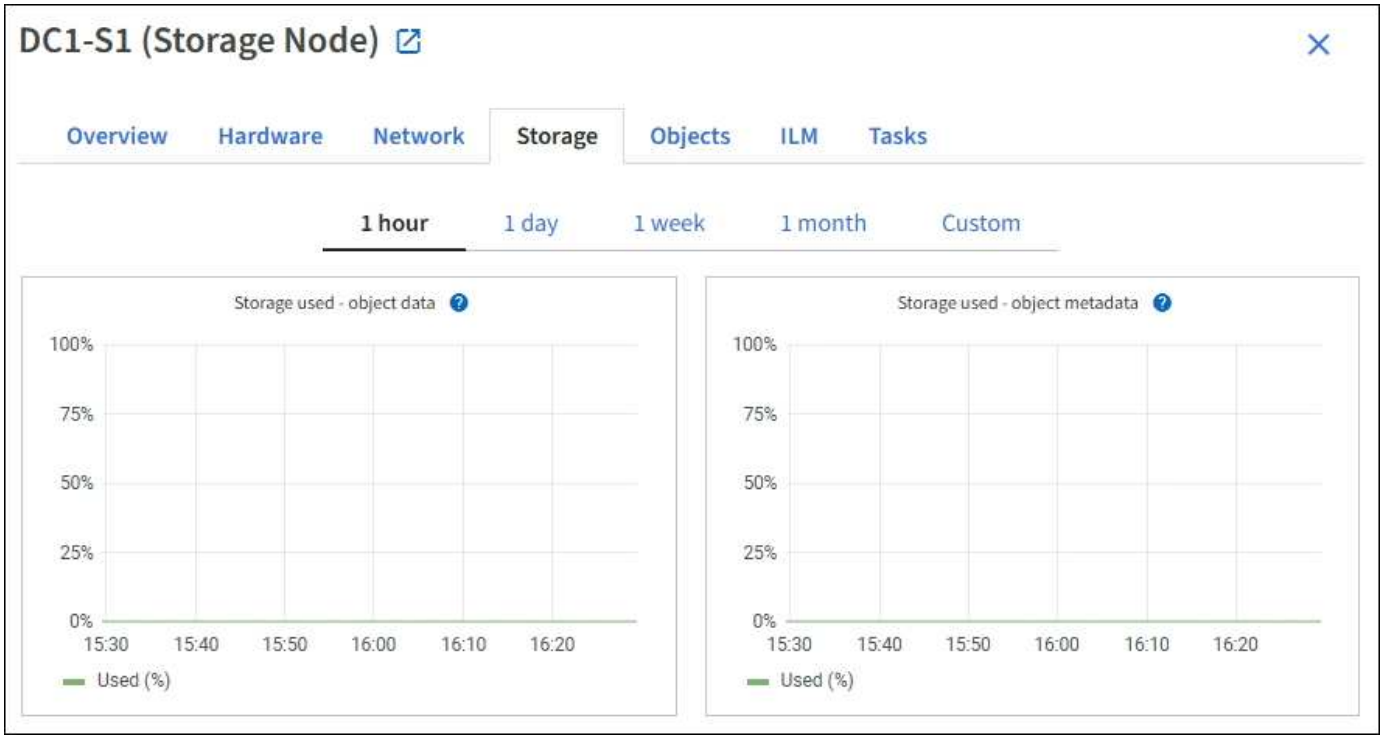
La scheda Storage riepiloga la disponibilità dello storage e altre metriche di storage.

Viene visualizzata la scheda Storage (archiviazione) per tutti i nodi, ciascun sito e l'intera griglia.

Grafici utilizzati per lo storage

Per i nodi di storage, ciascun sito e l'intero grid, la scheda Storage include grafici che mostrano la quantità di storage utilizzata dai dati degli oggetti e dai metadati degli oggetti nel tempo.

Quando un nodo non è connesso alla griglia, ad esempio durante l'aggiornamento o uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della griglia. Dopo che un nodo si ricollega alla griglia, attendere alcuni minuti per consentire la stabilizzazione dei valori.



Dischi, volumi e tabelle di archiviazione degli oggetti

Per tutti i nodi, la scheda Storage contiene i dettagli relativi ai dischi e ai volumi sul nodo. Per i nodi di storage, la tabella degli archivi di oggetti fornisce informazioni su ciascun volume di storage.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

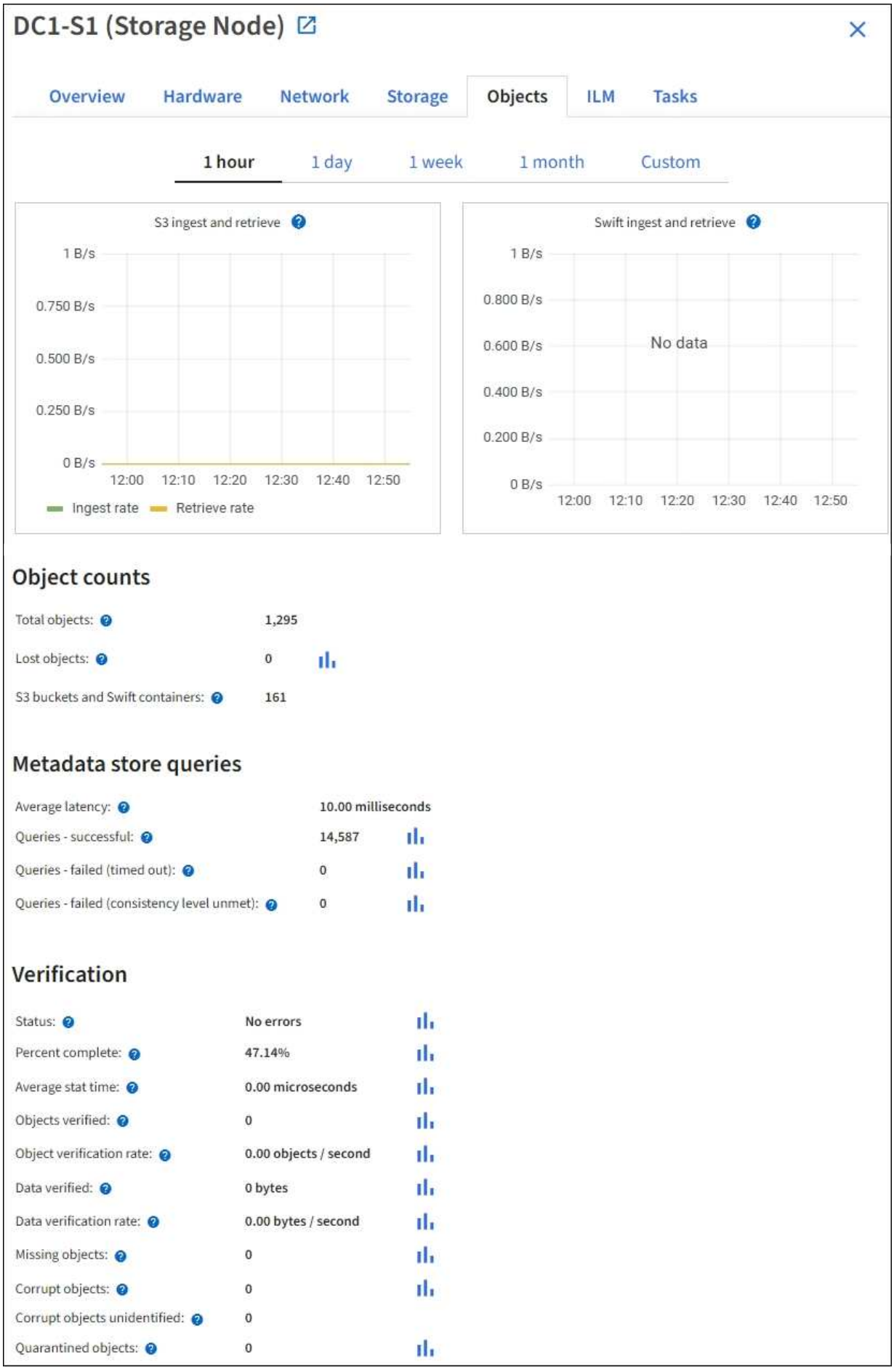
Informazioni correlate

"Monitorare la capacità dello storage"

Visualizzare la scheda oggetti

La scheda oggetti fornisce informazioni su "S3" e. "Rapido" velocità di acquisizione e recupero.

Viene visualizzata la scheda oggetti per ciascun nodo di storage, ciascun sito e l'intera griglia. Per i nodi di storage, la scheda oggetti fornisce anche conteggi di oggetti e informazioni sulle query dei metadati e sulla verifica in background.

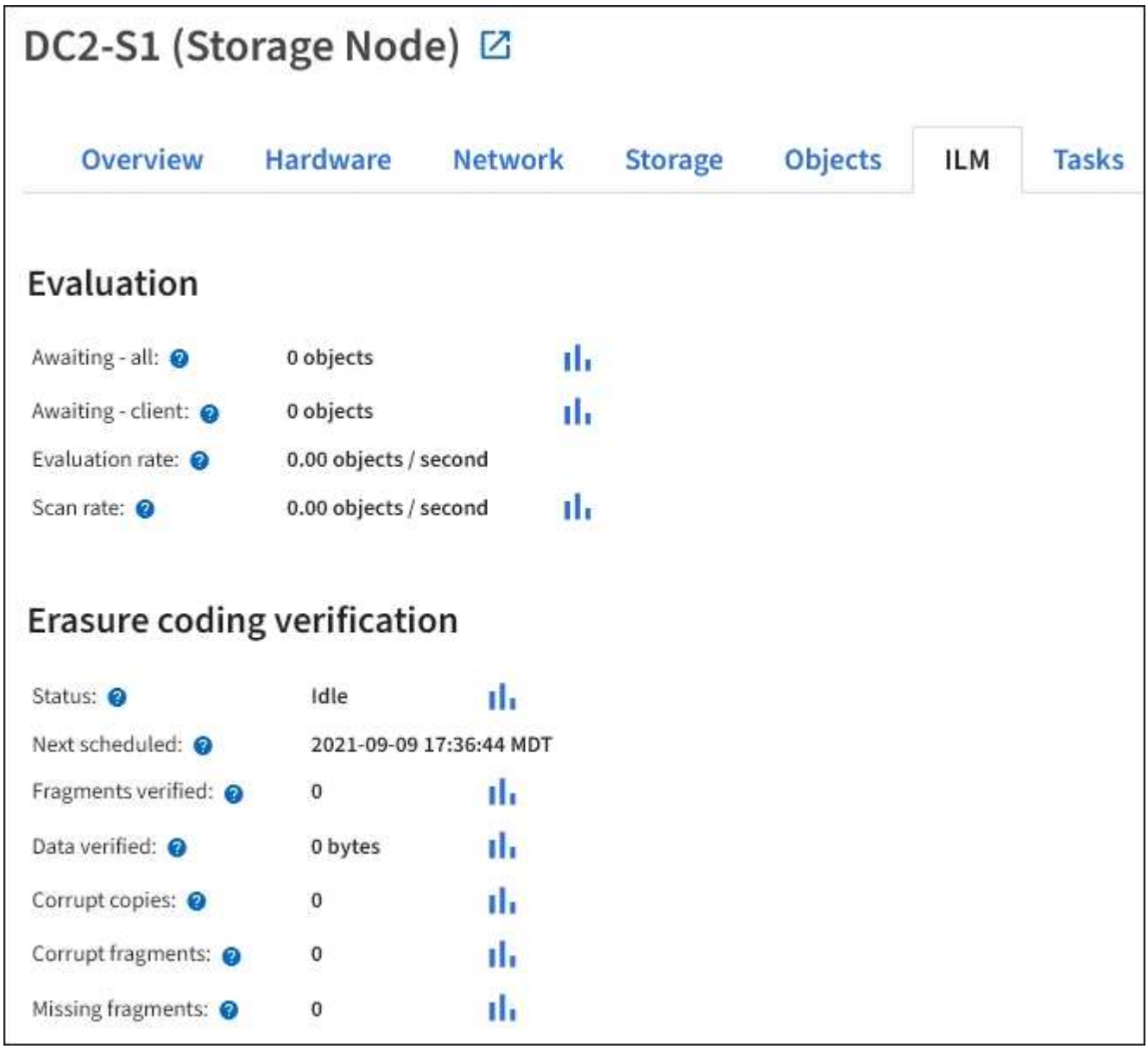

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

Visualizzare la scheda ILM

La scheda ILM fornisce informazioni sulle operazioni di Information Lifecycle management (ILM).

Viene visualizzata la scheda ILM per ciascun nodo di storage, ciascun sito e l'intera griglia. Per ogni sito e griglia, la scheda ILM mostra un grafico della coda ILM nel tempo. Per la griglia, questa scheda fornisce anche il tempo stimato per completare una scansione ILM completa di tutti gli oggetti.

Per i nodi storage, la scheda ILM fornisce dettagli sulla valutazione ILM e sulla verifica in background per gli oggetti sottoposti a erasure coding.



Informazioni correlate

"Monitorare la gestione del ciclo di vita delle informazioni"

"Amministrare StorageGRID"

Utilizzare la scheda attività

Viene visualizzata la scheda attività per tutti i nodi. È possibile utilizzare questa scheda per rinominare o riavviare un nodo o per impostare un nodo appliance in modalità di manutenzione.

Per i requisiti e le istruzioni completi per ciascuna opzione di questa scheda, vedere quanto segue:

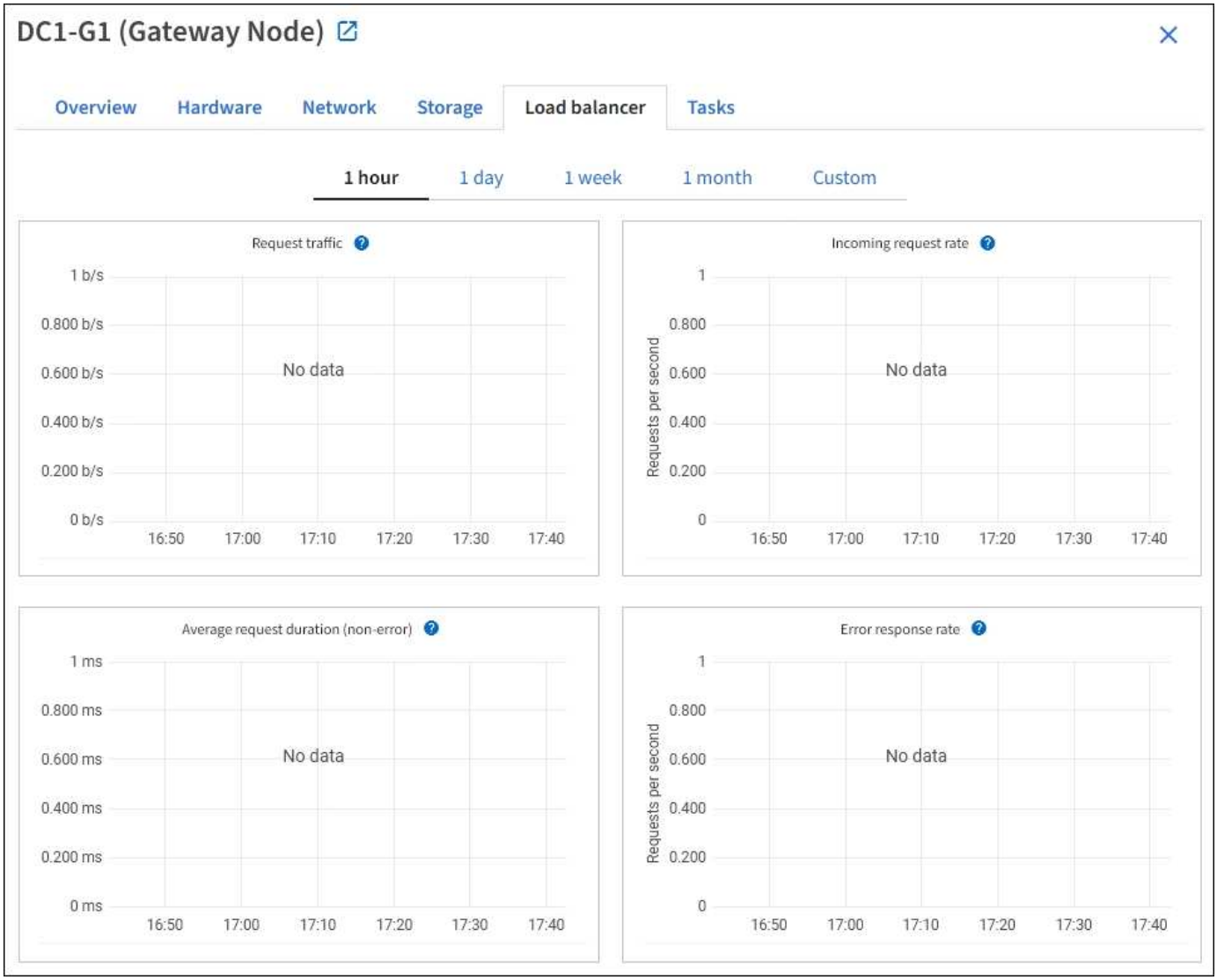
- "Rinominare la griglia, i siti e i nodi"
- "Nodo di reboot grid"
- "Impostare l'apparecchio in modalità di manutenzione"

Visualizzare la scheda bilanciamento del carico

La scheda bilanciamento del carico include i grafici delle performance e diagnostici relativi al funzionamento del servizio bilanciamento del carico.

Viene visualizzata la scheda Load Balancer (bilanciamento carico) per i nodi Admin e Gateway, per ciascun sito e per l'intera griglia. Per ogni sito, la scheda bilanciamento del carico fornisce un riepilogo aggregato delle statistiche per tutti i nodi del sito. Per l'intera griglia, la scheda bilanciamento del carico fornisce un riepilogo aggregato delle statistiche per tutti i siti.

Se non viene eseguito alcun i/o attraverso il servizio di bilanciamento del carico o non è configurato alcun bilanciamento del carico, i grafici visualizzano "Nessun dato".



Richiesta di traffico

Questo grafico fornisce una media mobile di 3 minuti del throughput dei dati trasmessi tra gli endpoint del bilanciamento del carico e i client che eseguono le richieste, in bit al secondo.

> Questo valore viene aggiornato al completamento di ogni richiesta. Di conseguenza, questo valore potrebbe differire dal throughput in tempo reale a bassi tassi di richiesta o per richieste di durata molto lunga. La scheda Network (rete) consente di ottenere una vista più realistica del comportamento corrente della rete.

Tasso di richiesta in entrata

Questo grafico fornisce una media mobile di 3 minuti del numero di nuove richieste al secondo, ripartita per tipo di richiesta (GET, PUT, HEAD e DELETE). Questo valore viene aggiornato quando le intestazioni di una nuova richiesta sono state convalidate.

Durata media della richiesta (non errore)

Questo grafico fornisce una media mobile di 3 minuti delle durate delle richieste, suddivisa per tipo di richiesta (GET, PUT, HEAD ed DELETE). Ogni durata della richiesta inizia quando un'intestazione di richiesta viene analizzata dal servizio Load Balancer e termina quando il corpo di risposta completo viene restituito al client.

Tasso di risposta agli errori

Questo grafico fornisce una media mobile di 3 minuti del numero di risposte agli errori restituite ai client al secondo, ripartito per codice di risposta agli errori.

Informazioni correlate

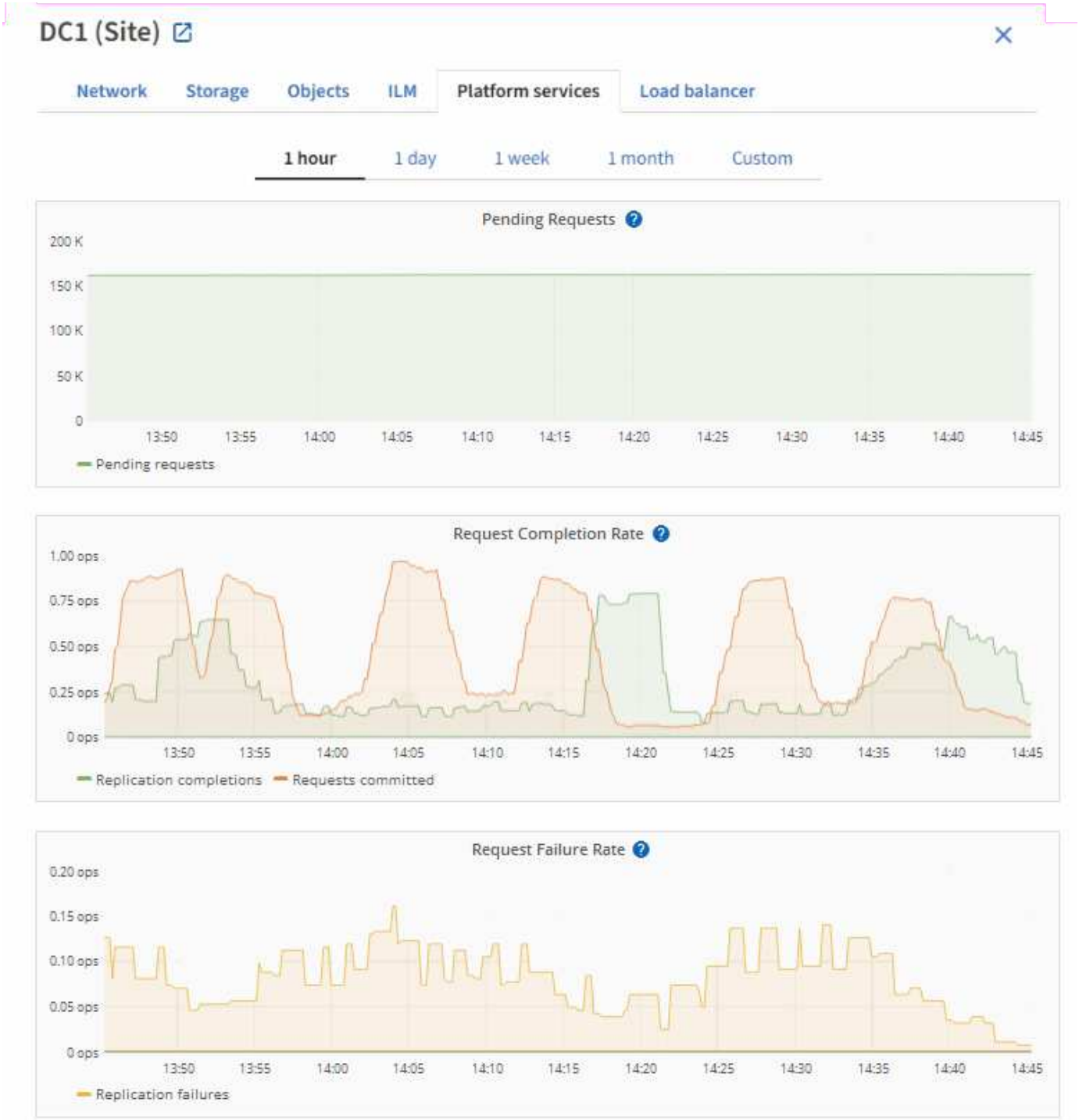
"Monitorare le operazioni di bilanciamento del carico"

"Amministrare StorageGRID"

Visualizzare la scheda Platform Services (servizi piattaforma)

La scheda Platform Services (servizi piattaforma) fornisce informazioni sulle operazioni di servizio della piattaforma S3 in un sito.

Viene visualizzata la scheda Platform Services (servizi piattaforma) per ciascun sito. Questa scheda fornisce informazioni sui servizi della piattaforma S3, come la replica CloudMirror e il servizio di integrazione della ricerca. I grafici di questa scheda mostrano metriche come il numero di richieste in sospeso, la percentuale di completamento della richiesta e la percentuale di guasti della richiesta.



Per ulteriori informazioni sui servizi della piattaforma S3, inclusi i dettagli sulla risoluzione dei problemi, consultare "Istruzioni per l'amministrazione di StorageGRID".

Visualizza la scheda Gestisci unità (solo SGF6112)

La scheda Manage Drives (Gestisci dischi) consente di accedere ai dettagli ed eseguire le attività di troubleshooting e manutenzione dei dischi dell'appliance SGF6112.

La scheda Gestisci dischi è disponibile solo per SGF6112 nodi di appliance di storage.

Utilizzando la scheda Gestisci unità, è possibile effettuare le seguenti operazioni:

- Visualizzare un layout delle unità di storage dei dati nell'appliance
- Visualizza una tabella in cui sono elencati ogni tipo, posizione, stato, versione del firmware e numero di serie del disco
- Eseguire le funzioni di risoluzione dei problemi e manutenzione su ciascuna unità

Per accedere alla scheda Gestisci unità, è necessario disporre di "Autorizzazione di accesso root o amministratore dell'appliance di storage".

Per informazioni sull'utilizzo della scheda Gestisci unità, vedere "Utilizzare la scheda Gestisci unità".

Visualizza la scheda SANtricity System Manager (solo e-Series)

La scheda Gestore di sistema di SANtricity consente di accedere a Gestore di sistema di SANtricity senza dover configurare o collegare la porta di gestione dell'appliance di storage. È possibile utilizzare questa scheda per esaminare le informazioni ambientali e di diagnostica dell'hardware, nonché i problemi relativi ai dischi.

> La scheda Gestore di sistema di SANtricity viene visualizzata solo per i nodi di appliance di storage che utilizzano hardware e-Series.

Utilizzando Gestione sistema di SANtricity, è possibile effettuare le seguenti operazioni:

- Visualizza i dati sulle performance come performance a livello di array di storage, latenza i/o, utilizzo della CPU del controller di storage e throughput.
- Controllare lo stato dei componenti hardware.
- Eseguire funzioni di supporto, tra cui la visualizzazione dei dati diagnostici e la configurazione di e-Series AutoSupport.

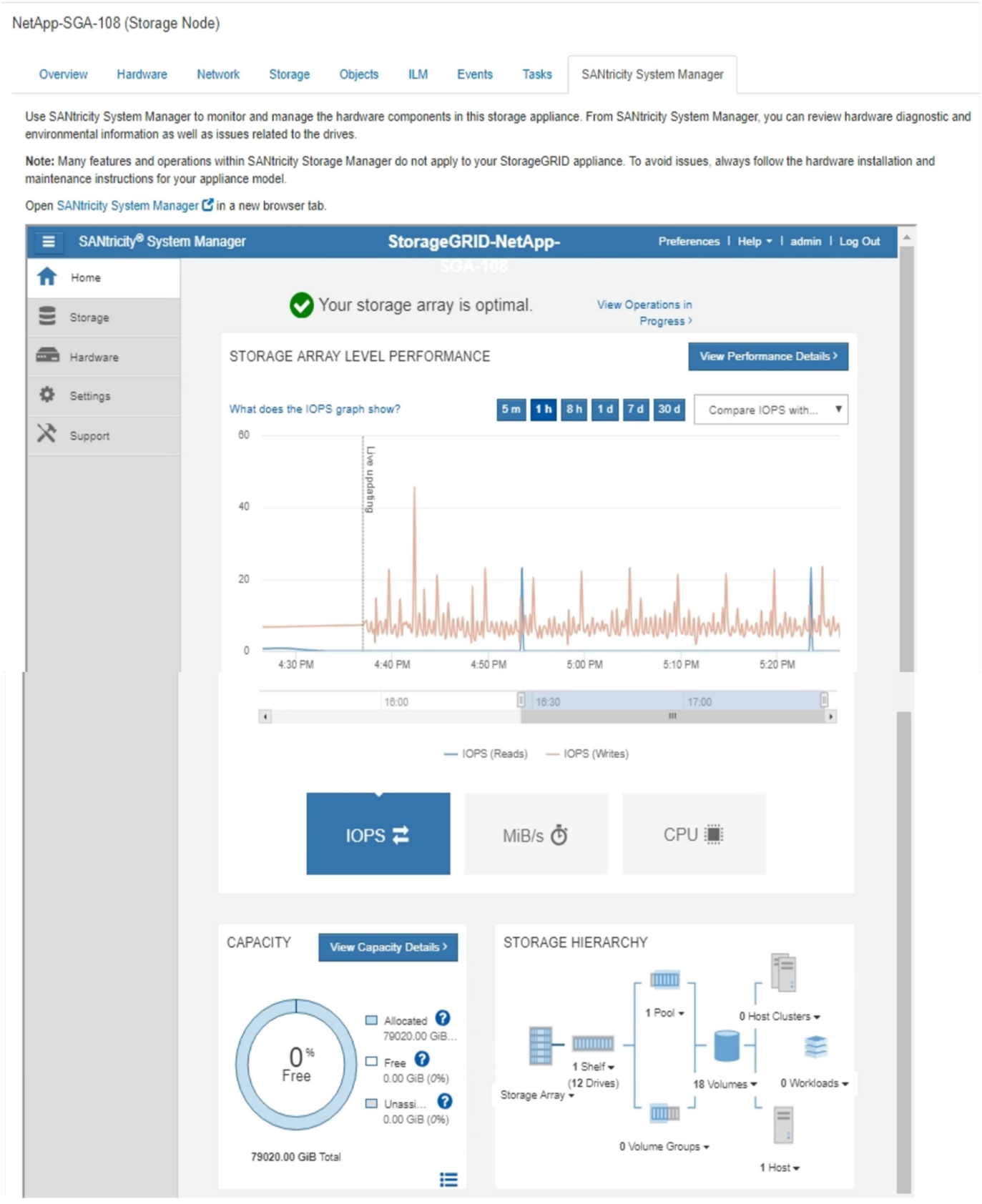
> Per utilizzare Gestione di sistema di SANtricity per configurare un proxy per e-Series AutoSupport, vedere "Invio dei pacchetti e-Series AutoSupport tramite StorageGRID".

Per accedere a Gestore di sistema di SANtricity tramite Gestione griglia, è necessario disporre di "Autorizzazione di accesso root o amministratore dell'appliance di storage".

> È necessario disporre del firmware SANtricity 8.70 o superiore per accedere a Gestione di sistema di SANtricity utilizzando Gestione griglia.

> L'accesso a Gestione di sistema SANtricity da Gestione griglia è generalmente destinato solo al monitoraggio dell'hardware dell'appliance e alla configurazione di e-Series AutoSupport. Molte funzionalità e operazioni di Gestione sistema di SANtricity, come l'aggiornamento del firmware, non si applicano al monitoraggio dell'appliance StorageGRID. Per evitare problemi, seguire sempre le istruzioni per la manutenzione dell'hardware dell'apparecchio.

La scheda visualizza la home page di Gestore di sistema di SANtricity.



È possibile utilizzare il collegamento Gestore di sistema di SANtricity per aprire Gestione di sistema di SANtricity in una nuova finestra del browser per una visualizzazione più semplice.

Per visualizzare i dettagli relativi all'utilizzo della capacità e delle prestazioni a livello di array di storage,

posizionare il cursore su ciascun grafico.

Per ulteriori informazioni sulla visualizzazione delle informazioni accessibili dalla scheda Gestore di sistema di SANtricity, vedere "Documentazione di NetApp e-Series e SANtricity".

Informazioni da monitorare regolarmente

Cosa e quando monitorare

Anche se il sistema StorageGRID può continuare a funzionare quando si verificano errori o parti della griglia non sono disponibili, è necessario monitorare e risolvere potenziali problemi prima che influiscano sull'efficienza o sulla disponibilità della rete.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Informazioni sulle attività di monitoraggio

Un sistema occupato genera grandi quantità di informazioni. Il seguente elenco fornisce indicazioni sulle informazioni più importanti da monitorare costantemente.

Cosa monitorare	Frequenza
"Stato di salute del sistema"	Ogni giorno
Valuta a quale "Capacità di metadati e oggetti del nodo di storage" è in corso di consumo	Settimanale
"Operazioni di gestione del ciclo di vita delle informazioni"	Settimanale
"Risorse di rete e di sistema"	Settimanale
"Attività del tenant"	Settimanale
"Operazioni dei client S3 e Swift"	Settimanale
"Operazioni di bilanciamento del carico"	Dopo la configurazione iniziale e dopo eventuali modifiche alla configurazione
"Connessioni a federazione di griglie"	Settimanale
"Capacità del sistema storage di archiviazione esterno"	Settimanale

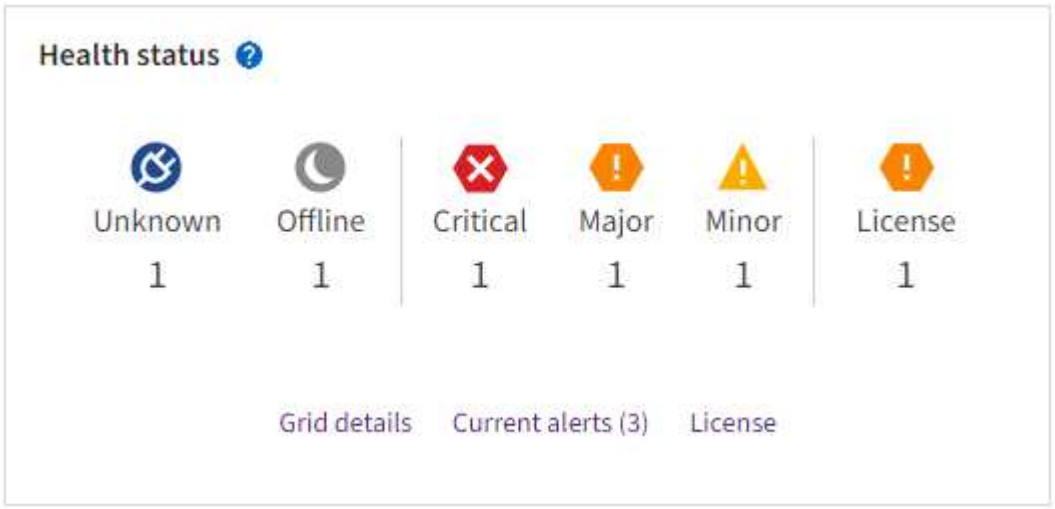
Monitorare lo stato del sistema

Monitorare quotidianamente lo stato di salute generale del sistema StorageGRID.

A proposito di questa attività

Il sistema StorageGRID può continuare a funzionare quando le parti della griglia non sono disponibili. I potenziali problemi indicati da avvisi o allarmi (sistema legacy) non sono necessariamente problemi con le operazioni del sistema. Esaminare i problemi riepilogati nella scheda di stato dello stato di salute del pannello di controllo di Grid Manager.

Per ricevere notifiche di avvisi non appena vengono attivati, è possibile "imposta le notifiche via email per gli avvisi" oppure "Configurare i trap SNMP".



In caso di problemi, vengono visualizzati collegamenti che consentono di visualizzare ulteriori dettagli:

Collegamento	Viene visualizzato quando…
Dettagli della griglia	Tutti i nodi sono disconnessi (stato di connessione sconosciuto o amministrativamente inattivo).
Avvisi correnti (critici, maggiori, minori)	Gli avvisi sono attualmente attivo.
Avvisi risolti di recente	Avvisi attivati la settimana scorsa sono ora risolti.
Licenza	Si è verificato un problema con la licenza software per questo sistema StorageGRID. È possibile "aggiornare le informazioni sulla licenza in base alle necessità".

Monitorare gli stati di connessione del nodo

Se uno o più nodi sono disconnessi dalla rete, potrebbero verificarsi problemi con le operazioni critiche di StorageGRID. Monitorare gli stati di connessione dei nodi e risolvere tempestivamente eventuali problemi.

Icona	Descrizione	Azione richiesta
	Non connesso - Sconosciuto Per un motivo sconosciuto, un nodo viene disconnesso o i servizi sul nodo vengono inaspettatamente disattivi. Ad esempio, un servizio sul nodo potrebbe essere stato arrestato o il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione dell'alimentazione o di un'interruzione imprevista. Potrebbe essere attivato anche l'avviso **Impossibile comunicare con il nodo**. Potrebbero essere attivi anche altri avvisi.	Richiede un'attenzione immediata. Selezionare ciascun avviso e seguire le azioni consigliate. Ad esempio, potrebbe essere necessario riavviare un servizio che ha arrestato o riavviato l'host per il nodo. **Nota**: 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 Per un motivo previsto, il nodo non è connesso alla rete. 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. In base al problema sottostante, questi nodi tornano spesso online senza alcun intervento.	Determinare se eventuali avvisi influiscono su questo nodo. Se sono attivi uno o più avvisi, selezionare ciascun avviso e seguire le azioni consigliate.
	Connesso Il nodo è collegato alla rete.	Non è richiesta alcuna azione.

Visualizzare gli avvisi correnti e risolti

Current alerts (Avvisi correnti): Quando viene attivato un avviso, viene visualizzata un'icona di avviso sul dashboard. Nella pagina nodi viene visualizzata anche un'icona di avviso per il nodo. Se "le notifiche e-mail di avviso sono configurate", viene inviata anche una notifica via email, a meno che l'avviso non sia stato tacitato.

Avvisi risolti: È possibile cercare e visualizzare una cronologia degli avvisi risolti.

Facoltativamente, hai guardato il video: "Video: Panoramica degli avvisi per StorageGRID 11,8"

La seguente tabella descrive le informazioni visualizzate in Grid Manager per gli avvisi correnti e risolti.

Intestazione di colonna	Descrizione
Nome o titolo	Il nome dell'avviso e la relativa descrizione.

Intestazione di colonna	Descrizione
Severità	La severità dell'avviso. Per gli avvisi correnti, se sono raggruppati più avvisi, la riga del titolo mostra il numero di istanze di tale avviso che si verificano a ogni livello di gravità. **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. **Major**: 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 esiste una condizione anomala che potrebbe influire sulla capacità di funzionamento del sistema se continua. È necessario monitorare e risolvere gli avvisi minori che non vengono risolti da soli per garantire che non causino problemi più gravi.
Tempo di attivazione	**Current alerts** (Avvisi correnti): La data e l'ora in cui l'avviso è stato attivato nell'ora locale e in UTC. Se vengono raggruppati più avvisi, la riga del titolo mostra l'ora dell'istanza più recente dell'avviso (*NEST*) e l'istanza più vecchia dell'avviso (*OLDEST*). **Resolved alerts** (Avvisi risolti): Quanto tempo fa è stato attivato l'avviso.
Sito/nodo	Il nome del sito e del nodo in cui si è verificato o si è verificato l'avviso.
Stato	Se l'avviso è attivo, tacitato o risolto. Se vengono raggruppati più avvisi e nell'elenco a discesa viene selezionato **tutti gli avvisi**, la riga del titolo mostra quante istanze di tale avviso sono attive e quante istanze sono state tacitati.
Tempo risolto (solo avvisi risolti)	Quanto tempo fa l'avviso è stato risolto.
Valori correnti o *valori di dati*	Il valore della metrica che ha causato l'attivazione dell'avviso. Per alcuni avvisi, vengono visualizzati valori aggiuntivi che consentono di comprendere e analizzare l'avviso. Ad esempio, i valori visualizzati per un avviso **Low Object Data Storage** includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata. **Nota:** se vengono raggruppati più avvisi correnti, i valori correnti non vengono visualizzati nella riga del titolo.

Intestazione di colonna	Descrizione
Valori attivati (solo avvisi risolti)	Il valore della metrica che ha causato l'attivazione dell'avviso. Per alcuni avvisi, vengono visualizzati valori aggiuntivi che consentono di comprendere e analizzare l'avviso. Ad esempio, i valori visualizzati per un avviso **Low Object Data Storage** includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata.

Fasi

1. Selezionare il collegamento **Avvisi correnti** o **Avvisi risolti** per visualizzare un elenco di avvisi in tali categorie. È inoltre possibile visualizzare i dettagli di un avviso selezionando **nodi** > ***nodo*** > **Panoramica** e selezionando l'avviso dalla tabella Avvisi.

   Per impostazione predefinita, gli avvisi correnti vengono visualizzati come segue:

   - Vengono visualizzati per primi gli avvisi attivati più di recente.
   - Più avvisi dello stesso tipo vengono visualizzati come gruppo.
   - Gli avvisi che sono stati tacitati non vengono visualizzati.
   - Per un avviso specifico su un nodo specifico, se le soglie vengono raggiunte per più di una severità, viene visualizzato solo l'allarme più grave. Ovvero, se vengono raggiunte soglie di allarme per i livelli di severità minori, maggiori e critici, viene visualizzato solo l'avviso critico.

     La pagina degli avvisi correnti viene aggiornata ogni due minuti.

2. Per espandere i gruppi di avvisi, selezionare il cart inferiore . Per chiudere i singoli avvisi in un gruppo, selezionare il caret up oppure selezionare il nome del gruppo.
3. Per visualizzare singoli avvisi invece di gruppi di avvisi, deselezionare la casella di controllo **Group alerts** (Avvisi di gruppo).
4. Per ordinare gli avvisi o i gruppi di avvisi correnti, selezionare le frecce su/giù in ogni intestazione di colonna.
   - Quando si seleziona **Group alerts** (Avvisi di gruppo), vengono ordinati sia i gruppi di avvisi che i singoli avvisi all'interno di ciascun gruppo. Ad esempio, è possibile ordinare gli avvisi in un gruppo in base all'ora * attivata per trovare l'istanza più recente di un avviso specifico.
   - Quando l'opzione **Group alerts** (Avvisi di gruppo) viene deselezionata, viene ordinato l'intero elenco di avvisi. Ad esempio, è possibile ordinare tutti gli avvisi in base a **nodo/sito** per visualizzare tutti gli avvisi relativi a un nodo specifico.
5. Per filtrare gli avvisi correnti in base allo stato (**tutti gli avvisi**, **attivi** o **silenziati**, utilizzare il menu a discesa nella parte superiore della tabella.

   Vedere "Tacitare le notifiche di avviso".

6. Per ordinare gli avvisi risolti:
   - Selezionare un periodo di tempo dal menu a discesa **quando attivato**.
   - Selezionare una o più severità dal menu a discesa **severità**.
   - Selezionare una o più regole di avviso predefinite o personalizzate dal menu a discesa **regola di avviso** per filtrare gli avvisi risolti correlati a una regola di avviso specifica.
   - Selezionare uno o più nodi dal menu a discesa **nodo** per filtrare gli avvisi risolti relativi a un nodo specifico.

7. Per visualizzare i dettagli di un avviso specifico, selezionarlo. Una finestra di dialogo fornisce dettagli e azioni consigliate per l'avviso selezionato.
8. (Facoltativo) per un avviso specifico, selezionare Silence this alert (tacita questo avviso) per tacitare la regola che ha causato l'attivazione dell'avviso.

   È necessario disporre di "Gestire gli avvisi o l'autorizzazione di accesso principale" per tacitare una regola di avviso.

   > Prestare attenzione quando si decide di tacitare una regola di avviso. Se una regola di avviso viene tacitata, è possibile che non si rilevi un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica.

9. Per visualizzare le condizioni correnti della regola di avviso:
   a. Dai dettagli dell'avviso, selezionare **View conditions** (Visualizza condizioni).

      Viene visualizzata una finestra a comparsa che elenca l'espressione Prometheus per ogni severità definita.

   b. Per chiudere la finestra a comparsa, fare clic in un punto qualsiasi all'esterno della finestra a comparsa.
10. Facoltativamente, selezionare **Edit rule** (Modifica regola) per modificare la regola di avviso che ha causato l'attivazione dell'avviso.

    È necessario disporre di "Gestire gli avvisi o l'autorizzazione di accesso principale" per modificare una regola di avviso.

    > Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

11. Per chiudere i dettagli dell'avviso, selezionare **Chiudi**.

Monitorare la capacità dello storage

Monitorare lo spazio utilizzabile totale disponibile per garantire che il sistema StorageGRID non esaurisca lo spazio di storage per gli oggetti o per i metadati degli oggetti.

StorageGRID memorizza i dati degli oggetti e i metadati degli oggetti separatamente e riserva una quantità specifica di spazio per un database Cassandra distribuito che contiene metadati degli oggetti. Monitorare la quantità totale di spazio consumata per gli oggetti e per i metadati degli oggetti, nonché le tendenze della quantità di spazio consumata per ciascuno di essi. Ciò consente di pianificare in anticipo l'aggiunta di nodi ed evitare interruzioni del servizio.

È possibile "visualizzare le informazioni sulla capacità dello storage" Per l'intero grid, per ogni sito e per ogni nodo di storage nel sistema StorageGRID.

Monitorare la capacità di storage per l'intero grid

Monitorare la capacità di storage complessiva del grid per garantire che rimanga spazio libero adeguato per i dati degli oggetti e i metadati degli oggetti. Comprendere come la capacità dello storage cambia nel tempo può aiutarti a pianificare l'aggiunta di nodi o volumi di storage prima che la capacità dello storage utilizzabile del

grid venga consumata.

La dashboard di Grid Manager consente di valutare rapidamente la quantità di storage disponibile per l'intero grid e per ciascun data center. La pagina nodi fornisce valori più dettagliati per i dati degli oggetti e i metadati degli oggetti.

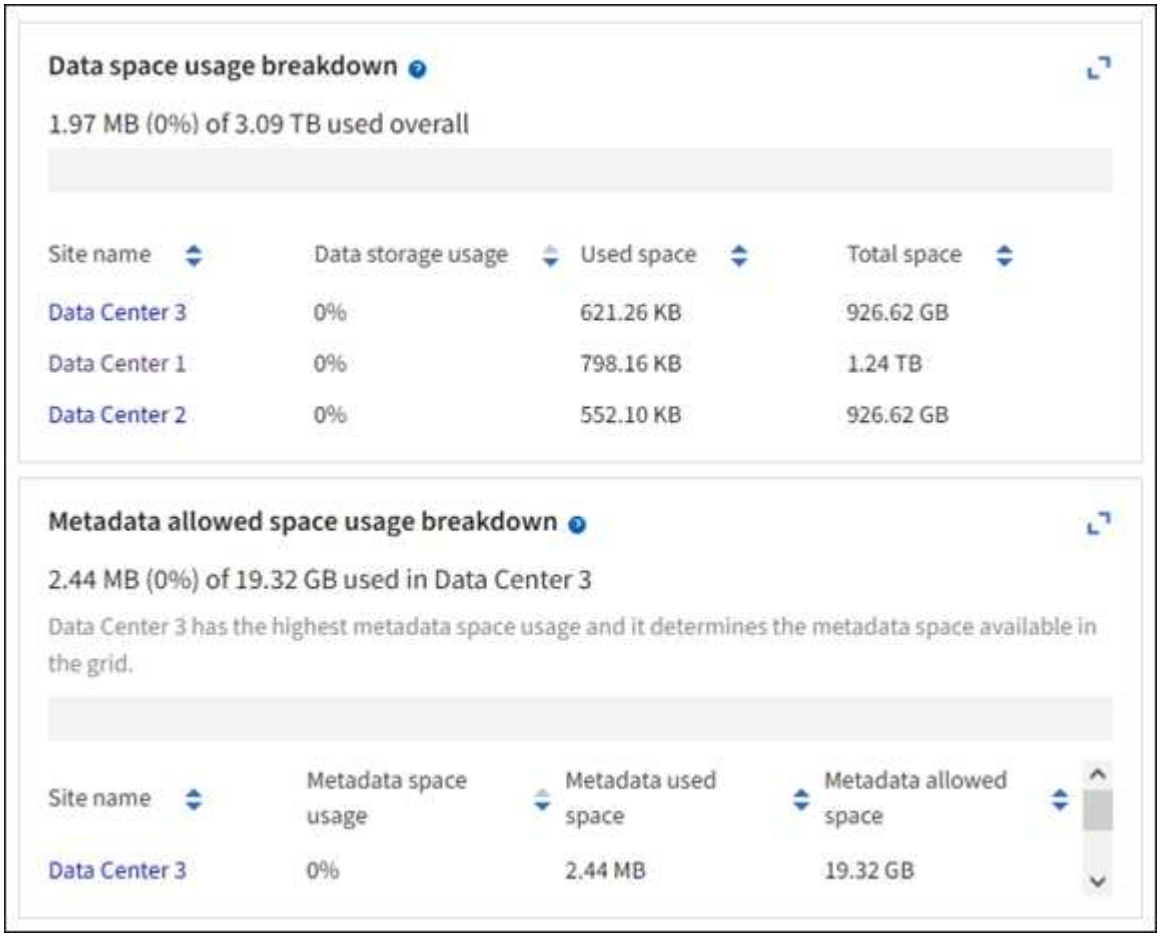
Fasi

1. Valutare la quantità di storage disponibile per l'intero grid e per ciascun data center.

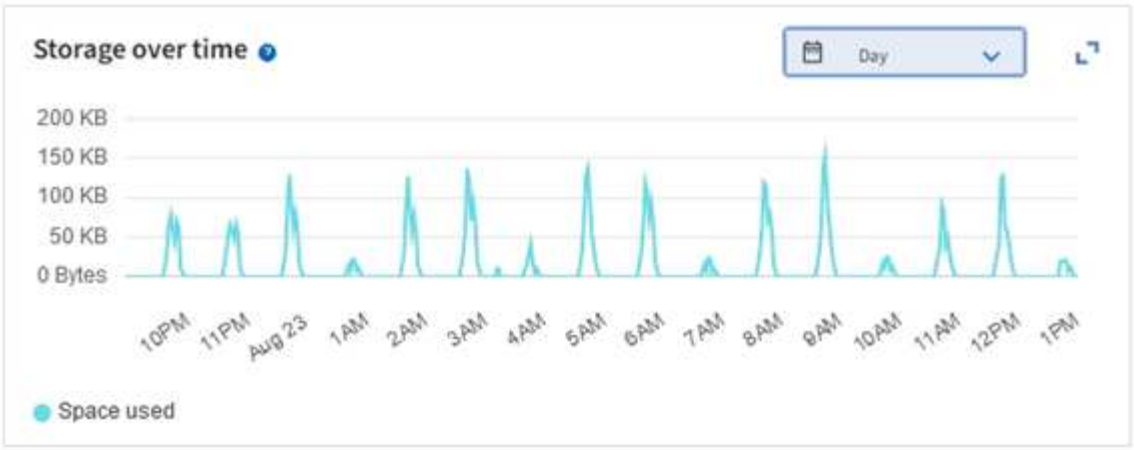
   a. Selezionare **Dashboard > Overview**.

   b. Prendere nota dei valori riportati nelle schede di analisi dell'utilizzo dello spazio dati e delle schede di analisi dell'utilizzo dello spazio consentito dai metadati. Ciascuna scheda elenca una percentuale di utilizzo dello storage, la capacità dello spazio utilizzato e lo spazio totale disponibile o consentito dal sito.

      Il riepilogo non include i supporti di archiviazione.



   a. Annotare il grafico sulla scheda Storage over Time (archiviazione nel tempo). Utilizzare il menu a discesa Time Period (periodo di tempo) per determinare la velocità di utilizzo dello storage.



2. Utilizzare la pagina nodi per ulteriori dettagli sulla quantità di storage utilizzata e sulla quantità di storage disponibile nella griglia per i dati degli oggetti e i metadati degli oggetti.
   a. Selezionare **NODI**.
   b. Selezionare ***grid*** > **Storage**.

   c. Posizionare il cursore sui grafici **Storage used - Object data** e **Storage used - Object metadata** per verificare la quantità di storage a oggetti e metadati a oggetti disponibile per l'intera griglia e la quantità di storage utilizzata nel tempo.

> I valori totali di un sito o di un grid non includono nodi che non hanno riportato metriche per almeno cinque minuti, come i nodi offline.

3. Pianificare un'espansione per aggiungere nodi di storage o volumi di storage prima che la capacità di storage utilizzabile del grid venga consumata.

   Quando si pianifica la tempistica di un'espansione, considerare quanto tempo sarà necessario per procurarsi e installare storage aggiuntivo.

Se la policy ILM utilizza la codifica erasure, è preferibile eseguire un'espansione quando i nodi di storage esistenti sono pieni al 70% circa per ridurre il numero di nodi da aggiungere.

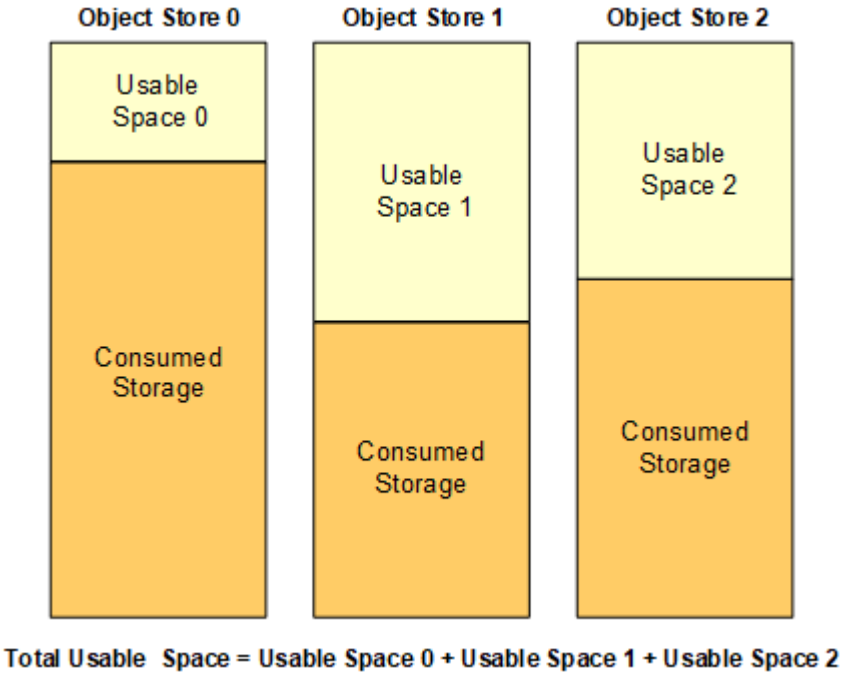
Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, consultare "Istruzioni per espandere StorageGRID".

Monitorare la capacità di storage per ciascun nodo di storage

Monitorare lo spazio totale utilizzabile per ciascun nodo di storage per garantire che il nodo disponga di spazio sufficiente per i nuovi dati dell'oggetto.

A proposito di questa attività

Lo spazio utilizzabile è la quantità di spazio di storage disponibile per memorizzare gli oggetti. Lo spazio totale utilizzabile per un nodo di storage viene calcolato sommando lo spazio disponibile in tutti gli archivi di oggetti all'interno del nodo.



Fasi

1. Selezionare **NODES** > ***Storage Node*** > **Storage**.

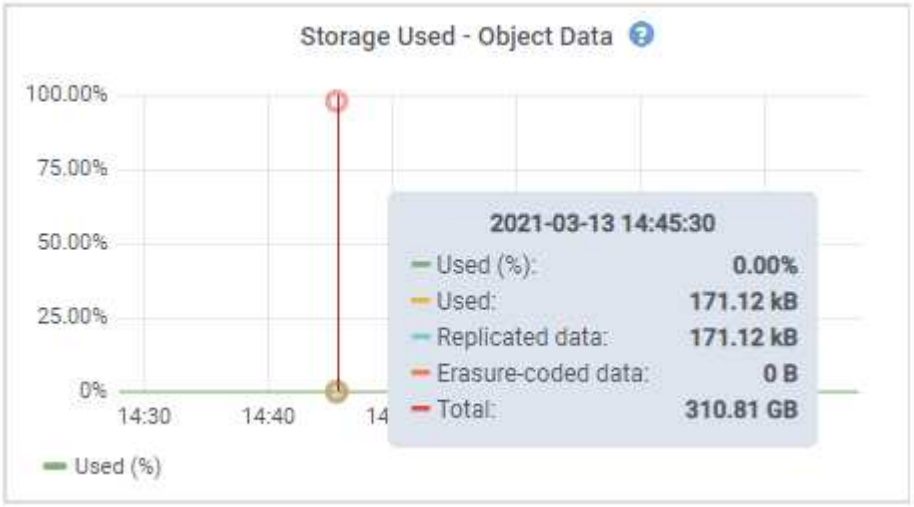
   Vengono visualizzati i grafici e le tabelle del nodo.

2. Posizionare il cursore sul grafico Storage Used - Object data (Storage utilizzato - dati oggetto).

   Vengono visualizzati i seguenti valori:

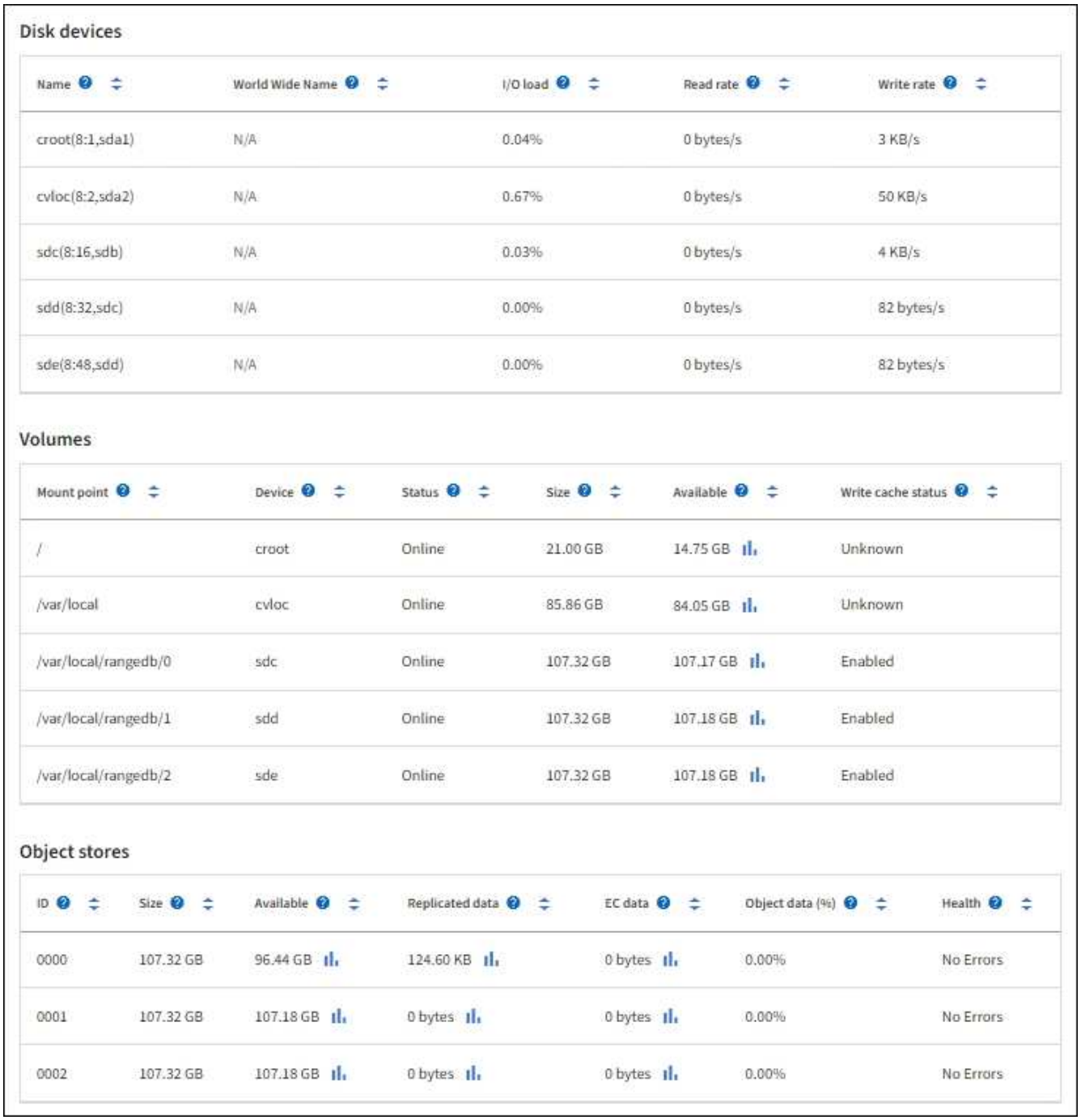
   - **Used (%)**: Percentuale dello spazio utilizzabile totale utilizzato per i dati dell'oggetto.
   - **Used**: Quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
   - **Dati replicati**: Stima della quantità di dati degli oggetti replicati su questo nodo, sito o griglia.
   - **Erasure-coded data**: Stima della quantità di dati dell'oggetto con codifica di cancellazione su questo nodo, sito o griglia.

◦ **Total**: Quantità totale di spazio utilizzabile su questo nodo, sito o griglia.
Il valore utilizzato è `storagegrid_storage_utilization_data_bytes` metrico.



3. Esaminare i valori disponibili nelle tabelle volumi e archivi di oggetti, sotto i grafici.

Per visualizzare i grafici di questi valori, fare clic sulle icone del grafico Nelle colonne disponibili.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

4. Monitorare i valori nel tempo per stimare il tasso di consumo dello spazio di storage utilizzabile.
5. Per mantenere le normali operazioni di sistema, aggiungere nodi di storage, aggiungere volumi di storage o archiviare i dati degli oggetti prima di consumare lo spazio utilizzabile.

   Quando si pianifica la tempistica di un'espansione, considerare quanto tempo sarà necessario per procurarsi e installare storage aggiuntivo.

   > Se la policy ILM utilizza la codifica erasure, è preferibile eseguire un'espansione quando i nodi di storage esistenti sono pieni al 70% circa per ridurre il numero di nodi da aggiungere.

   Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, consultare "Istruzioni per espandere StorageGRID".

Il "Storage dei dati a oggetti basso" L'avviso viene attivato quando rimane spazio insufficiente per memorizzare i dati dell'oggetto su un nodo di storage.

Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage

Monitorare l'utilizzo dei metadati per ciascun nodo di storage per garantire che rimanga spazio sufficiente per le operazioni essenziali del database. È necessario aggiungere nuovi nodi di storage in ogni sito prima che i metadati dell'oggetto superino il 100% dello spazio consentito per i metadati.

A proposito di questa attività

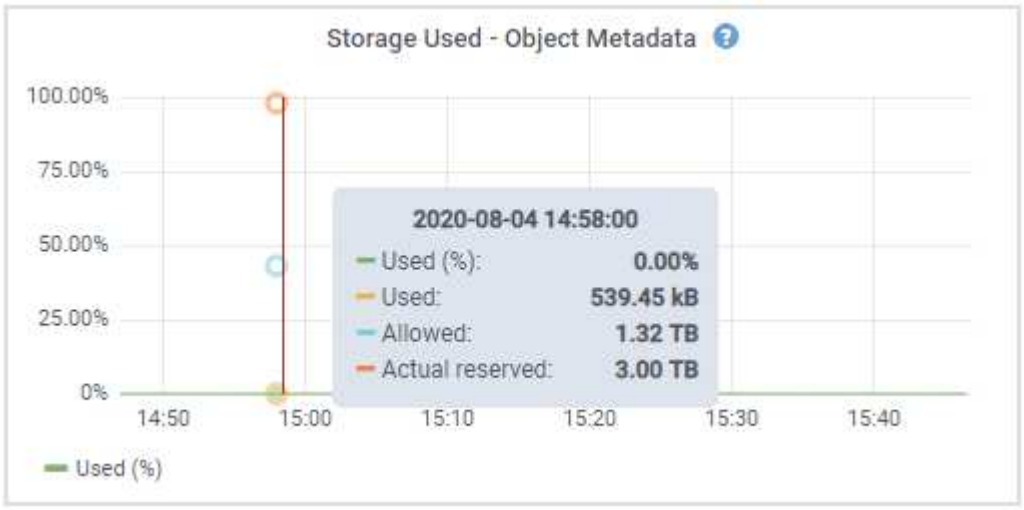
StorageGRID conserva tre copie dei metadati degli oggetti in ogni sito per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie vengono distribuite uniformemente su tutti i nodi di storage di ogni sito utilizzando lo spazio riservato ai metadati sul volume di storage 0 di ogni nodo di storage.

In alcuni casi, la capacità dei metadati degli oggetti della griglia potrebbe essere consumata più rapidamente della capacità dello storage a oggetti. Ad esempio, se in genere si acquisiscono grandi quantità di oggetti di piccole dimensioni, potrebbe essere necessario aggiungere nodi di storage per aumentare la capacità dei metadati anche se rimane sufficiente capacità di storage a oggetti.

Alcuni dei fattori che possono aumentare l'utilizzo dei metadati includono la dimensione e la quantità di tag e metadati dell'utente, il numero totale di parti in un caricamento multiparte e la frequenza delle modifiche alle posizioni di storage ILM.

Fasi

1. Selezionare **NODES** > ***Storage Node*** > **Storage**.
2. Posizionare il cursore sul grafico Storage Used - Object metadata (Storage utilizzato - metadati oggetto) per visualizzare i valori relativi a un orario specifico.



Utilizzato (%)

La percentuale dello spazio consentito per i metadati che è stato utilizzato su questo nodo di storage.

Metriche Prometheus: `storagegrid_storage_utilization_metadata_bytes` e. `storagegrid_storage_utilization_metadata_allowed_bytes`

Utilizzato

I byte dello spazio di metadati consentito che sono stati utilizzati su questo nodo di storage.

Metrica Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Consentito

Lo spazio consentito per i metadati dell'oggetto su questo nodo di storage. Per informazioni su come determinare questo valore per ciascun nodo di storage, vedere "Descrizione completa dello spazio consentito per i metadati".

Metrica Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Riservato

Lo spazio effettivo riservato ai metadati su questo nodo di storage. Include lo spazio consentito e lo spazio richiesto per le operazioni essenziali dei metadati. Per informazioni su come viene calcolato questo valore per ciascun nodo di storage, vedere "Descrizione completa dello spazio riservato effettivo per i metadati".

La metrica Prometheus verrà aggiunta in una release futura.

I valori totali di un sito o di un grid non includono nodi che non hanno riportato metriche per almeno cinque minuti, come i nodi offline.

3. Se il valore **utilizzato (%)** è pari o superiore al 70%, espandere il sistema StorageGRID aggiungendo nodi di storage a ciascun sito.

L'avviso **Low metadata storage** viene attivato quando il valore **used (%)** raggiunge determinate soglie. I risultati indesiderati possono verificarsi se i metadati dell'oggetto utilizzano più del 100% dello spazio consentito.

Quando si aggiungono nuovi nodi, il sistema ribilancia automaticamente i metadati degli oggetti in tutti i nodi di storage all'interno del sito. Vedere "Istruzioni per espandere un sistema StorageGRID".

Monitorare le previsioni di utilizzo dello spazio

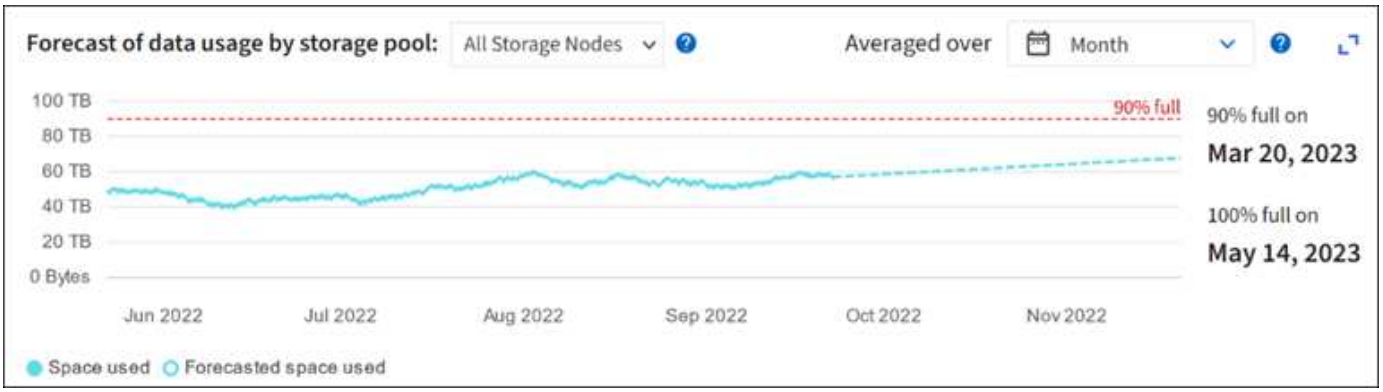
Monitorare le previsioni di utilizzo dello spazio per i dati utente e i metadati per stimare quando sarà necessario "espandere una griglia".

Se si nota che il tasso di consumo cambia nel tempo, selezionare un intervallo più breve dal menu a discesa **mediato su** per riflettere solo i modelli di acquisizione più recenti. Se si notano schemi stagionali, selezionare un intervallo più lungo.

Se si dispone di una nuova installazione StorageGRID, consentire l'accumulo di dati e metadati prima di valutare le previsioni di utilizzo dello spazio.

Fasi

1. Nella dashboard, selezionare **Storage**.
2. Visualizza le schede della dashboard, la previsione dell'utilizzo dei dati per pool di storage e la previsione dell'utilizzo dei metadati per sito.
3. Utilizza questi valori per valutare quando sarà necessario aggiungere nuovi nodi di storage per lo storage di dati e metadati.



Monitorare la gestione del ciclo di vita delle informazioni

Il sistema ILM (Information Lifecycle Management) fornisce la gestione dei dati per tutti gli oggetti memorizzati nella griglia. È necessario monitorare le operazioni ILM per capire se la griglia è in grado di gestire il carico corrente o se sono necessarie più risorse.

A proposito di questa attività

Il sistema StorageGRID gestisce gli oggetti applicando i criteri ILM attivi. I criteri ILM e le regole ILM associate determinano il numero di copie eseguite, il tipo di copie create, il luogo in cui vengono collocate e la durata di conservazione di ciascuna copia.

L'acquisizione di oggetti e altre attività correlate agli oggetti possono superare la velocità con cui StorageGRID può valutare ILM, causando la messa in coda degli oggetti le cui istruzioni di posizionamento ILM non possono essere soddisfatte quasi in tempo reale. È necessario controllare se StorageGRID è al passo con le azioni del client.

USA la scheda del pannello di controllo di Grid Manager

Fasi

Utilizzare la scheda ILM nella dashboard di Grid Manager per monitorare le operazioni ILM:

1. Accedi a Grid Manager.
2. Dal dashboard, selezionare la scheda ILM e annotare i valori sulla scheda coda ILM (oggetti) e sulla scheda velocità di valutazione ILM.

   Sono previsti picchi temporanei nella scheda della coda ILM (oggetti) sul dashboard. Ma se la coda continua ad aumentare e non diminuisce mai, la griglia necessita di più risorse per funzionare in modo efficiente: Più nodi di storage o, se il criterio ILM colloca gli oggetti in posizioni remote, una maggiore larghezza di banda della rete.

Utilizzare la pagina NODI

Fasi

Inoltre, esaminare le code ILM utilizzando la pagina **NODI**:

> I grafici della pagina **NODI** verranno sostituiti con le schede del dashboard corrispondenti in una futura versione di StorageGRID.

1. Selezionare **NODI**.

2. Selezionare ***grid name*** > **ILM**.
3. Posizionare il cursore sul grafico della coda ILM per visualizzare il valore dei seguenti attributi in un determinato momento:
   - **Oggetti accodati (da operazioni client)**: Il numero totale di oggetti in attesa di valutazione ILM a causa delle operazioni del client (ad esempio, acquisizione).
   - **Oggetti accodati (da tutte le operazioni)**: Il numero totale di oggetti in attesa di valutazione ILM.
   - **Scan rate (objects/sec)**: La velocità con cui gli oggetti nella griglia vengono sottoposti a scansione e messi in coda per ILM.
   - **Evaluation rate (objects/sec)**: La velocità corrente alla quale gli oggetti vengono valutati rispetto alla policy ILM nella griglia.
4. Nella sezione ILM Queue (coda ILM), esaminare i seguenti attributi.

   La sezione coda ILM è inclusa solo per la griglia. Queste informazioni non vengono visualizzate nella scheda ILM per un sito o un nodo di storage.

   - **Periodo di scansione - stimato**: Il tempo stimato per completare una scansione ILM completa di tutti gli oggetti.

     Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti.

   - **Riparazioni tentate**: Il numero totale di operazioni di riparazione degli oggetti per i dati replicati che sono stati tentati. Questo numero aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Le riparazioni ILM ad alto rischio hanno la priorità se la rete diventa occupata.

     La stessa riparazione dell'oggetto potrebbe aumentare di nuovo se la replica non è riuscita dopo la riparazione.

   Questi attributi possono essere utili quando si monitora l'avanzamento del ripristino del volume di Storage Node. Se il numero di riparazioni tentate ha smesso di aumentare ed è stata completata una scansione completa, la riparazione probabilmente è stata completata.

Monitorare le risorse di rete e di sistema

L'integrità e la larghezza di banda della rete tra nodi e siti, nonché l'utilizzo delle risorse da parte dei singoli nodi di rete, sono fondamentali per operazioni efficienti.

Monitorare le connessioni di rete e le performance

La connettività di rete e la larghezza di banda sono particolarmente importanti se il criterio ILM (Information Lifecycle Management) copia gli oggetti replicati tra siti o archivia oggetti con codifica di cancellazione utilizzando uno schema che fornisce la protezione dalla perdita di sito. Se la rete tra siti non è disponibile, la latenza di rete è troppo elevata o la larghezza di banda della rete è insufficiente, alcune regole ILM potrebbero non essere in grado di posizionare oggetti dove previsto. Questo può portare a errori di acquisizione (quando l'opzione di acquisizione rigorosa è selezionata per le regole ILM) o a scarse performance di acquisizione e backlog ILM.

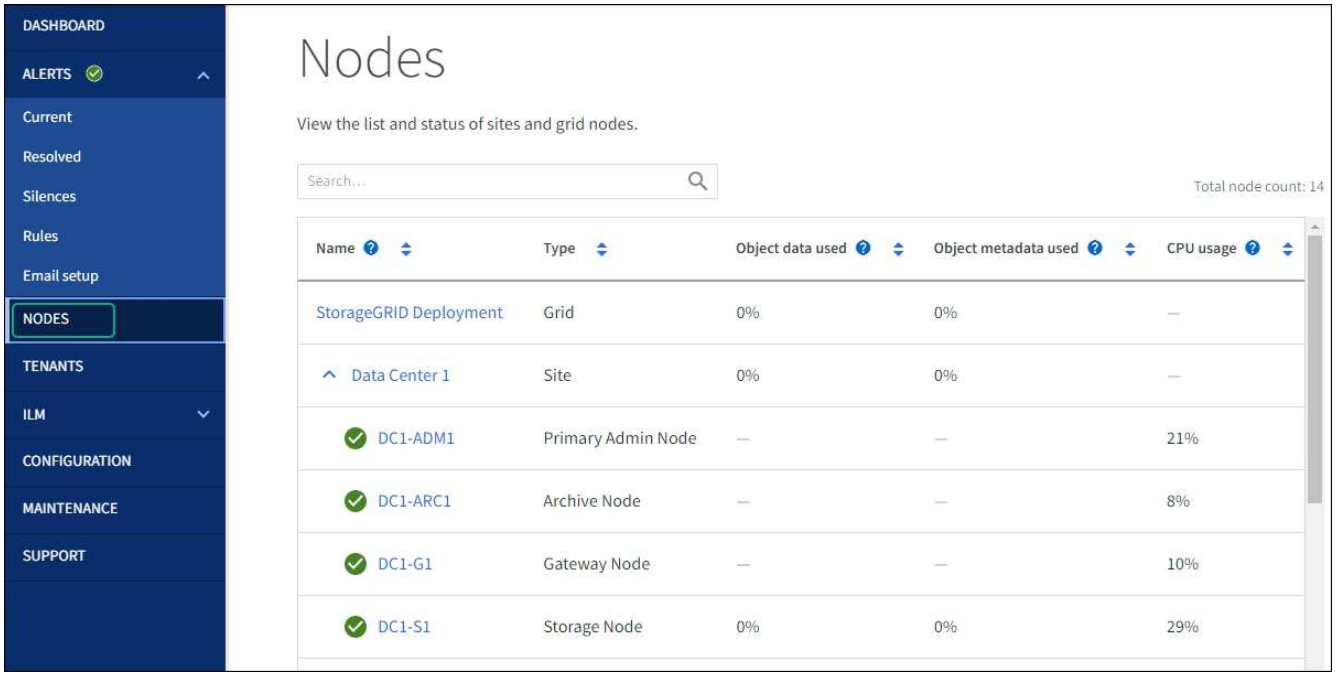
Utilizza Grid Manager per monitorare la connettività e le performance di rete, in modo da poter risolvere tempestivamente qualsiasi problema.

Inoltre, prendere in considerazione "creazione di criteri di classificazione del traffico di rete" in modo da poter monitorare il traffico relativo a tenant, bucket, subnet o endpoint del bilanciamento del carico specifici. È possibile impostare criteri di limitazione del traffico in base alle esigenze.

Fasi

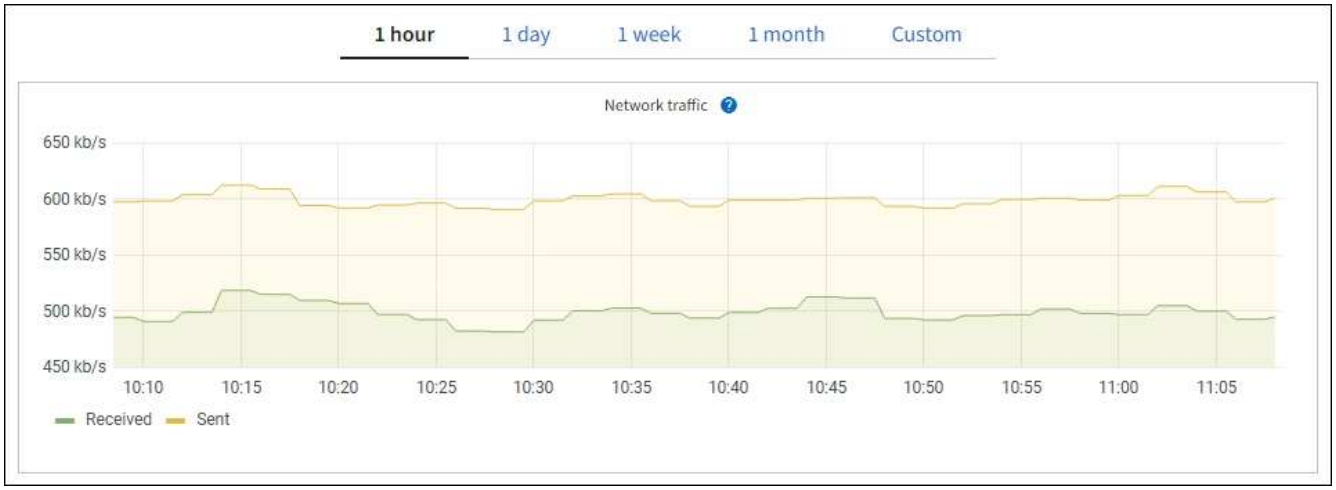
1. Selezionare **NODI**.

   Viene visualizzata la pagina nodi. Ciascun nodo della griglia viene elencato in formato tabella.

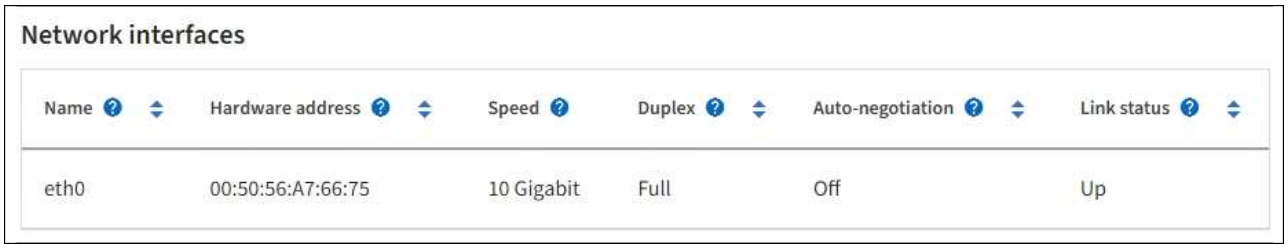


2. Selezionare il nome della griglia, un sito del data center specifico o un nodo della griglia, quindi selezionare la scheda **Network**.

   Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo per l'intera griglia, il sito del data center o il nodo.

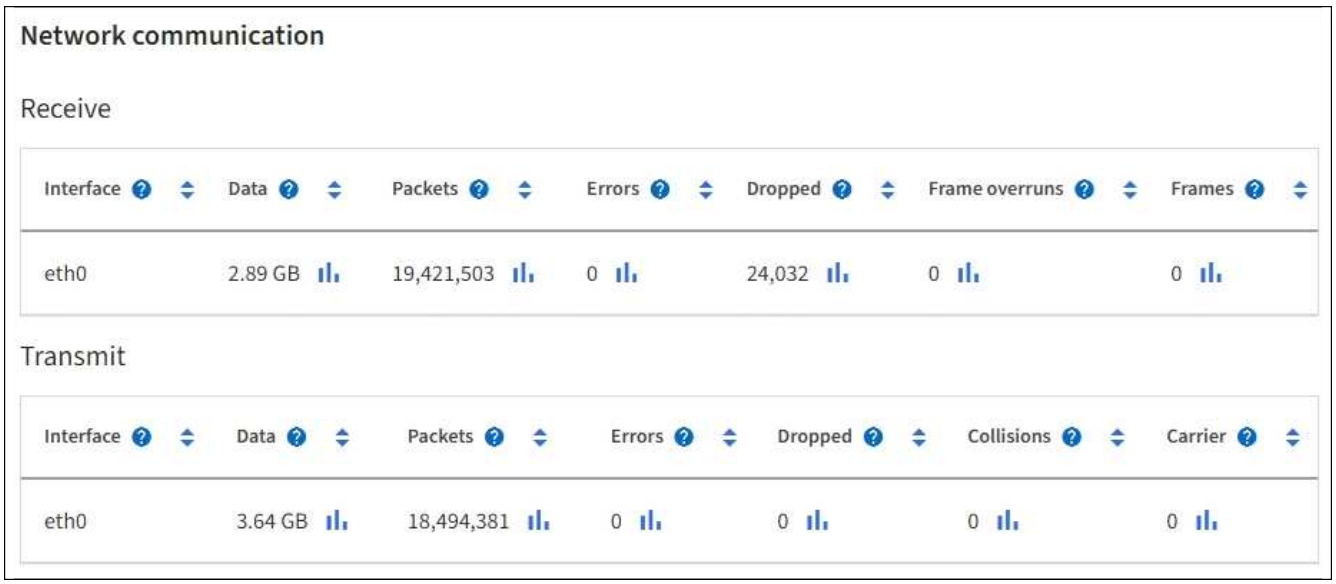


   a. Se è stato selezionato un nodo della griglia, scorrere verso il basso per esaminare la sezione **Network Interfaces** della pagina.



b. Per i nodi della griglia, scorrere verso il basso per esaminare la sezione **Network Communication** della pagina.

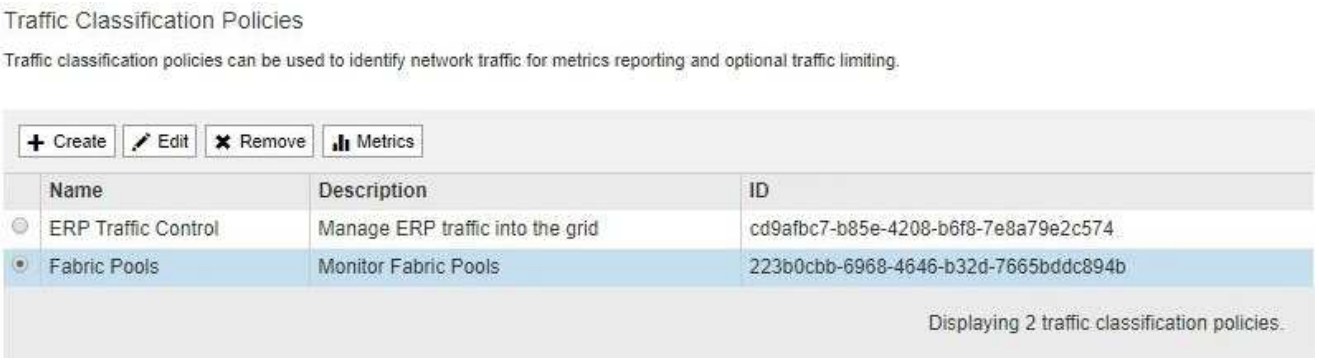
   Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, nonché altre metriche di ricezione e trasmissione.



3. Utilizza le metriche associate alle policy di classificazione del traffico per monitorare il traffico di rete.

   a. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

      Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.



   a. Per visualizzare i grafici che mostrano le metriche di rete associate a un criterio, selezionare il pulsante di opzione a sinistra del criterio, quindi fare clic su **metriche**.

   b. Esaminare i grafici per comprendere il traffico di rete associato alla policy.

      Se un criterio di classificazione del traffico è progettato per limitare il traffico di rete, analizzare la

frequenza con cui il traffico è limitato e decidere se il criterio continua a soddisfare le proprie esigenze. Di tanto in tanto, "modificare ogni policy di classificazione del traffico in base alle esigenze".

Informazioni correlate

"Visualizzare la scheda rete"

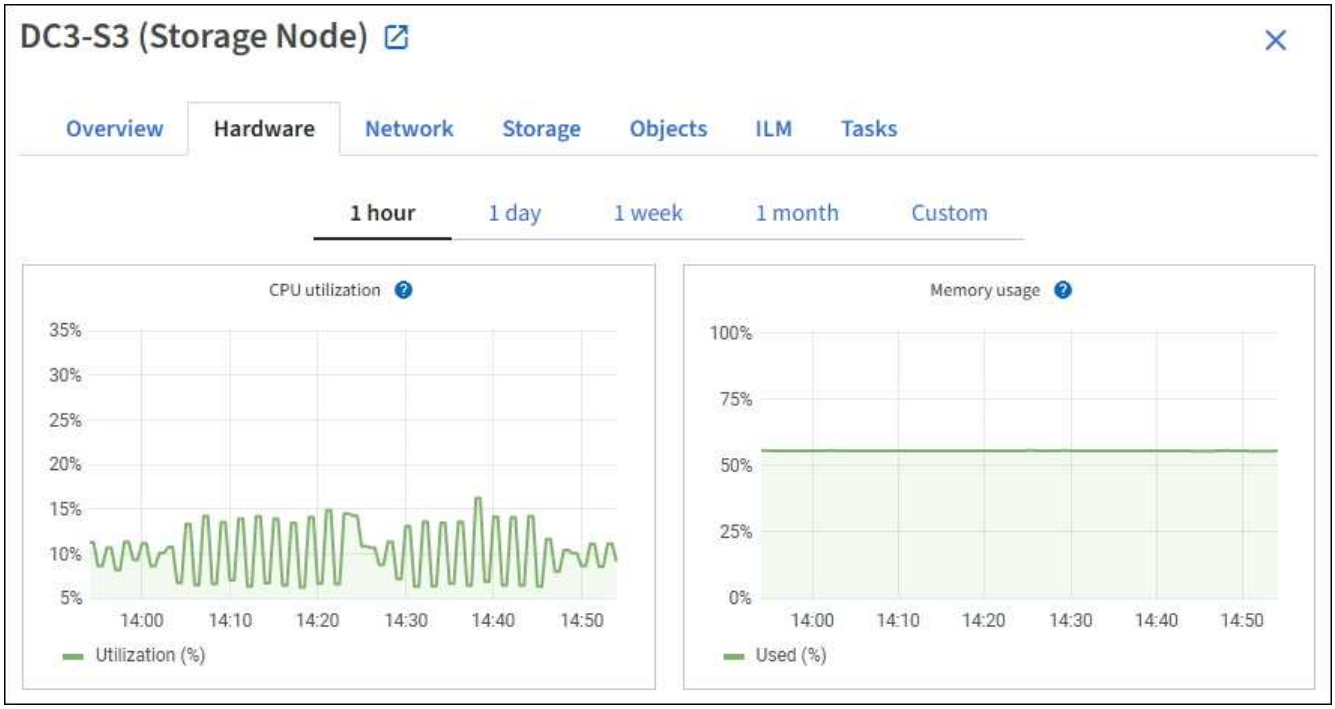
"Monitorare gli stati di connessione del nodo"

Monitorare le risorse a livello di nodo

Monitorare i singoli nodi di griglia per verificare i livelli di utilizzo delle risorse. Se i nodi sono costantemente sovraccarichi, potrebbero essere necessari più nodi per operazioni efficienti.

Fasi

1. Dalla pagina **NODES**, selezionare il nodo.
2. Selezionare la scheda **hardware** per visualizzare i grafici relativi all'utilizzo della CPU e della memoria.



3. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.
4. Se il nodo è ospitato su un'appliance di storage o su un'appliance di servizi, scorrere verso il basso per visualizzare le tabelle dei componenti. Lo stato di tutti i componenti deve essere "nominale". Esaminare i componenti che presentano qualsiasi altro stato.

Informazioni correlate

"Visualizza informazioni sui nodi di storage dell'appliance"

"Visualizza informazioni sui nodi di amministrazione dell'appliance e sui nodi gateway"

Monitorare l'attività del tenant

Tutte le attività dei client S3 e Swift sono associate agli account del tenant StorageGRID. È possibile utilizzare Grid Manager per monitorare l'utilizzo dello storage o il traffico di rete di tutti i tenant o di uno specifico tenant. È possibile utilizzare il registro di controllo o le dashboard Grafana per ottenere informazioni più dettagliate sull'utilizzo di StorageGRID da parte dei tenant.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Accesso root o autorizzazione account tenant".

Visualizza tutti i tenant

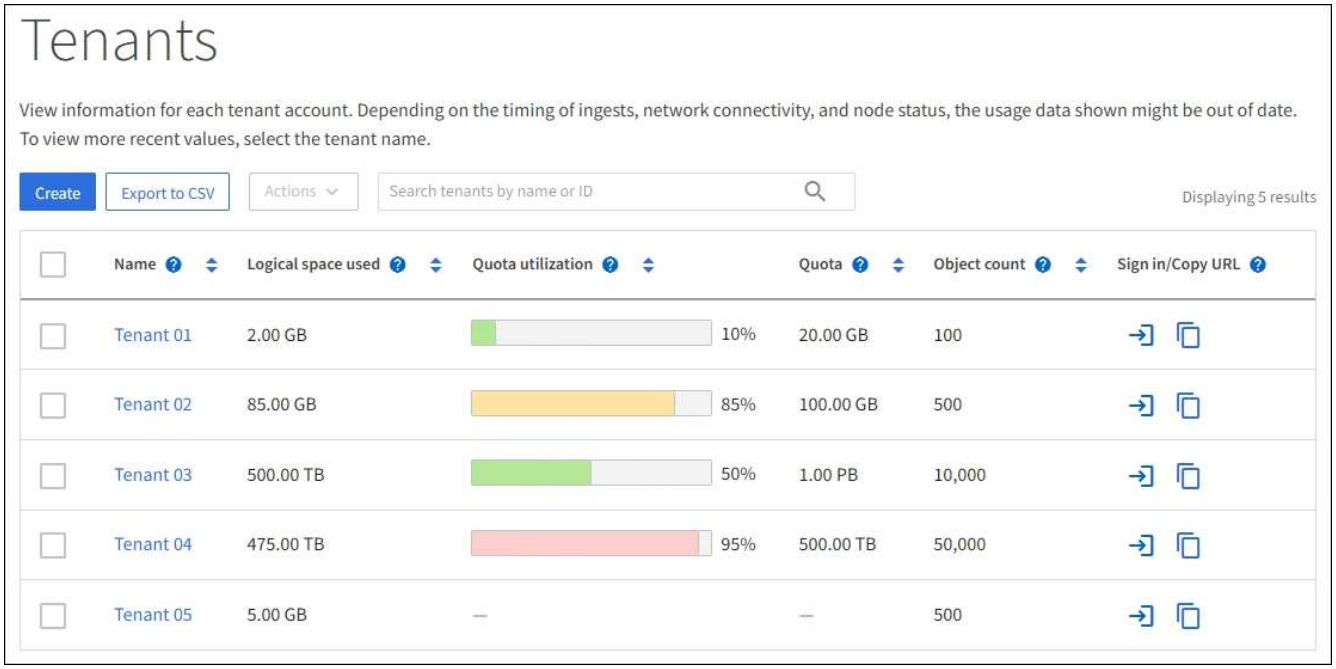
La pagina tenant mostra le informazioni di base per tutti gli account tenant correnti.

Fasi

1. Selezionare **TENANT**.
2. Esaminare le informazioni visualizzate nelle pagine del tenant.

   Per ogni tenant vengono elencati lo spazio logico utilizzato, l'utilizzo della quota, la quota e il numero di oggetti. Se non viene impostata una quota per un tenant, i campi relativi all'utilizzo della quota e alla quota contengono un trattino (& 8212;).

   > I valori dello spazio utilizzato sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi.



3. Se lo si desidera, accedere a un account tenant selezionando il collegamento di accesso Nella colonna **URL di accesso/copia**.
4. Se si desidera, copiare l'URL della pagina di accesso del tenant selezionando il collegamento URL della copia Nella colonna **URL di accesso/copia**.

5. In alternativa, selezionare **Export to CSV** (Esporta in CSV) per visualizzare ed esportare un `.csv` file contenente i valori di utilizzo per tutti i tenant.

   Viene richiesto di aprire o salvare `.csv` file.

   Il contenuto di `.csv` il file è simile al seguente esempio:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

   È possibile aprire `.csv` file in un'applicazione per fogli di calcolo o utilizzarlo in automazione.

6. Se non sono presenti oggetti nell'elenco, selezionare **azioni** > **Elimina** per rimuovere uno o più tenant. Vedere "Elimina account tenant".

   Non puoi rimuovere un account tenant se l'account include bucket o container.

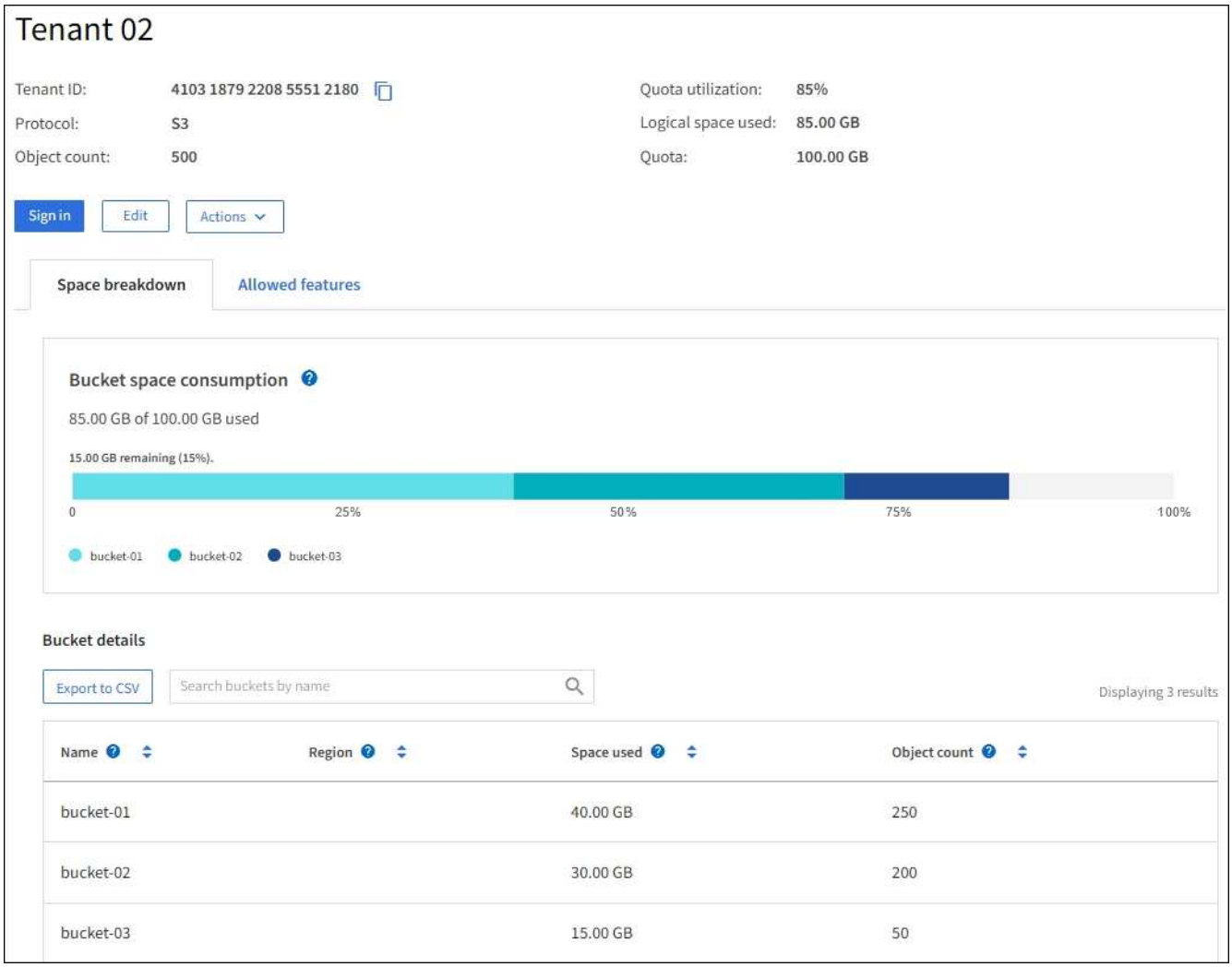
Visualizzare un tenant specifico

È possibile visualizzare i dettagli di un tenant specifico.

Fasi

1. Selezionare il nome del tenant dalla pagina tenant.

   Viene visualizzata la pagina dei dettagli del tenant.



2. Esaminare la panoramica del tenant nella parte superiore della pagina.

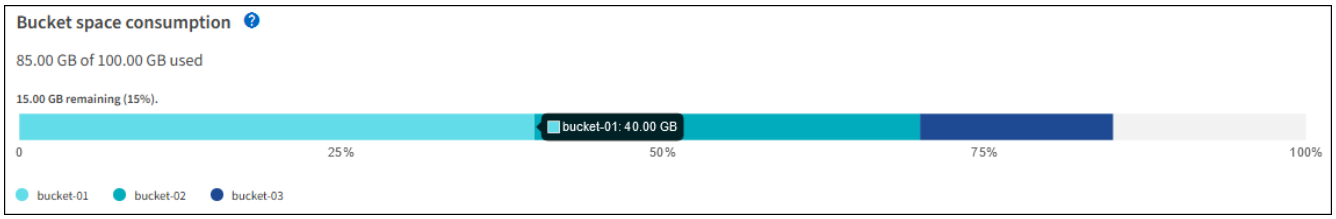
   Questa sezione della pagina dei dettagli fornisce informazioni riepilogative per il tenant, tra cui il numero di oggetti del tenant, l'utilizzo della quota, lo spazio logico utilizzato e l'impostazione della quota.

3. Dalla scheda **Space disruption** (suddivisione spazio), esaminare il grafico **Space Consumption** (consumo spazio).

   Questo grafico mostra il consumo totale di spazio per tutti i bucket S3 (o container Swift) del tenant.

   Se è stata impostata una quota per questo tenant, la quantità di quota utilizzata e rimanente viene visualizzata in testo (ad esempio, `85.00 GB of 100 GB used`). Se non è stata impostata alcuna quota, il tenant ha una quota illimitata e il testo include solo una quantità di spazio utilizzato (ad esempio, `85.00 GB used`). Il grafico a barre mostra la percentuale di quota in ciascun bucket o container. Se il tenant ha superato la quota di storage di oltre l'1% e di almeno 1 GB, il grafico mostra la quota totale e la quantità in eccesso.

   È possibile posizionare il cursore sul grafico a barre per visualizzare lo storage utilizzato da ciascun bucket o container. È possibile posizionare il cursore sul segmento di spazio libero per visualizzare la quantità di spazio rimanente.



L'utilizzo delle quote si basa su stime interne e in alcuni casi potrebbe essere superato. Ad esempio, StorageGRID controlla la quota quando un tenant avvia il caricamento degli oggetti e rifiuta le nuove ricerche se il tenant ha superato la quota. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente quando determina se la quota è stata superata. Se gli oggetti vengono eliminati, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti fino a quando l'utilizzo della quota non viene ricalcolato. I calcoli di utilizzo delle quote possono richiedere 10 minuti o più.

L'utilizzo della quota di un tenant indica la quantità totale di dati oggetto che il tenant ha caricato in StorageGRID (dimensione logica). L'utilizzo della quota non rappresenta lo spazio utilizzato per memorizzare le copie di tali oggetti e dei relativi metadati (dimensione fisica).

È possibile attivare la regola di avviso **quota elevata utilizzo tenant** per determinare se i tenant consumano le proprie quote. Se attivato, questo avviso viene attivato quando un tenant utilizza il 90% della propria quota. Per istruzioni, vedere "Modificare le regole degli avvisi".

4. Dalla scheda **Space breakdown** (suddivisione spazio), rivedere i **Bucket details** (Dettagli bucket).

   Questa tabella elenca i bucket S3 (o container Swift) per il tenant. Lo spazio utilizzato è la quantità totale di dati dell'oggetto nel bucket o nel container. Questo valore non rappresenta lo spazio di storage richiesto per le copie ILM e i metadati degli oggetti.

5. Facoltativamente, selezionare **Export to CSV** (Esporta in CSV) per visualizzare ed esportare un file .csv contenente i valori di utilizzo per ciascun bucket o container.

   Il contenuto di un singolo tenant S3 `.csv` il file è simile al seguente esempio:

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   È possibile aprire `.csv` file in un'applicazione per fogli di calcolo o utilizzarlo in automazione.

6. Se si desidera, selezionare la scheda **funzioni consentite** per visualizzare un elenco delle autorizzazioni e delle funzionalità attivate per il tenant. Vedere "Modificare l'account tenant" se è necessario modificare una di queste impostazioni.
7. Se il tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, selezionare la scheda **federazione griglia** per ulteriori informazioni sulla connessione.

   Vedere "Che cos'è la federazione di griglie?" e. "Gestire i tenant consentiti per la federazione di grid".

Visualizzare il traffico di rete

Se per un tenant sono in vigore criteri di classificazione del traffico, esaminare il traffico di rete per tale tenant.

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.

2. Esaminare l'elenco delle policy per identificare quelle applicabili a un tenant specifico.
3. Per visualizzare le metriche associate a un criterio, selezionare il pulsante di opzione a sinistra del criterio e selezionare **metriche**.
4. Analizzare i grafici per determinare la frequenza con cui il criterio limita il traffico e se è necessario modificare il criterio.

Vedere "Gestire le policy di classificazione del traffico" per ulteriori informazioni.

Utilizzare il registro di controllo

Facoltativamente, è possibile utilizzare il registro di audit per un monitoraggio più granulare delle attività di un tenant.

Ad esempio, è possibile monitorare i seguenti tipi di informazioni:

- Operazioni client specifiche, come PUT, GET o DELETE
- Dimensioni degli oggetti
- La regola ILM applicata agli oggetti
- L'IP di origine delle richieste del client

I registri di audit vengono scritti in file di testo che è possibile analizzare utilizzando lo strumento di analisi dei log scelto. Ciò consente di comprendere meglio le attività del cliente o di implementare sofisticati modelli di chargeback e fatturazione.

Vedere "Esaminare i registri di audit" per ulteriori informazioni.

Utilizza le metriche Prometheus

Facoltativamente, utilizza le metriche Prometheus per generare report sull'attività del tenant.

- In Grid Manager, selezionare **SUPPORT** > **Tools** > **Metrics**. È possibile utilizzare dashboard esistenti, ad esempio S3 Overview, per esaminare le attività del client.

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

- Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**. È possibile utilizzare le metriche nella sezione metriche dell'API Grid Management per creare regole di avviso e dashboard personalizzati per l'attività del tenant.

Vedere "Rivedere le metriche di supporto" per ulteriori informazioni.

Monitoraggio di operazioni client S3 e Swift

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

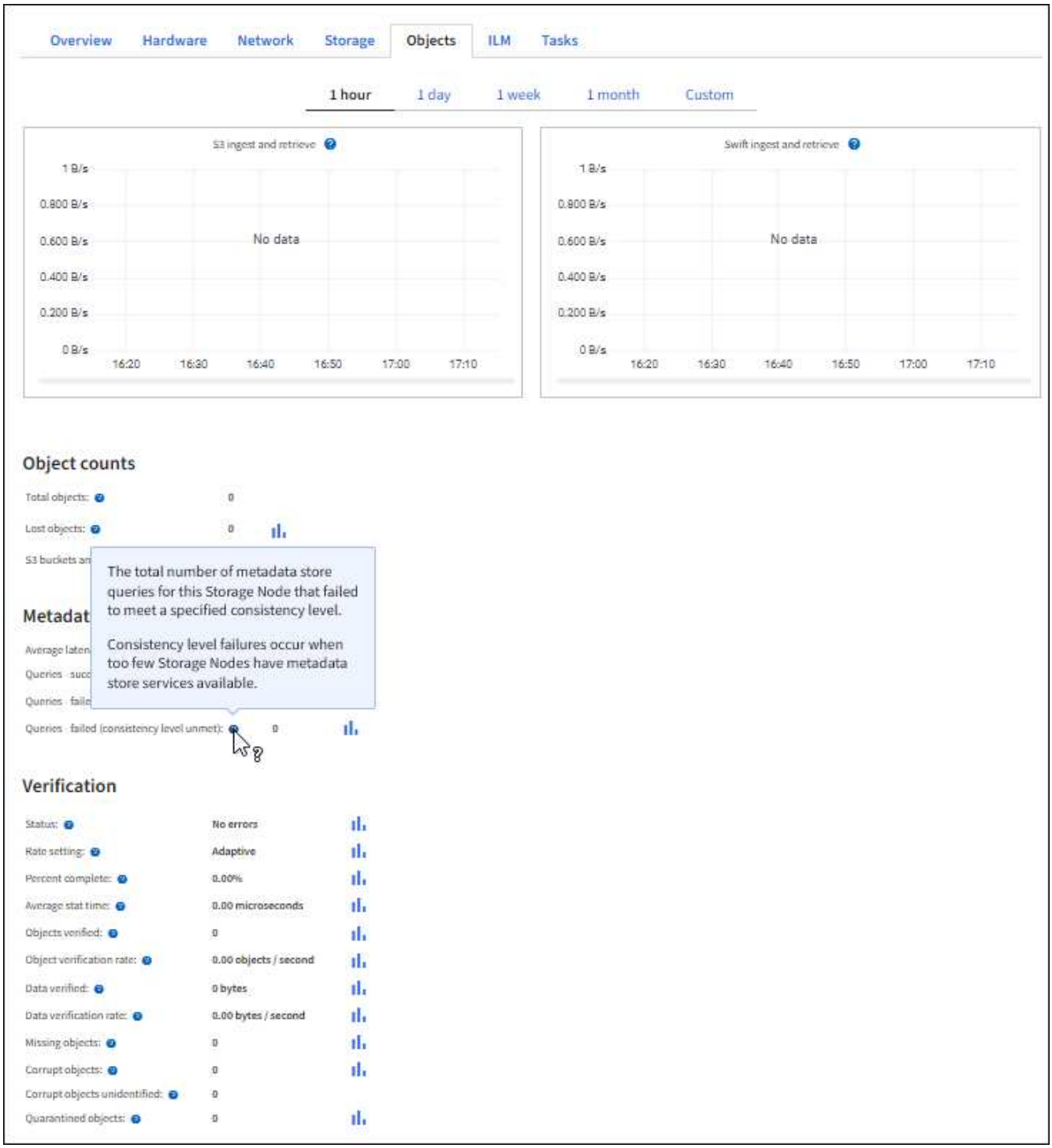
Fasi

1. Dalla dashboard, selezionare la scheda **prestazioni**.
2. Fai riferimento ai grafici S3 e Swift, che riassumono il numero di operazioni client eseguite dai nodi storage e il numero di richieste API ricevute dai nodi storage durante l'intervallo di tempo selezionato.
3. Selezionare **NODI** per accedere alla pagina nodi.
4. Dalla home page dei nodi (livello griglia), selezionare la scheda **oggetti**.

   Il grafico mostra le velocità di acquisizione e recupero di S3 e Swift per l'intero sistema StorageGRID in byte al secondo e la quantità di dati acquisiti o recuperati. È possibile selezionare un intervallo di tempo o applicare un intervallo personalizzato.

5. Per visualizzare le informazioni relative a un determinato nodo di archiviazione, selezionare il nodo dall'elenco a sinistra e selezionare la scheda **oggetti**.

   Il grafico mostra le velocità di acquisizione e recupero per il nodo. Questa scheda include inoltre metriche per il numero di oggetti, le query sui metadati e le operazioni di verifica.



Monitorare le operazioni di bilanciamento del carico

Se si utilizza un bilanciamento del carico per gestire le connessioni client a StorageGRID, è necessario monitorare le operazioni di bilanciamento del carico dopo aver configurato il sistema inizialmente e dopo aver apportato modifiche alla configurazione o aver eseguito un'espansione.

A proposito di questa attività

È possibile utilizzare il servizio Load Balancer sui nodi Admin o Gateway o un bilanciamento del carico esterno di terze parti per distribuire le richieste dei client su più nodi di storage.

Dopo aver configurato il bilanciamento del carico, è necessario confermare che le operazioni di recupero e acquisizione degli oggetti vengono distribuite uniformemente tra i nodi di storage. Le richieste distribuite in modo uniforme garantiscono che StorageGRID rimanga reattivo alle richieste dei client sotto carico e possa contribuire a mantenere le performance dei client.

Se è stato configurato un gruppo ad alta disponibilità (ha) di nodi gateway o nodi di amministrazione in modalità Active-backup, solo un nodo del gruppo distribuisce attivamente le richieste dei client.

Per ulteriori informazioni, vedere "Configurare le connessioni client S3 e Swift".

Fasi

1. Se i client S3 o Swift si connettono utilizzando il servizio Load Balancer, verificare che i nodi Admin o Gateway distribuiscono attivamente il traffico come previsto:
   a. Selezionare **NODI**.
   b. Selezionare un nodo gateway o un nodo amministratore.
   c. Nella scheda **Overview**, verificare se un'interfaccia di nodo è in un gruppo ha e se l'interfaccia di nodo ha il ruolo di primario.

      I nodi con il ruolo di primario e i nodi che non fanno parte di un gruppo ha devono distribuire attivamente le richieste ai client.

   d. Per ogni nodo che deve distribuire attivamente le richieste client, selezionare "Scheda bilanciamento del carico".
   e. Esaminare il grafico del traffico di richiesta del bilanciamento del carico dell'ultima settimana per assicurarsi che il nodo stia distribuendo attivamente le richieste.

      I nodi di un gruppo ha con backup attivo potrebbero assumere di tanto in tanto il ruolo di backup. Durante questo periodo, i nodi non distribuiscono le richieste dei client.

   f. Esaminare il grafico del tasso di richiesta in entrata del bilanciamento del carico dell'ultima settimana per esaminare il throughput degli oggetti del nodo.
   g. Ripetere questi passaggi per ogni nodo amministratore o nodo gateway nel sistema StorageGRID.
   h. Facoltativamente, utilizzare le policy di classificazione del traffico per visualizzare un'analisi più dettagliata del traffico fornito dal servizio Load Balancer.
2. Verificare che queste richieste vengano distribuite uniformemente ai nodi di storage.
   a. Selezionare ***Storage Node*** > **LDR** > **HTTP**.
   b. Esaminare il numero di **sessioni in entrata attualmente stabilite**.
   c. Ripetere l'operazione per ogni nodo di storage nella griglia.

      Il numero di sessioni deve essere approssimativamente uguale in tutti i nodi di storage.

Monitorare le connessioni a federazione di griglie

È possibile monitorare le informazioni di base su tutti "connessioni a federazione di griglie", Informazioni dettagliate su una connessione specifica o metriche Prometheus sulle operazioni di replica cross-grid. È possibile monitorare una connessione da entrambe le griglie.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su una delle griglie utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root" per la griglia a cui si è effettuato l'accesso.

Visualizza tutte le connessioni

La pagina Grid Federation mostra informazioni di base su tutte le connessioni a federazione di griglie e su tutti gli account tenant autorizzati a utilizzare le connessioni a federazione di griglie.

Fasi

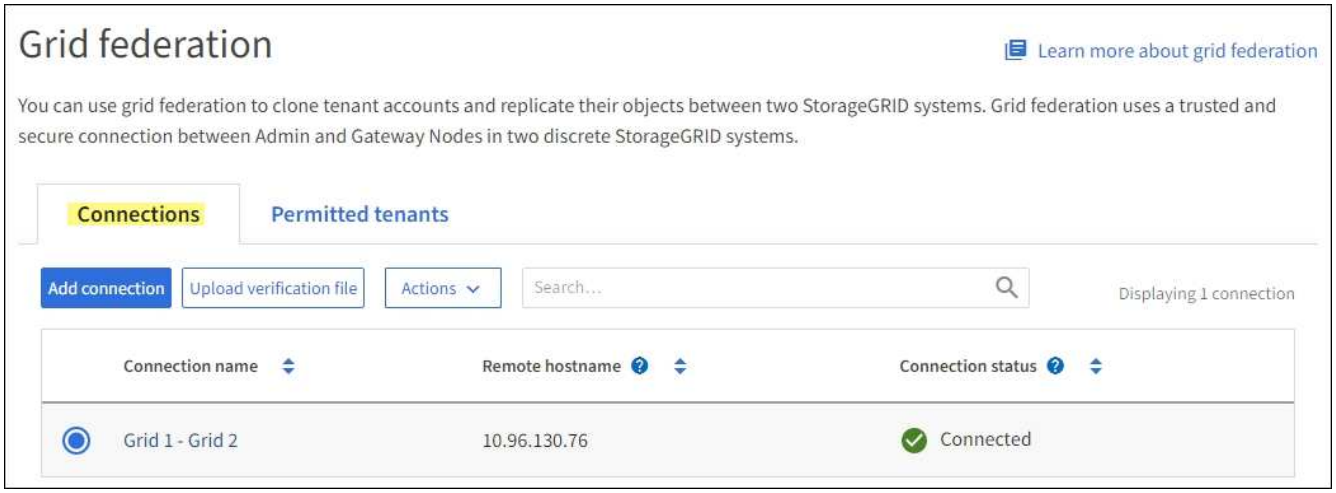
1. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.

   Viene visualizzata la pagina Grid Federation.

2. Per visualizzare le informazioni di base su tutte le connessioni in questa griglia, selezionare la scheda **connessioni**.

   Da questa scheda è possibile:

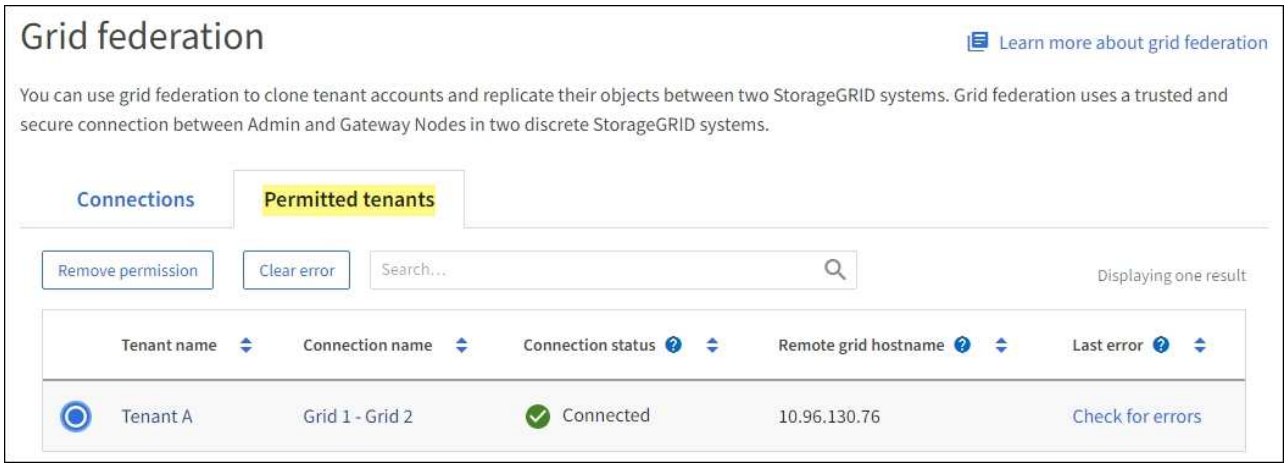
   - "Creare una nuova connessione".
   - Selezionare una connessione esistente a. "modifica o verifica".



3. Per visualizzare le informazioni di base per tutti gli account tenant di questa griglia che dispongono dell'autorizzazione **Usa connessione federazione griglia**, selezionare la scheda **tenant consentiti**.

   Da questa scheda è possibile:

   - "Visualizza la pagina dei dettagli per ciascun tenant consentito".
   - Visualizzare la pagina dei dettagli per ciascuna connessione. Vedere Visualizzare una connessione specifica.
   - Selezionare un tenant consentito e scegliere "rimuovere l'autorizzazione".
   - Verificare la presenza di errori di replica tra griglie e cancellare l'ultimo errore, se presente. Vedere "Risolvere i problemi relativi agli errori di federazione della griglia".



Visualizza una connessione specifica

È possibile visualizzare i dettagli di una connessione a federazione di griglie specifica.

Fasi

1. Selezionare una delle schede dalla pagina Grid Federation, quindi selezionare il nome della connessione dalla tabella.

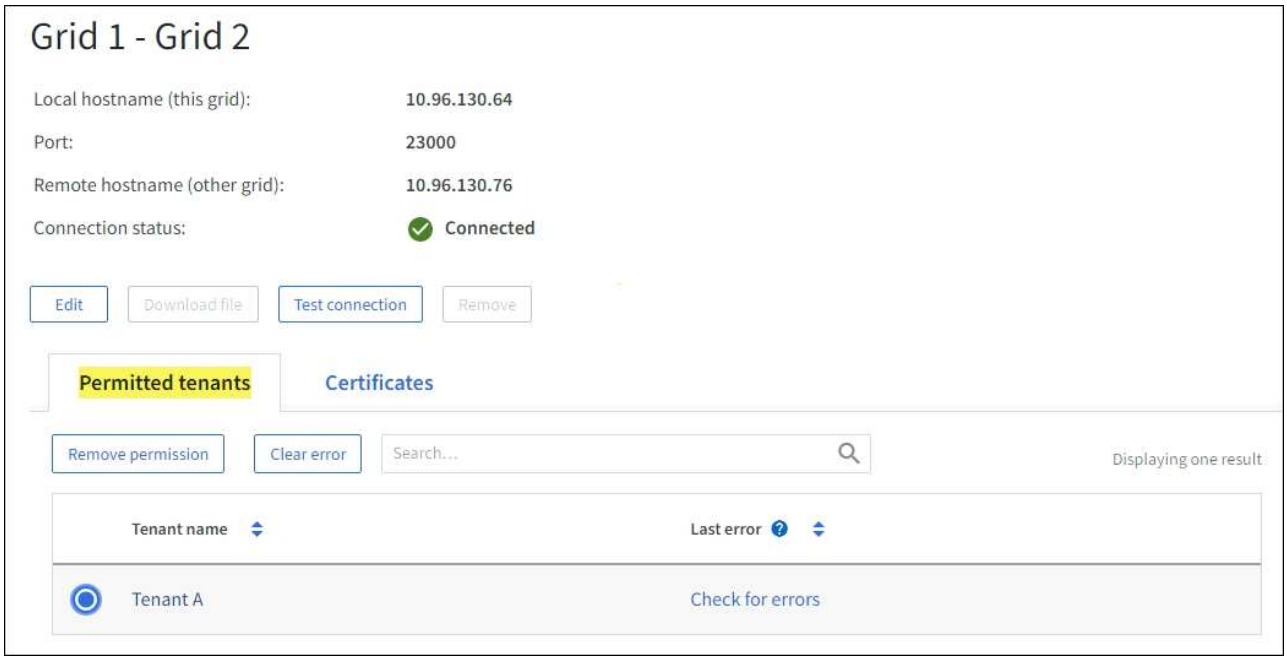
   Dalla pagina dei dettagli per la connessione, è possibile:

   - Consultare le informazioni di base sullo stato della connessione, inclusi i nomi host locali e remoti, la porta e lo stato della connessione.
   - Selezionare una connessione a. "modifica, verifica o rimozione".

2. Quando si visualizza una connessione specifica, selezionare la scheda **tenant consentiti** per visualizzare i dettagli relativi ai tenant consentiti per la connessione.

   Da questa scheda è possibile:

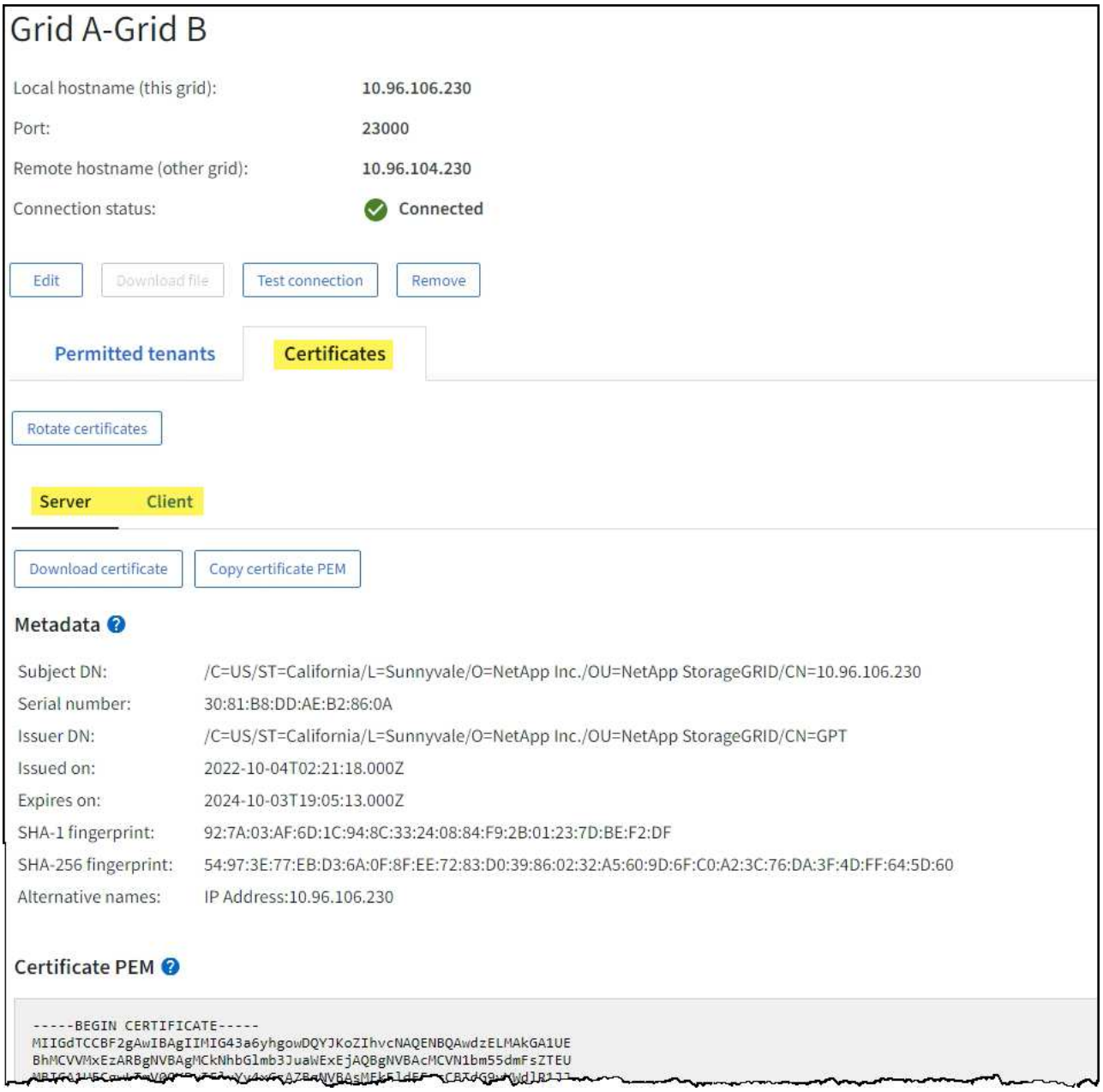
   - "Visualizza la pagina dei dettagli per ciascun tenant consentito".
   - "Rimuovere l'autorizzazione di un tenant" per utilizzare la connessione.
   - Verificare la presenza di errori di replica tra griglie e cancellare l'ultimo errore. Vedere "Risolvere i problemi relativi agli errori di federazione della griglia".



3. Quando si visualizza una connessione specifica, selezionare la scheda **certificati** per visualizzare i certificati server e client generati dal sistema per questa connessione.

   Da questa scheda è possibile:

   - "Ruotare i certificati di connessione".
   - Selezionare **Server** o **Client** per visualizzare o scaricare il certificato associato o copiare il PEM del certificato.



Analisi delle metriche di replica cross-grid

Puoi utilizzare la dashboard di replica cross-grid di Grafana per visualizzare le metriche Prometheus sulle operazioni di replica cross-grid sul tuo grid.

Fasi

1. Da Grid Manager, selezionare **SUPPORT** > **Tools** > **Metrics**.

   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. Vedere l'elenco di "Metriche Prometheus comunemente utilizzate".

2. Nella sezione Grafana della pagina, selezionare **Cross Grid Replication**.

   Per istruzioni dettagliate, vedere "Rivedere le metriche di supporto".

3. Per riprovare la replica degli oggetti che non sono riusciti a replicare, vedere "Identificare e riprovare le operazioni di replica non riuscite".

Monitorare la capacità di archiviazione

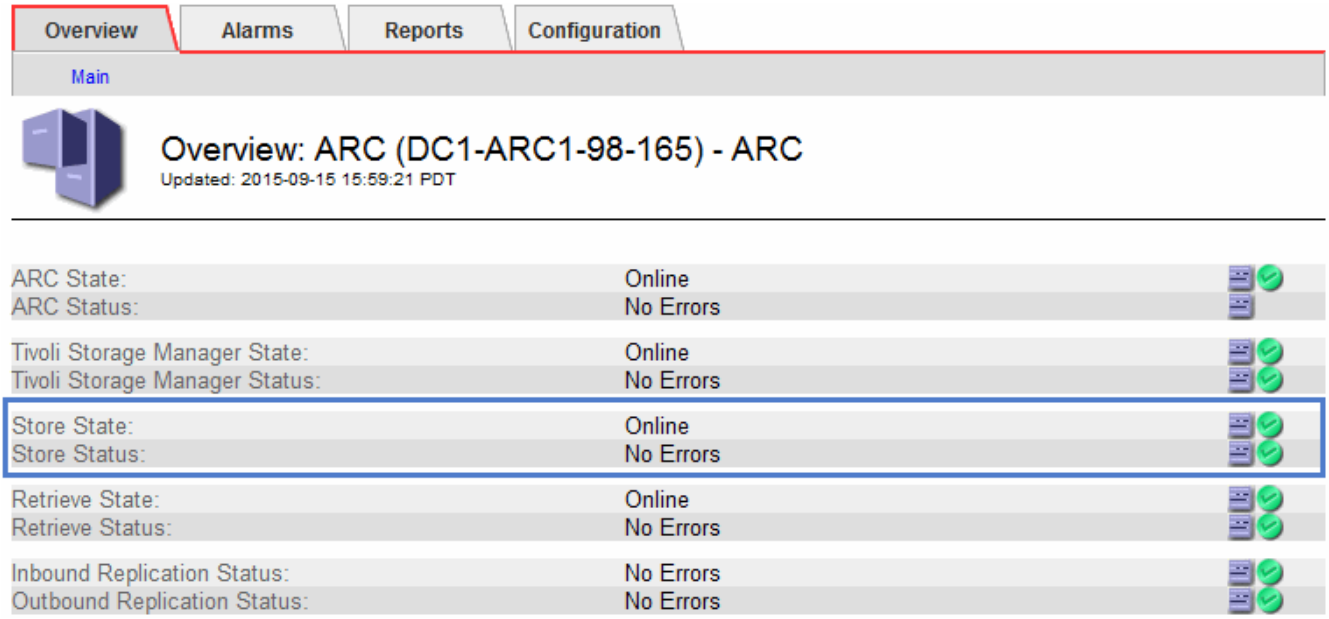
Non è possibile monitorare direttamente la capacità di un sistema storage di archiviazione esterno attraverso il sistema StorageGRID. Tuttavia, è possibile controllare se il nodo di archiviazione può ancora inviare i dati degli oggetti alla destinazione di archiviazione, il che potrebbe indicare che è necessaria un'espansione dei supporti di archiviazione.

A proposito di questa attività

È possibile monitorare il componente Store per verificare se il nodo di archiviazione è ancora in grado di inviare i dati dell'oggetto al sistema di storage di archiviazione di destinazione. L'allarme Store Failures (ARVF) potrebbe anche indicare che il sistema storage di archiviazione di destinazione ha raggiunto la capacità e non può più accettare i dati degli oggetti.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC> Overview> Main**.
3. Controllare gli attributi Store state (Stato archiviazione) e Store Status (Stato archiviazione) per verificare che il componente Store sia online senza errori.



Un componente offline Store o un componente con errori potrebbe indicare che il sistema storage di archiviazione di destinazione non può più accettare dati a oggetti perché ha raggiunto la capacità.

Avvisi e allarmi

Gestire avvisi e allarmi: Panoramica

Il sistema di allerta StorageGRID è progettato per informare l'utente sui problemi operativi che richiedono attenzione. Il sistema di allarme legacy è obsoleto.

Sistema di allerta

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 fornisce un'interfaccia di facile utilizzo per rilevare, valutare e risolvere i problemi.

Gli avvisi vengono attivati a livelli di severità specifici quando le condizioni delle regole di avviso vengono valutate come vere. Quando viene attivato un avviso, si verificano le seguenti azioni:

- Sul dashboard di Grid Manager viene visualizzata un'icona di severità degli avvisi e il numero di avvisi correnti viene incrementato.
- L'avviso viene visualizzato nella pagina di riepilogo **NODI** e nella scheda **NODI** > ***nodo*** > **Panoramica**.
- Viene inviata una notifica e-mail, presupponendo che sia stato configurato un server SMTP e che siano stati forniti indirizzi e-mail per i destinatari.
- Viene inviata una notifica SNMP (Simple Network Management Protocol), presupponendo che l'agente SNMP StorageGRID sia stato configurato.

Sistema di allarme legacy

Analogamente agli avvisi, gli allarmi vengono attivati a livelli di severità specifici quando gli attributi raggiungono valori di soglia definiti. Tuttavia, a differenza degli avvisi, vengono attivati molti allarmi per gli eventi che è possibile ignorare in modo sicuro, il che potrebbe causare un numero eccessivo di notifiche e-mail o SNMP.

> Il sistema di allarme è obsoleto e verrà rimosso in una versione futura. Se si utilizzano ancora allarmi legacy, è necessario passare completamente al sistema di allarme il prima possibile.

Quando viene attivato un allarme, si verificano le seguenti azioni:

- L'allarme viene visualizzato nella pagina **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.
- Viene inviata una notifica via email, a condizione che sia stato configurato un server SMTP e siano state configurate una o più mailing list.
- È possibile che venga inviata una notifica SNMP, purché sia stato configurato l'agente SNMP di StorageGRID. (Le notifiche SNMP non vengono inviate per tutti gli allarmi o le gravità degli allarmi).

Confrontare avvisi e allarmi

Esistono diverse analogie tra il sistema di allarme e il sistema di allarme legacy, ma il sistema di allarme offre notevoli vantaggi ed è più semplice da utilizzare.

Fare riferimento alla seguente tabella per informazioni su come eseguire operazioni simili.

	Avvisi	Allarmi (sistema precedente)
Come si visualizzano gli avvisi o gli allarmi attivi?	• Selezionare il collegamento **Current alerts** (Avvisi correnti) nella dashboard. • Selezionare l'avviso nella pagina **NODI** > **Panoramica**. • Selezionare **ALERTS** > **current**. "Visualizzare gli avvisi correnti"	Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**. "Gestire gli allarmi (sistema legacy)"
Cosa causa l'attivazione di un allarme o di un allarme?	Gli avvisi vengono attivati quando un'espressione Prometheus in una regola di avviso valuta true per la condizione di attivazione e la durata specifiche. "Visualizzare le regole degli avvisi"	Gli allarmi vengono attivati quando un attributo StorageGRID raggiunge un valore di soglia. "Gestire gli allarmi (sistema legacy)"
Se viene attivato un allarme o un allarme, come si risolve il problema sottostante?	Le azioni consigliate per un avviso sono incluse nelle notifiche e-mail e sono disponibili nelle pagine Avvisi di Grid Manager. Come richiesto, ulteriori informazioni sono fornite nella documentazione di StorageGRID. "Riferimenti agli avvisi"	Per informazioni su un allarme, selezionare il nome dell'attributo oppure cercare un codice di allarme nella documentazione di StorageGRID. "Riferimento allarmi (sistema legacy)"
Dove è possibile visualizzare un elenco di avvisi o allarmi risolti?	Selezionare **ALERTS** > **resolved**. "Visualizzare gli avvisi correnti e risolti"	Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi storici**. "Gestire gli allarmi (sistema legacy)"
Dove posso gestire le impostazioni?	Selezionare **ALERTS** > **Rules**. "Gestire gli avvisi"	Selezionare **SUPPORT**. Quindi, utilizzare le opzioni nella sezione **Allarmi (legacy)** del menu. "Gestire gli allarmi (sistema legacy)"

	Avvisi	Allarmi (sistema precedente)
Quali autorizzazioni di gruppo utenti sono necessarie?	• Chiunque possa accedere a Grid Manager può visualizzare gli avvisi correnti e risolti. • È necessario disporre dell'autorizzazione Manage alerts (Gestisci avvisi) per gestire silenzi, notifiche di avviso e regole di avviso. "Amministrare StorageGRID"	• Chiunque possa accedere a Grid Manager può visualizzare gli allarmi legacy. • Per riconoscere gli allarmi, è necessario disporre dell'autorizzazione di riconoscimento degli allarmi. • Per gestire gli allarmi globali e le notifiche e-mail, è necessario disporre sia della configurazione della pagina topologia griglia che di altre autorizzazioni di configurazione griglia. "Amministrare StorageGRID"
Come si gestiscono le notifiche e-mail?	Selezionare **ALERTS** > **email setup**. **Nota:** poiché gli allarmi e gli avvisi sono sistemi indipendenti, la configurazione dell'e-mail utilizzata per le notifiche di allarme e AutoSupport non viene utilizzata per le notifiche di avviso. Tuttavia, è possibile utilizzare lo stesso server di posta per tutte le notifiche. "Imposta le notifiche via email per gli avvisi"	Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**. "Gestire gli allarmi (sistema legacy)"
Come si gestiscono le notifiche SNMP?	Selezionare **CONFIGURATION** > **Monitoring** > **SNMP Agent**. "Utilizzare il monitoraggio SNMP"	*Non supportato*
Come posso controllare chi riceve le notifiche?	1. Selezionare **ALERTS** > **email setup**. 2. Nella sezione **destinatari**, immettere un indirizzo e-mail per ciascun elenco o persona che deve ricevere un'e-mail quando si verifica un avviso. "Imposta le notifiche via email per gli avvisi"	1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**. 2. Creazione di una mailing list. 3. Selezionare **Notifiche**. 4. Selezionare la mailing list. "Gestire gli allarmi (sistema legacy)"

	Avvisi	Allarmi (sistema precedente)
Quali nodi di amministrazione inviano notifiche?	Un singolo nodo Admin (il mittente preferito). "Che cos'è un nodo amministratore?"	Un singolo nodo Admin (il mittente preferito). "Che cos'è un nodo amministratore?"
Come posso eliminare alcune notifiche?	1. Selezionare **ALERTS** > **silences**. 2. Selezionare la regola di avviso che si desidera disattivare. 3. Specificare la durata del silenzio. 4. Selezionare il livello di gravità dell'avviso che si desidera disattivare. 5. Selezionare per applicare il silenzio all'intera griglia, a un singolo sito o a un singolo nodo. **Nota**: Se è stato attivato l'agente SNMP, le silenzi sopprimono anche i trap SNMP e informano. "Tacitare le notifiche di avviso"	1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**. 2. Selezionare **Notifiche**. 3. Selezionare una mailing list e selezionare **Sospendi**. "Gestire gli allarmi (sistema legacy)"
Come posso eliminare tutte le notifiche?	Selezionare **ALERTS** > **silences**.quindi, selezionare **All rules**. **Nota**: Se è stato attivato l'agente SNMP, le silenzi sopprimono anche i trap SNMP e informano. "Tacitare le notifiche di avviso"	*Non supportato*
Come si personalizzano le condizioni e i trigger?	1. Selezionare **ALERTS** > **Rules**. 2. Selezionare una regola predefinita da modificare oppure selezionare **Crea regola personalizzata**. "Modificare le regole degli avvisi" "Creare regole di avviso personalizzate"	1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**. 2. Creare un allarme personalizzato globale per ignorare un allarme predefinito o per monitorare un attributo che non ha un allarme predefinito. "Gestire gli allarmi (sistema legacy)"

	Avvisi	Allarmi (sistema precedente)
Come si disattiva un singolo avviso o allarme?	1. Selezionare **ALERTS** > **Rules**. 2. Selezionare la regola e selezionare **Modifica regola**. 3. Deselezionare la casella di controllo **Enabled**. "Disattiva le regole di avviso"	1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**. 2. Selezionare la regola e l'icona Modifica. 3. Deselezionare la casella di controllo **Enabled**. "Gestire gli allarmi (sistema legacy)"

Gestire gli avvisi

Gestisci avvisi: Panoramica

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.

È possibile creare avvisi personalizzati, modificare o disattivare gli avvisi e gestire le notifiche degli avvisi.

Per saperne di più:

- Guarda il video: "Video: Panoramica degli avvisi per StorageGRID 11,8"
- Guarda il video: "Video: Utilizzo delle metriche per creare avvisi personalizzati in StorageGRID 11,8"
- Vedere "Riferimenti agli avvisi".

Visualizzare le regole degli avvisi

Le regole di avviso definiscono le condizioni che si attivano "avvisi specifici". StorageGRID include una serie di regole di avviso predefinite, che è possibile utilizzare così com'è o modificare, oppure è possibile creare regole di avviso personalizzate.

È possibile visualizzare l'elenco di tutte le regole di avviso predefinite e personalizzate per scoprire quali condizioni attiveranno ciascun avviso e per verificare se gli avvisi sono disattivati.

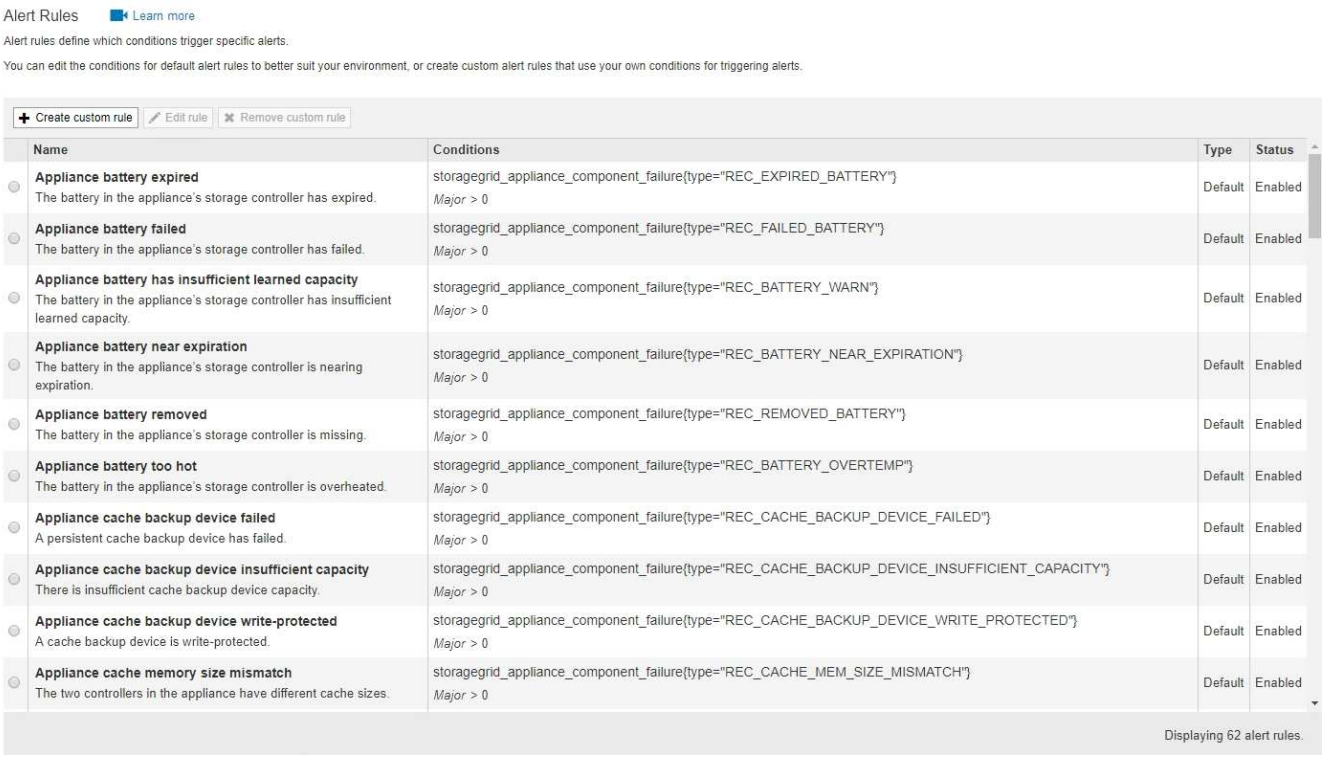
Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".
- Facoltativamente, hai guardato il video: "Video: Panoramica degli avvisi per StorageGRID 11,8"

Fasi

1. Selezionare **ALERTS** > **Rules**.

Viene visualizzata la pagina regole di avviso.



2. Esaminare le informazioni nella tabella delle regole di avviso:

Intestazione di colonna	Descrizione
Nome	Nome univoco e descrizione della regola di avviso. Vengono elencate per prime le regole di avviso personalizzate, seguite dalle regole di avviso predefinite. Il nome della regola di avviso è l'oggetto delle notifiche e-mail.
Condizioni	Le espressioni Prometheus che determinano quando viene attivato questo avviso. Un avviso può essere attivato in uno o più dei seguenti livelli di severità, ma non è richiesta alcuna condizione per ogni severità. • **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 garantire che non causino problemi più gravi.

Intestazione di colonna	Descrizione
Tipo	Il tipo di regola di avviso: • **Default**: Una regola di avviso fornita con il sistema. È possibile disattivare una regola di avviso predefinita o modificare le condizioni e la durata di una regola di avviso predefinita. Non è possibile rimuovere una regola di avviso predefinita. • **Default***: Una regola di avviso predefinita che include una condizione o una durata modificate. Se necessario, è possibile ripristinare facilmente le impostazioni predefinite originali di una condizione modificata. • **Personalizzato**: Una regola di avviso creata dall'utente. È possibile disattivare, modificare e rimuovere regole di avviso personalizzate.
Stato	Se questa regola di avviso è attualmente attivata o disattivata. Le condizioni per le regole di avviso disabilitate non vengono valutate, quindi non vengono attivati avvisi.

Creare regole di avviso personalizzate

È possibile creare regole di avviso personalizzate per definire le proprie condizioni di attivazione degli avvisi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".
- Conosci già "Metriche Prometheus comunemente utilizzate".
- Hai capito "Sintassi delle query Prometheus".
- Facoltativamente, hai guardato il video: "Video: Utilizzo delle metriche per creare avvisi personalizzati in StorageGRID 11,8".

A proposito di questa attività

StorageGRID non convalida gli avvisi personalizzati. Se si decide di creare regole di avviso personalizzate, attenersi alle seguenti linee guida generali:

- Esaminare le condizioni per le regole di avviso predefinite e utilizzarle come esempi per le regole di avviso personalizzate.
- Se si definiscono più condizioni per una regola di avviso, utilizzare la stessa espressione per tutte le condizioni. Quindi, modificare il valore di soglia per ciascuna condizione.
- Controllare attentamente ogni condizione per verificare la presenza di errori di tipo e logici.
- Utilizzare solo le metriche elencate nell'API Grid Management.
- Quando si esegue il test di un'espressione utilizzando l'API Grid Management, tenere presente che una risposta "riuscita" potrebbe essere un corpo di risposta vuoto (nessun avviso attivato). Per verificare se l'avviso è effettivamente attivato, è possibile impostare temporaneamente una soglia su un valore che si prevede sia vero al momento.

Ad esempio, per testare l'espressione `node_memory_MemTotal_bytes < 24000000000`, eseguire prima `node_memory_MemTotal_bytes >= 0` e assicurati di ottenere i risultati attesi (tutti i nodi restituiscono un valore). Quindi, riportare l'operatore e la soglia ai valori previsti ed eseguire di nuovo. Nessun risultato indica che non sono presenti avvisi correnti per questa espressione.

- Non presumere che un avviso personalizzato funzioni a meno che non sia stata convalidata l'attivazione dell'avviso quando previsto.

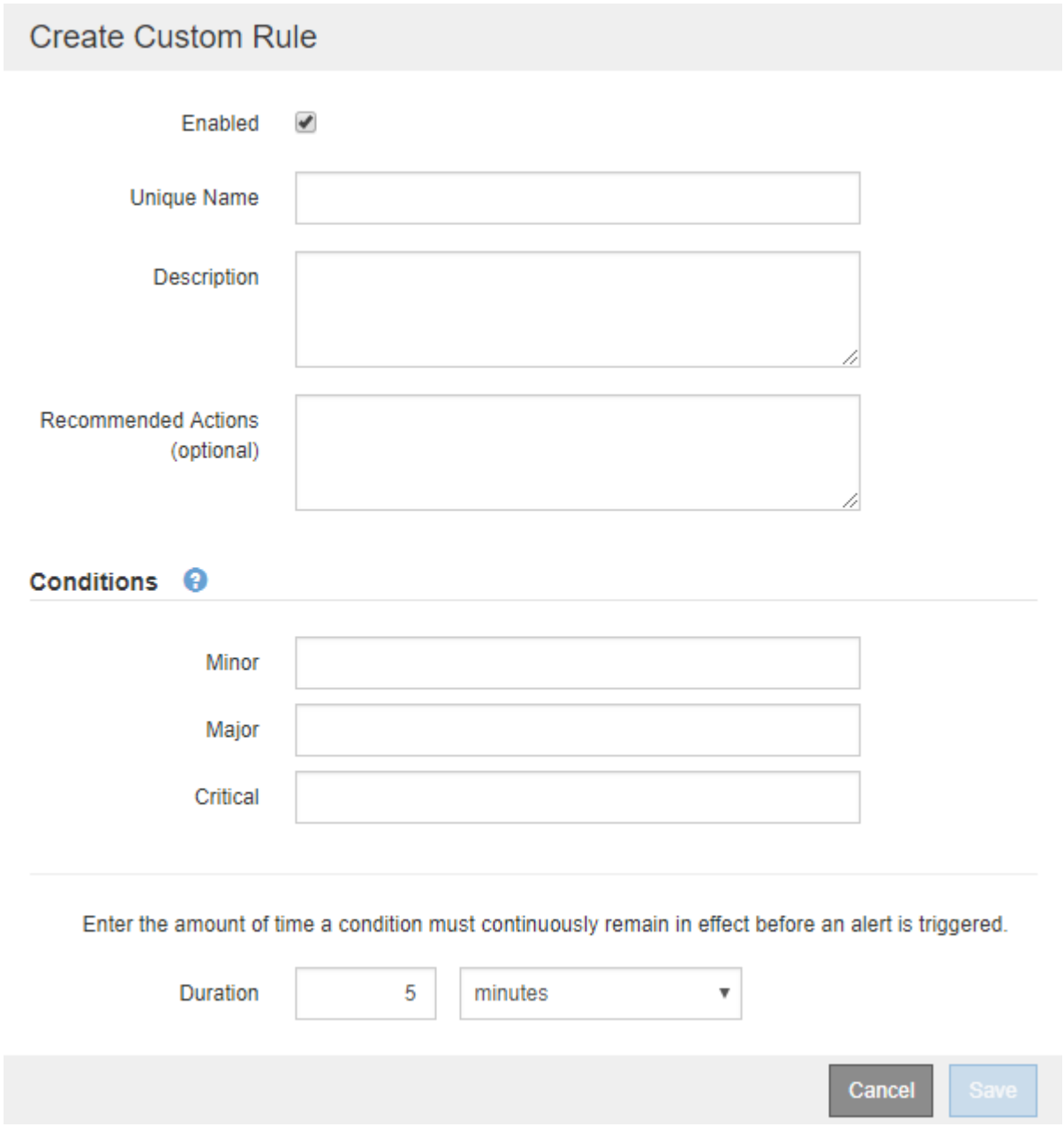
Fasi

1. Selezionare **ALERTS** > **Rules**.

   Viene visualizzata la pagina regole di avviso.

2. Selezionare **Crea regola personalizzata**.

   Viene visualizzata la finestra di dialogo Create Custom Rule (Crea regola personalizzata).



3. Selezionare o deselezionare la casella di controllo **Enabled** per determinare se questa regola di avviso è attualmente attivata.

   Se una regola di avviso è disattivata, le sue espressioni non vengono valutate e non vengono attivati avvisi.

4. Inserire le seguenti informazioni:

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi ed è anche l'oggetto delle notifiche e-mail. I nomi delle regole di avviso possono essere compresi tra 1 e 64 caratteri.
Descrizione	Una descrizione del problema che si verifica. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono essere comprese tra 1 e 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Immettere le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono essere comprese tra 0 e 1,024 caratteri.

5. Nella sezione Condizioni, immettere un'espressione Prometheus per uno o più livelli di gravità dell'avviso.

   Un'espressione di base è in genere della forma:

   ```
   [metric] [operator] [value]
   ```

   Le espressioni possono essere di qualsiasi lunghezza, ma vengono visualizzate su una singola riga dell'interfaccia utente. È richiesta almeno un'espressione.

   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_bytes < 24000000000
   ```

   Per visualizzare le metriche disponibili e verificare le espressioni Prometheus, selezionare l'icona della guida E segui il link alla sezione metriche dell'API Grid Management.

6. Nel campo **durata**, immettere il periodo di tempo in cui una condizione deve rimanere in vigore continuamente prima che l'allarme venga attivato e selezionare un'unità di tempo.

   Per attivare un avviso immediatamente quando una condizione diventa vera, immettere **0**. Aumentare questo valore per evitare che condizioni temporanee attivino avvisi.

   L'impostazione predefinita è 5 minuti.

7. Selezionare **Salva**.

   La finestra di dialogo si chiude e la nuova regola di avviso personalizzata viene visualizzata nella tabella

regole di avviso.

Modificare le regole degli avvisi

È possibile modificare una regola di avviso per modificare le condizioni di attivazione; per una regola di avviso personalizzata, è anche possibile aggiornare il nome della regola, la descrizione e le azioni consigliate.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

A proposito di questa attività

Quando si modifica una regola di avviso predefinita, è possibile modificare le condizioni per gli avvisi minori, maggiori e critici e la durata. Quando si modifica una regola di avviso personalizzata, è anche possibile modificare il nome, la descrizione e le azioni consigliate della regola.

> Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

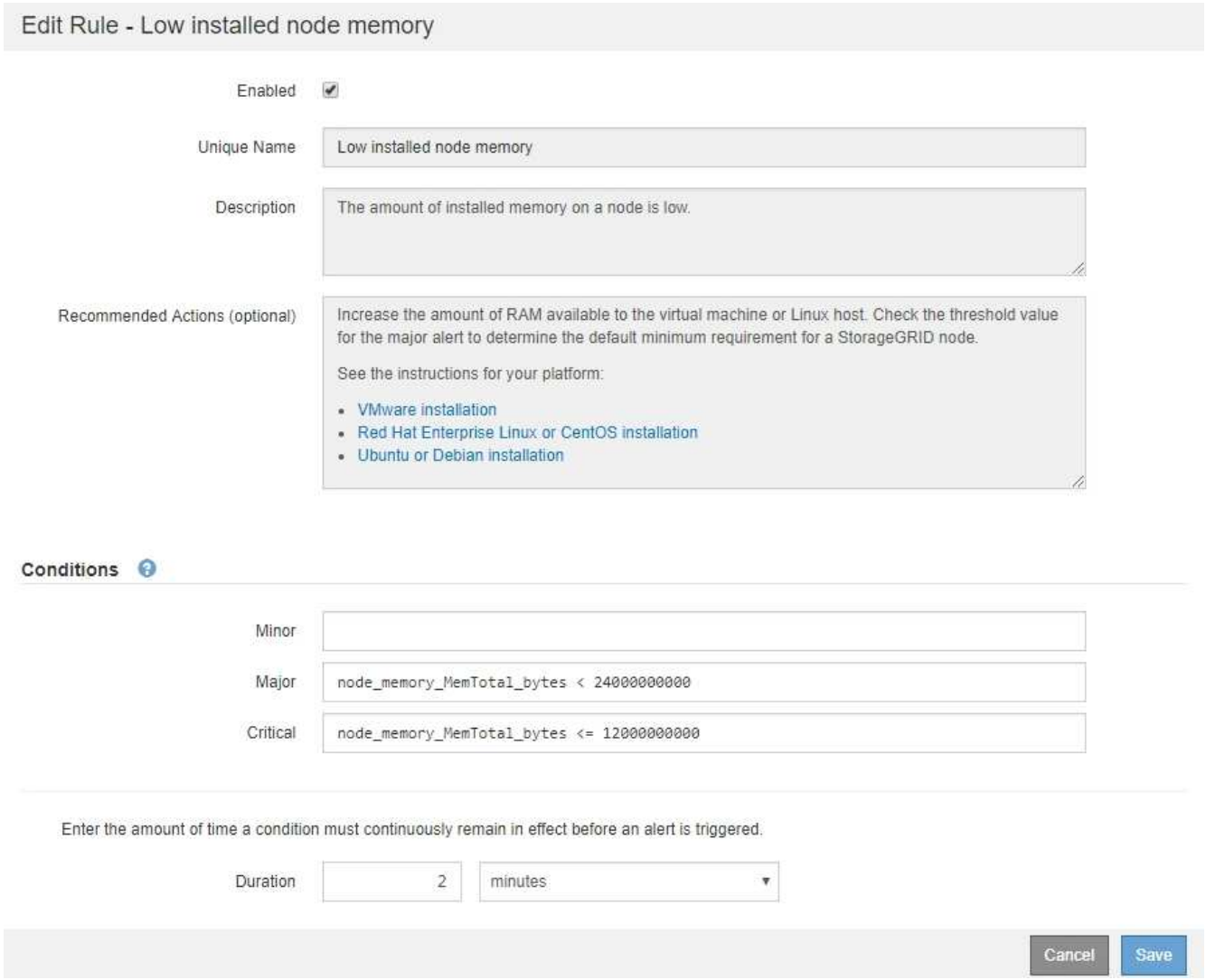
Fasi

1. Selezionare **ALERTS** > **Rules**.

   Viene visualizzata la pagina regole di avviso.

2. Selezionare il pulsante di opzione corrispondente alla regola di avviso che si desidera modificare.
3. Selezionare **Modifica regola**.

   Viene visualizzata la finestra di dialogo Edit Rule (Modifica regola). Questo esempio mostra una regola di avviso predefinita: I campi Nome univoco, Descrizione e azioni consigliate sono disattivati e non possono essere modificati.



4. Selezionare o deselezionare la casella di controllo **Enabled** per determinare se questa regola di avviso è attualmente attivata.

   Se una regola di avviso è disattivata, le sue espressioni non vengono valutate e non vengono attivati avvisi.

   > Se si disattiva la regola di avviso per un avviso corrente, è necessario attendere alcuni minuti affinché l'avviso non venga più visualizzato come avviso attivo.

   > In generale, la disattivazione di una regola di avviso predefinita non è consigliata. Se una regola di avviso è disattivata, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

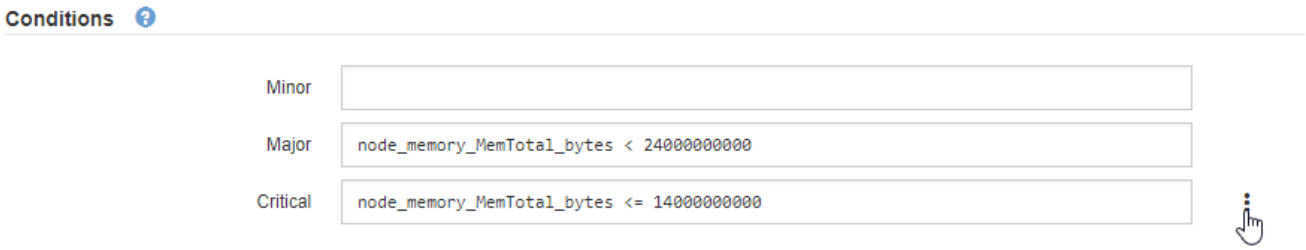
5. Per le regole di avviso personalizzate, aggiornare le seguenti informazioni secondo necessità.

   > Non puoi modificare queste informazioni per le regole di avviso predefinite.

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi ed è anche l'oggetto delle notifiche e-mail. I nomi delle regole di avviso possono essere compresi tra 1 e 64 caratteri.
Descrizione	Una descrizione del problema che si verifica. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono essere comprese tra 1 e 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Immettere le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono essere comprese tra 0 e 1,024 caratteri.

6. Nella sezione Condizioni, immettere o aggiornare l'espressione Prometheus per uno o più livelli di gravità dell'avviso.

Se si desidera ripristinare il valore originale di una condizione per una regola di avviso predefinita modificata, selezionare i tre punti a destra della condizione modificata.



Se si aggiornano le condizioni per un avviso corrente, le modifiche potrebbero non essere implementate fino a quando la condizione precedente non viene risolta. Al successivo soddisfacimento di una delle condizioni per la regola, l'avviso rifletterà i valori aggiornati.

Un'espressione di base è in genere della forma:

```
[metric] [operator] [value]
```

Le espressioni possono essere di qualsiasi lunghezza, ma vengono visualizzate su una singola riga dell'interfaccia utente. È richiesta almeno un'espressione.

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_bytes < 24000000000
```

7. Nel campo **durata**, immettere il periodo di tempo in cui una condizione deve rimanere in vigore continuamente prima che l'allarme venga attivato, quindi selezionare l'unità di tempo.

Per attivare un avviso immediatamente quando una condizione diventa vera, immettere **0**. Aumentare

questo valore per evitare che condizioni temporanee attivino avvisi.

L'impostazione predefinita è 5 minuti.

8. Selezionare **Salva**.

   Se è stata modificata una regola di avviso predefinita, nella colonna tipo viene visualizzato **Default***. Se è stata disattivata una regola di avviso predefinita o personalizzata, nella colonna **Status** viene visualizzato **Disabled**.

Disattiva le regole di avviso

È possibile modificare lo stato attivato/disattivato per una regola di avviso predefinita o personalizzata.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

A proposito di questa attività

Quando una regola di avviso viene disattivata, le sue espressioni non vengono valutate e non vengono attivati avvisi.

> In generale, la disattivazione di una regola di avviso predefinita non è consigliata. Se una regola di avviso è disattivata, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

Fasi

1. Selezionare **ALERTS** > **Rules**.

   Viene visualizzata la pagina regole di avviso.

2. Selezionare il pulsante di opzione corrispondente alla regola di avviso che si desidera attivare o disattivare.
3. Selezionare **Modifica regola**.

   Viene visualizzata la finestra di dialogo Edit Rule (Modifica regola).

4. Selezionare o deselezionare la casella di controllo **Enabled** per determinare se questa regola di avviso è attualmente attivata.

   Se una regola di avviso è disattivata, le sue espressioni non vengono valutate e non vengono attivati avvisi.

   > Se si disattiva la regola di avviso per un avviso corrente, è necessario attendere alcuni minuti affinché l'avviso non venga più visualizzato come avviso attivo.

5. Selezionare **Salva**.

   Disabled viene visualizzato nella colonna **Status**.

Rimuovere le regole di avviso personalizzate

È possibile rimuovere una regola di avviso personalizzata se non si desidera più utilizzarla.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

Fasi

1. Selezionare **ALERTS** > **Rules**.

   Viene visualizzata la pagina regole di avviso.

2. Selezionare il pulsante di opzione per la regola di avviso personalizzata che si desidera rimuovere.

   Non è possibile rimuovere una regola di avviso predefinita.

3. Selezionare **Rimuovi regola personalizzata**.

   Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **OK** per rimuovere la regola di avviso.

   Tutte le istanze attive dell'avviso verranno risolte entro 10 minuti.

Gestire le notifiche di avviso

Impostare le notifiche SNMP per gli avvisi

Se si desidera che StorageGRID invii notifiche SNMP quando si verificano avvisi, è necessario attivare l'agente SNMP StorageGRID e configurare una o più destinazioni trap.

È possibile utilizzare l'opzione **CONFIGURAZIONE** > **monitoraggio** > **agente SNMP** in Gestione griglia o gli endpoint SNMP per l'API di gestione griglia per attivare e configurare l'agente SNMP StorageGRID. L'agente SNMP supporta tutte e tre le versioni del protocollo SNMP.

Per informazioni sulla configurazione dell'agente SNMP, vedere "Utilizzare il monitoraggio SNMP".

Dopo aver configurato l'agente SNMP StorageGRID, è possibile inviare due tipi di notifiche basate sugli eventi:

- I 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 di trap e notifica vengono inviate quando viene attivato un avviso predefinito o personalizzato a qualsiasi livello di gravità. Per eliminare le notifiche SNMP per un avviso, è necessario configurare un silenzio per l'avviso. Vedere "Tacitare le notifiche di avviso".

Se la distribuzione StorageGRID include più nodi amministrativi, il nodo amministrativo primario è il mittente preferito per le notifiche di avviso, i pacchetti AutoSupport, le trap e le notifiche SNMP e le notifiche di allarme legacy. Se il nodo di amministrazione primario non è più disponibile, le notifiche vengono inviate temporaneamente da altri nodi di amministrazione. Vedere "Che cos'è un nodo amministratore?".

Imposta le notifiche via email per gli avvisi

Se si desidera che le notifiche e-mail vengano inviate quando si verificano avvisi, è necessario fornire informazioni sul server SMTP. È inoltre necessario immettere gli indirizzi e-mail per i destinatari delle notifiche di avviso.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

A proposito di questa attività

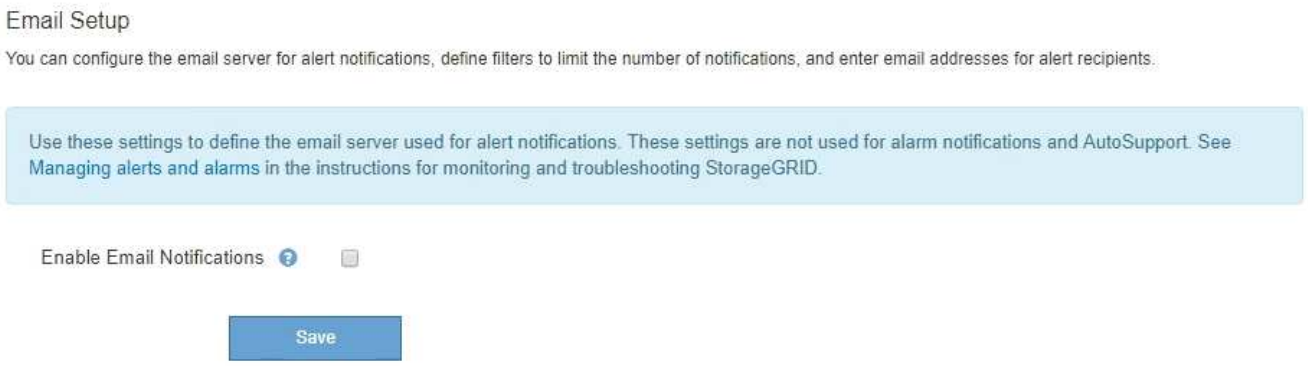
Poiché gli allarmi e gli avvisi sono sistemi indipendenti, la configurazione e-mail utilizzata per le notifiche di avviso non viene utilizzata per le notifiche di allarme e i pacchetti AutoSupport. Tuttavia, è possibile utilizzare lo stesso server di posta elettronica per tutte le notifiche.

Se la distribuzione StorageGRID include più nodi amministrativi, il nodo amministrativo primario è il mittente preferito per le notifiche di avviso, i pacchetti AutoSupport, le trap e le notifiche SNMP e le notifiche di allarme legacy. Se il nodo di amministrazione primario non è più disponibile, le notifiche vengono inviate temporaneamente da altri nodi di amministrazione. Vedere "Che cos'è un nodo amministratore?".

Fasi

1. Selezionare **ALERTS** > **email setup**.

   Viene visualizzata la pagina Configurazione e-mail.



2. Selezionare la casella di controllo **Enable Email Notifications** (attiva notifiche e-mail) per indicare che si desidera inviare e-mail di notifica quando gli avvisi raggiungono le soglie configurate.

   Vengono visualizzate le sezioni Server e-mail (SMTP), TLS (Transport Layer Security), indirizzi e-mail e filtri.

3. Nella sezione Server e-mail (SMTP), immettere le informazioni necessarie per l'accesso al server SMTP da parte di StorageGRID.

   Se il server SMTP richiede l'autenticazione, è necessario fornire sia un nome utente che una password.

Campo	Invio
Server di posta	Il nome di dominio completo (FQDN) o l'indirizzo IP del server SMTP.
Porta	Porta utilizzata per accedere al server SMTP. Deve essere compreso tra 1 e 65535.
Nome utente (opzionale)	Se il server SMTP richiede l'autenticazione, immettere il nome utente con cui eseguire l'autenticazione.
Password (opzionale)	Se il server SMTP richiede l'autenticazione, immettere la password con cui eseguire l'autenticazione.

4. Nella sezione indirizzi e-mail, immettere gli indirizzi e-mail per il mittente e per ciascun destinatario.

   a. Per **Sender Email Address**, specificare un indirizzo e-mail valido da utilizzare come indirizzo da per le notifiche degli avvisi.

      Ad esempio: `storagegrid-alerts@example.com`

   b. Nella sezione destinatari, immettere un indirizzo e-mail per ciascun elenco o persona che deve ricevere un'e-mail quando si verifica un avviso.

      Selezionare l'icona più ➕ per aggiungere destinatari.

5. Se TLS (Transport Layer Security) è richiesto per le comunicazioni con il server SMTP, selezionare **Richiedi TLS** nella sezione Transport Layer Security (TLS).

   a. Nel campo **certificato CA**, fornire il certificato CA che verrà utilizzato per verificare l'identificazione del server SMTP.

È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfoglia** e selezionare il file.

È necessario fornire un singolo file contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

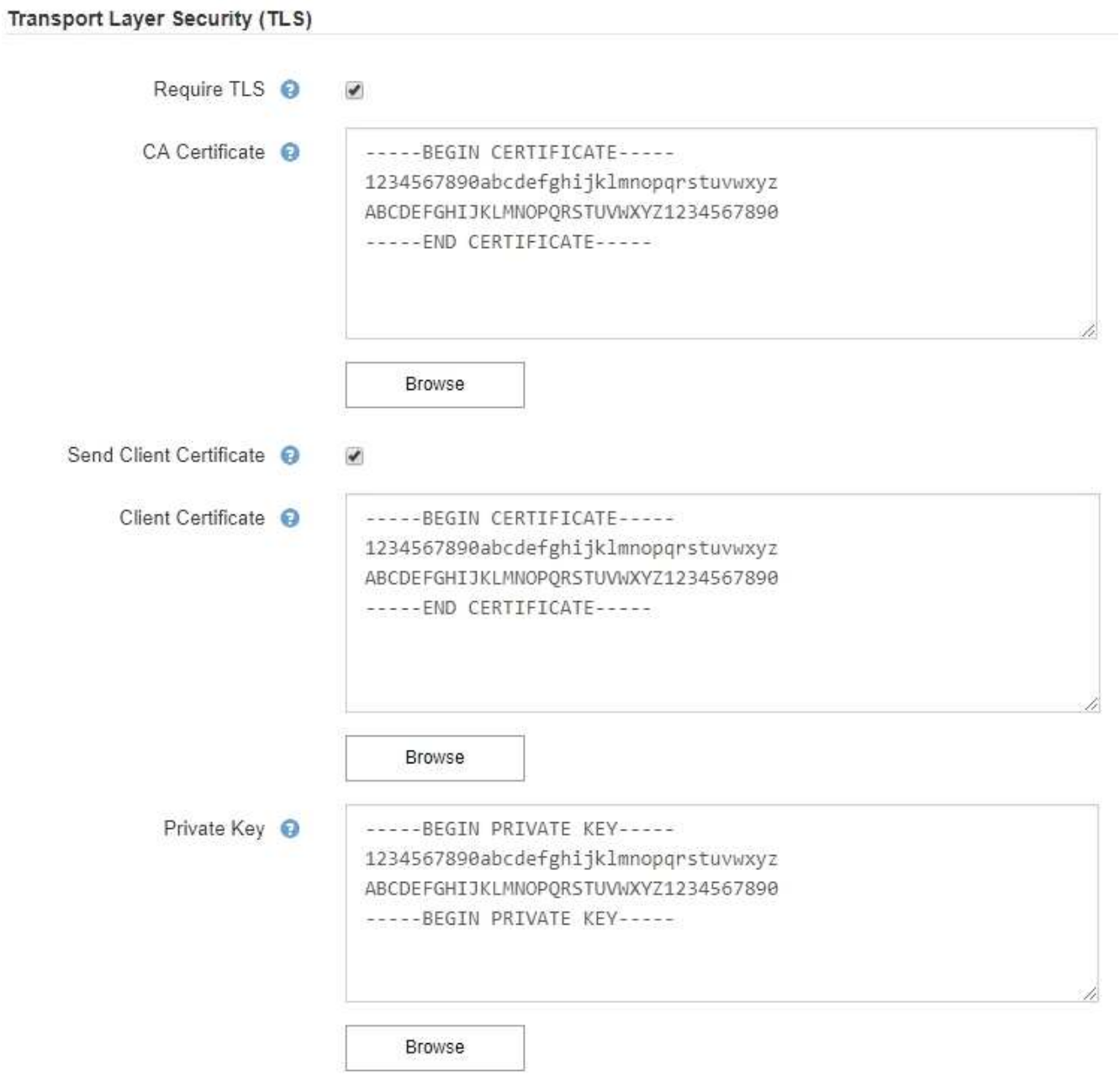
b. Selezionare la casella di controllo **Send Client Certificate** (Invia certificato client) se il server di posta SMTP richiede l'invio di certificati client per l'autenticazione da parte dei mittenti di posta elettronica.
c. Nel campo **certificato client**, fornire il certificato client con codifica PEM da inviare al server SMTP.

   È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfoglia** e selezionare il file.

d. Nel campo **Private Key** (chiave privata), immettere la chiave privata per il certificato client in codifica PEM non crittografata.

   È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfoglia** e selezionare il file.

> Se si desidera modificare la configurazione dell'e-mail, selezionare l'icona a forma di matita per aggiornare questo campo.



6. Nella sezione filtri, selezionare i livelli di severità degli avvisi che devono generare le notifiche via email, a meno che la regola per uno specifico avviso non sia stata tacitata.

Severità	Descrizione
Minore, maggiore, critico	Viene inviata una notifica via email quando viene soddisfatta la condizione minore, maggiore o critica di una regola di avviso.
Importante, critico	Viene inviata una notifica via email quando viene soddisfatta la condizione principale o critica per una regola di avviso. Le notifiche non vengono inviate per avvisi minori.

Severità	Descrizione
Solo critico	Una notifica via email viene inviata solo quando viene soddisfatta la condizione critica per una regola di avviso. Le notifiche non vengono inviate per avvisi minori o maggiori.

7. Quando si è pronti a verificare le impostazioni e-mail, attenersi alla seguente procedura:
   a. Selezionare **Invia email di prova**.

      Viene visualizzato un messaggio di conferma che indica l'invio di un'e-mail di prova.

   b. Selezionare le caselle di posta in arrivo di tutti i destinatari e confermare che è stata ricevuta un'e-mail di prova.

      Se l'e-mail non viene ricevuta entro pochi minuti o se viene attivato l'avviso **errore notifica e-mail**, controllare le impostazioni e riprovare.

   c. Accedi a qualsiasi altro nodo Admin e invia un'e-mail di prova per verificare la connettività da tutti i siti.

      Quando si verificano le notifiche di avviso, è necessario accedere a ogni nodo amministratore per verificare la connettività. Ciò è in contrasto con il test dei pacchetti AutoSupport e delle notifiche di allarme legacy, in cui tutti i nodi amministrativi inviano l'e-mail di prova.

8. Selezionare **Salva**.

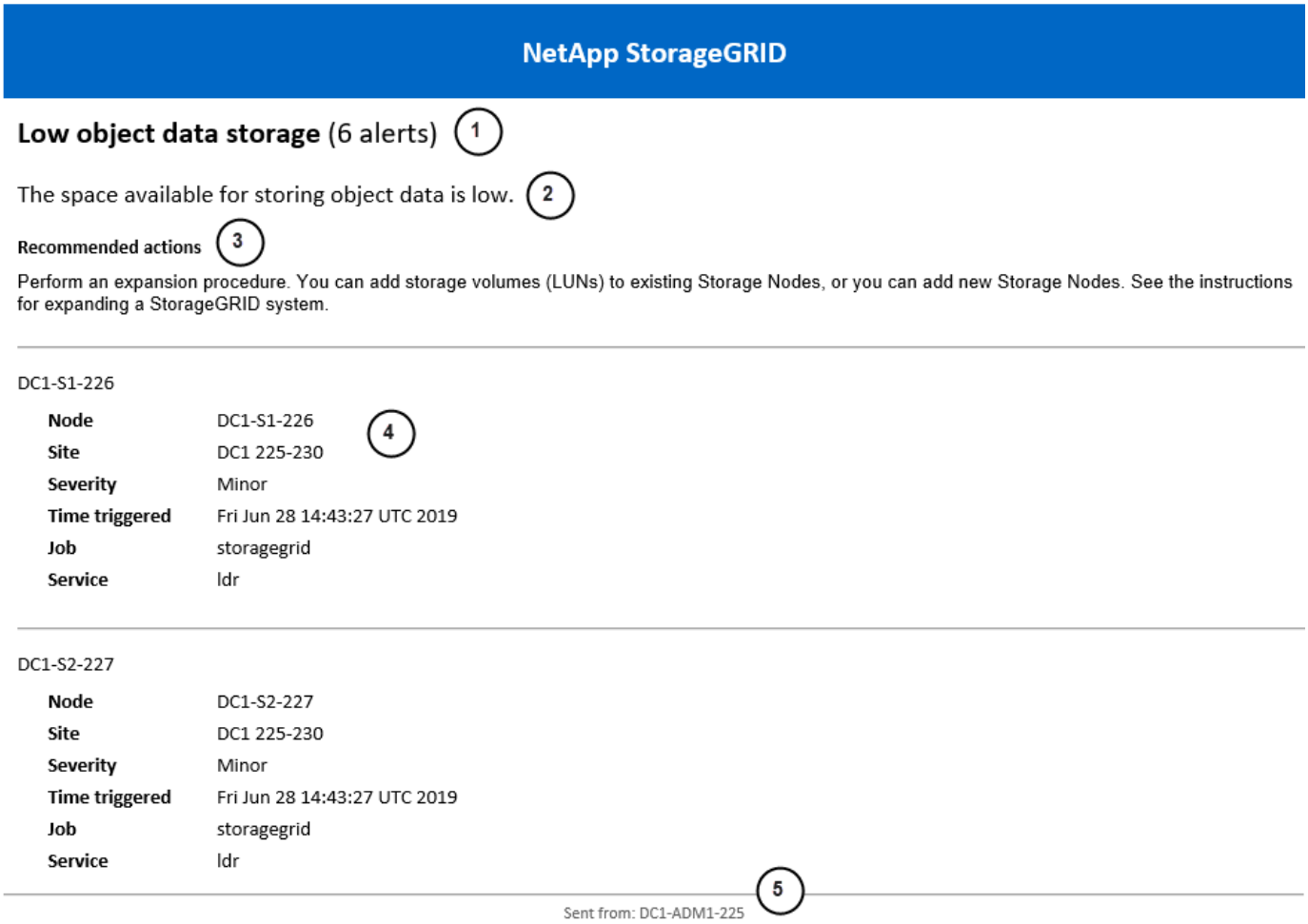
   L'invio di un'e-mail di prova non salva le impostazioni. Selezionare **Salva**.

   Le impostazioni e-mail vengono salvate.

Informazioni incluse nelle notifiche e-mail di avviso

Dopo aver configurato il server di posta SMTP, le notifiche e-mail vengono inviate ai destinatari designati quando viene attivato un avviso, a meno che la regola di avviso non venga soppressa da un silenzio. Vedere "Tacitare le notifiche di avviso".

Le notifiche e-mail includono le seguenti informazioni:



Didascalia	Descrizione
1	Il nome dell'avviso, seguito dal numero di istanze attive dell'avviso.
2	La descrizione dell'avviso.
3	Qualsiasi azione consigliata per l'avviso.
4	Dettagli su ogni istanza attiva dell'avviso, inclusi il nodo e il sito interessati, la severità dell'avviso, l'ora UTC in cui è stata attivata la regola di avviso e il nome del servizio e del processo interessati.
5	Il nome host del nodo amministratore che ha inviato la notifica.

Modalità di raggruppamento degli avvisi

Per impedire l'invio di un numero eccessivo di notifiche e-mail quando vengono attivati gli avvisi, StorageGRID tenta di raggruppare più avvisi nella stessa notifica.

Fare riferimento alla tabella seguente per alcuni esempi di come StorageGRID raggruppa più avvisi nelle notifiche e-mail.

Comportamento	Esempio
Ogni notifica di avviso si applica solo agli avvisi con lo stesso nome. Se vengono attivati contemporaneamente due avvisi con nomi diversi, vengono inviate due notifiche e-mail.	• L'avviso A viene attivato su due nodi contemporaneamente. Viene inviata una sola notifica. • L'allarme A viene attivato sul nodo 1 e l'allarme B viene attivato contemporaneamente sul nodo 2. Vengono inviate due notifiche, una per ogni avviso.
Per un avviso specifico su un nodo specifico, se le soglie vengono raggiunte per più di una severità, viene inviata una notifica solo per l'avviso più grave.	• Viene attivato l'allarme A e vengono raggiunte le soglie di allarme minore, maggiore e critico. Viene inviata una notifica per l'avviso critico.
La prima volta che viene attivato un avviso, StorageGRID attende 2 minuti prima di inviare una notifica. Se durante questo periodo vengono attivati altri avvisi con lo stesso nome, StorageGRID raggruppa tutti gli avvisi nella notifica iniziale.	1. L'allarme A viene attivato sul nodo 1 alle 08:00. Non viene inviata alcuna notifica. 2. L'allarme A viene attivato sul nodo 2 alle 08:01. Non viene inviata alcuna notifica. 3. Alle 08:02, viene inviata una notifica per segnalare entrambe le istanze dell'avviso.
Se viene attivato un altro avviso con lo stesso nome, StorageGRID attende 10 minuti prima di inviare una nuova notifica. La nuova notifica riporta tutti gli avvisi attivi (gli avvisi correnti che non sono stati tacitati), anche se precedentemente segnalati.	1. L'allarme A viene attivato sul nodo 1 alle 08:00. Viene inviata una notifica alle ore 08:02. 2. L'allarme A viene attivato sul nodo 2 alle 08:05. Una seconda notifica viene inviata alle 08:15 (10 minuti dopo). Vengono segnalati entrambi i nodi.
Se sono presenti più avvisi correnti con lo stesso nome e uno di questi viene risolto, non viene inviata una nuova notifica se l'avviso si ripresenta sul nodo per il quale l'avviso è stato risolto.	1. Viene attivato l'avviso A per il nodo 1. Viene inviata una notifica. 2. L'avviso A viene attivato per il nodo 2. Viene inviata una seconda notifica. 3. L'avviso A è stato risolto per il nodo 2, ma rimane attivo per il nodo 1. 4. L'avviso A viene nuovamente attivato per il nodo 2. Non viene inviata alcuna nuova notifica perché l'avviso è ancora attivo per il nodo 1.
StorageGRID continua a inviare notifiche via email ogni 7 giorni fino a quando tutte le istanze dell'avviso non vengono risolte o la regola dell'avviso non viene tacitata.	1. L'allarme A viene attivato per il nodo 1 l'8 marzo. Viene inviata una notifica. 2. L'avviso A non viene risolto o tacitato. Ulteriori notifiche verranno inviate il 15 marzo, il 22 marzo, il 29 marzo e così via.

Risolvere i problemi relativi alle notifiche email di avviso

Se viene attivato l'avviso **errore notifica email** o non si riesce a ricevere la notifica email di avviso del test, attenersi alla procedura descritta di seguito per risolvere il problema.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

Fasi

1. Verificare le impostazioni.
   a. Selezionare **ALERTS** > **email setup**.
   b. Verificare che le impostazioni del server e-mail (SMTP) siano corrette.
   c. Verificare di aver specificato indirizzi e-mail validi per i destinatari.
2. Controllare il filtro antispam e assicurarsi che l'e-mail non sia stata inviata a una cartella di posta indesiderata.
3. Chiedi all'amministratore dell'email di confermare che le e-mail dell'indirizzo del mittente non vengono bloccate.
4. Raccogliere un file di log per l'Admin Node, quindi contattare il supporto tecnico.

   Il supporto tecnico può utilizzare le informazioni contenute nei registri per determinare l'errore. Ad esempio, il file prometheus.log potrebbe visualizzare un errore durante la connessione al server specificato.

   Vedere "Raccogliere i file di log e i dati di sistema".

Tacitare le notifiche di avviso

In alternativa, è possibile configurare le silenzi in modo da eliminare temporaneamente le notifiche di avviso.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

A proposito di questa attività

È possibile disattivare le regole di avviso sull'intera griglia, su un singolo sito o su un singolo nodo e per una o più severità. Ogni silenzio elimina tutte le notifiche per una singola regola di avviso o per tutte le regole di avviso.

Se è stato attivato l'agente SNMP, le silenzi sopprimono anche i trap SNMP e informano.

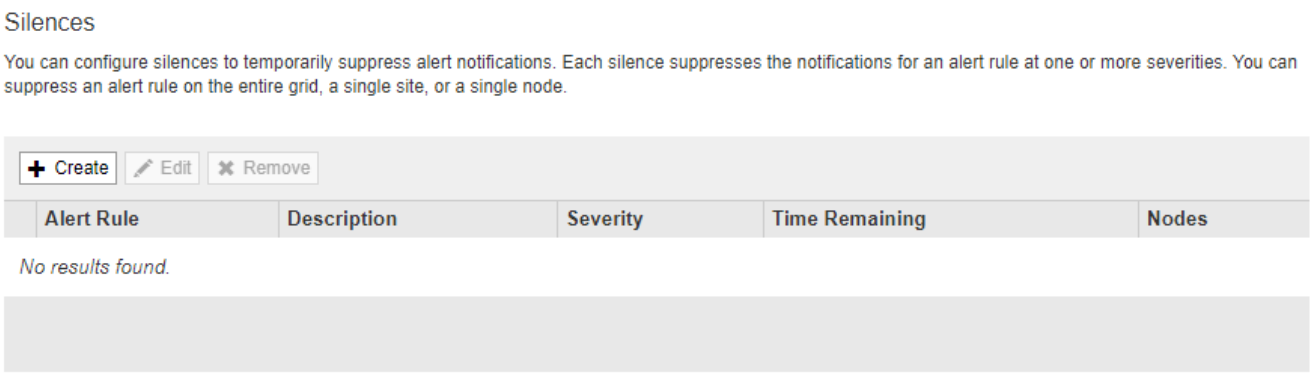
> Prestare attenzione quando si decide di tacitare una regola di avviso. Se si tacita un avviso, potrebbe non essere possibile rilevare un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica.

> Poiché gli allarmi e gli avvisi sono sistemi indipendenti, non è possibile utilizzare questa funzionalità per eliminare le notifiche di allarme.

Fasi

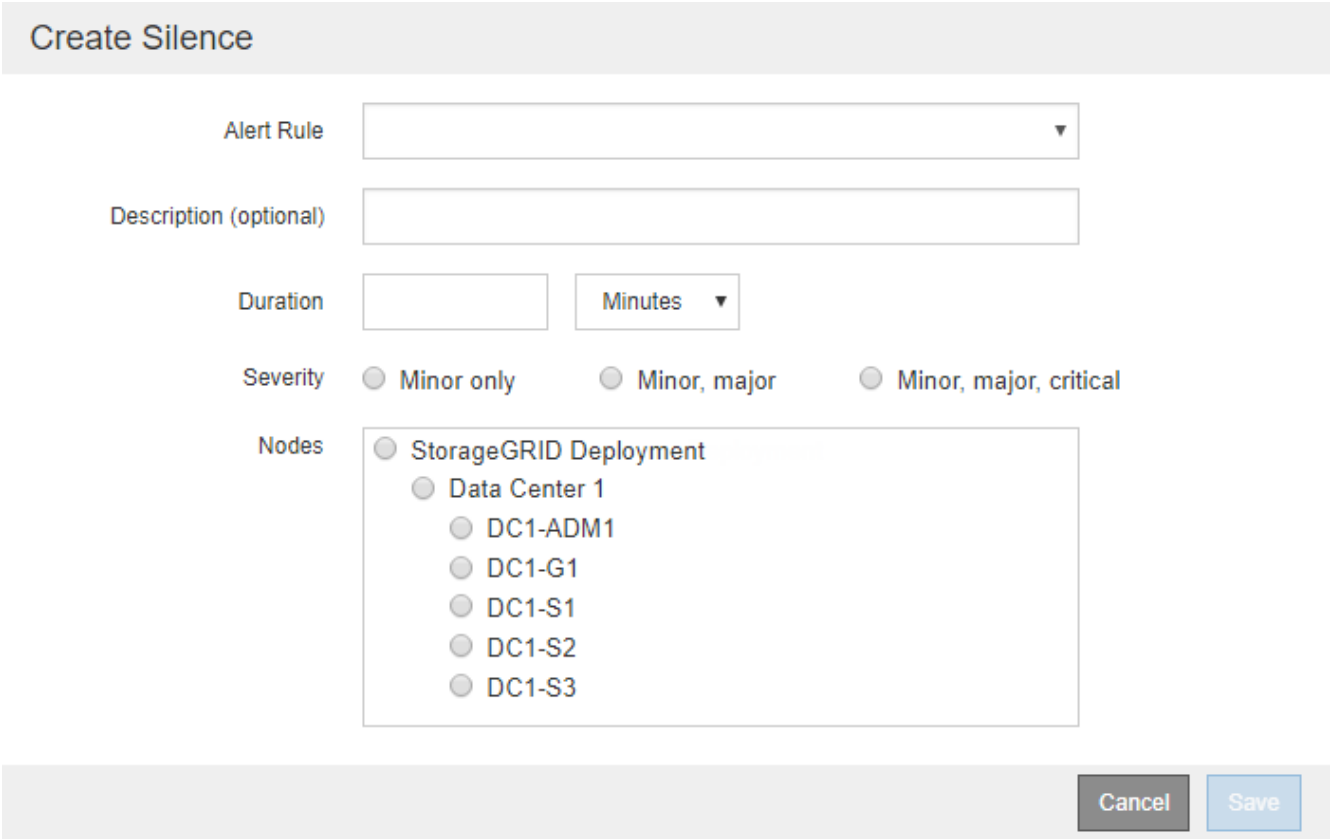
1. Selezionare **ALERTS** > **silences**.

   Viene visualizzata la pagina Silences (silenzi).



2. Selezionare **Crea**.

   Viene visualizzata la finestra di dialogo Crea silenzio.



3. Selezionare o inserire le seguenti informazioni:

Campo	Descrizione
Regola di avviso	Il nome della regola di avviso che si desidera disattivare. È possibile selezionare qualsiasi regola di avviso predefinita o personalizzata, anche se la regola di avviso è disattivata. **Nota:** selezionare **tutte le regole** se si desidera disattivare tutte le regole di avviso utilizzando i criteri specificati in questa finestra di dialogo.

Campo	Descrizione
Descrizione	Facoltativamente, una descrizione del silenzio. Ad esempio, descrivi lo scopo di questo silenzio.
Durata	Per quanto tempo si desidera che questo silenzio rimanga attivo, in minuti, ore o giorni. Un silenzio può essere in vigore da 5 minuti a 1,825 giorni (5 anni). **Nota:** non disattivare una regola di avviso per un periodo di tempo prolungato. Se una regola di avviso viene tacitata, è possibile che non si rilevi un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica. Tuttavia, potrebbe essere necessario utilizzare un silenzio esteso se un avviso viene attivato da una configurazione specifica e intenzionale, ad esempio per gli avvisi **link down** dell'appliance di servizi e **link down** dell'appliance di storage.
Severità	Quale severità o severità degli avvisi deve essere tacitata. Se l'avviso viene attivato in una delle severità selezionate, non viene inviata alcuna notifica.
Nodi	A quale nodo o nodi si desidera applicare questo silenzio. È possibile eliminare una regola di avviso o tutte le regole dell'intera griglia, di un singolo sito o di un singolo nodo. Se si seleziona l'intera griglia, il silenzio viene applicato a tutti i siti e a tutti i nodi. Se si seleziona un sito, il silenzio si applica solo ai nodi di quel sito. **Nota:** non è possibile selezionare più di un nodo o più siti per ogni silenzio. Se si desidera eliminare la stessa regola di avviso su più di un nodo o più siti contemporaneamente, è necessario creare silenzi aggiuntivi.

4. Selezionare **Salva**.
5. Se si desidera modificare o terminare un silenzio prima della scadenza, è possibile modificarlo o rimuoverlo.

Opzione	Descrizione
Modificare un silenzio	a. Selezionare **ALERTS** > **silences**. b. Dalla tabella, selezionare il pulsante di opzione relativo al silenzio che si desidera modificare. c. Selezionare **Modifica**. d. Modificare la descrizione, il tempo rimanente, le severità selezionate o il nodo interessato. e. Selezionare **Salva**.

Opzione	Descrizione
Eliminare un silenzio	a. Selezionare **ALERTS** > **silences**. b. Dalla tabella, selezionare il pulsante di opzione per il silenzio che si desidera rimuovere. c. Selezionare **Rimuovi**. d. Selezionare **OK** per confermare che si desidera rimuovere questo silenzio. **Nota**: Le notifiche verranno inviate quando viene attivato questo avviso (a meno che non venga eliminato da un altro silenzio). Se questo avviso viene attivato, potrebbero essere necessari alcuni minuti per l'invio di notifiche e-mail o SNMP e per l'aggiornamento della pagina Avvisi.

Informazioni correlate

- "Configurare l'agente SNMP"

Riferimenti agli avvisi

Questo riferimento elenca gli avvisi predefiniti visualizzati in Grid Manager. Le azioni consigliate sono contenute nel messaggio di avviso ricevuto.

Se necessario, è possibile creare regole di avviso personalizzate per adattarsi al proprio approccio di gestione del sistema.

Alcuni degli avvisi predefiniti vengono utilizzati "Metriche Prometheus".

Avvisi sull'appliance

Nome dell'avviso	Descrizione
Batteria dell'appliance scaduta	La batteria del controller di storage dell'appliance è scaduta.
Batteria dell'appliance guasta	La batteria del controller di storage dell'appliance si è guastata.
La capacità appresa della batteria dell'appliance non è sufficiente	La capacità appresa della batteria nel controller di storage dell'appliance non è sufficiente.
Batteria dell'apparecchio quasi scaduta	La batteria del controller di storage dell'appliance sta per scadere.
Batteria dell'apparecchio rimossa	La batteria nel controller di storage dell'appliance non è presente.
Batteria dell'apparecchio troppo calda	La batteria del controller di storage dell'apparecchio è surriscaldata.
Errore di comunicazione BMC dell'appliance	La comunicazione con il BMC (Baseboard Management Controller) è stata persa.

Nome dell'avviso	Descrizione
Periferica di backup della cache dell'appliance non riuscita	Si è verificato un errore in una periferica di backup della cache persistente.
Capacità insufficiente del dispositivo di backup della cache dell'appliance	La capacità della periferica di backup della cache è insufficiente.
Dispositivo di backup cache dell'appliance protetto da scrittura	Una periferica di backup della cache è protetta da scrittura.
Mancata corrispondenza delle dimensioni della memoria cache dell'appliance	I due controller dell'appliance hanno dimensioni della cache diverse.
Temperatura dello chassis del controller di calcolo dell'appliance troppo alta	La temperatura del controller di calcolo in un'appliance StorageGRID ha superato una soglia nominale.
Temperatura CPU del controller di calcolo dell'appliance troppo alta	La temperatura della CPU nel controller di calcolo di un'appliance StorageGRID ha superato una soglia nominale.
Il controller di calcolo dell'appliance richiede attenzione	È stato rilevato un guasto hardware nel controller di calcolo di un'appliance StorageGRID.
Si è verificato un problema nell'alimentatore A del controller di calcolo dell'appliance	L'alimentazione A nel controller di calcolo presenta un problema.
Si è verificato un problema nell'alimentatore B del controller di calcolo dell'appliance	L'alimentazione B nel controller di calcolo presenta un problema.
Il servizio di monitoraggio dell'hardware di calcolo dell'appliance si è bloccato	Il servizio che monitora lo stato dell'hardware dello storage si è bloccato.
Unità DAS dell'appliance che supera il limite per i dati scritti al giorno	Una quantità eccessiva di dati viene scritta su un'unità ogni giorno, il che potrebbe invalidare la garanzia.
Rilevato guasto al disco DAS dell'appliance	È stato rilevato un problema con un disco DAS (Direct-Attached Storage) nell'appliance.
Spia localizzatore unità DAS dell'appliance accesa	La spia di posizionamento dell'unità per una o più unità DAS (Direct-Attached Storage) in un nodo di archiviazione dell'appliance è accesa.

Nome dell'avviso	Descrizione
Ricostruzione del disco DAS dell'appliance	È in corso la ricostruzione di un disco DAS (Direct-Attached Storage). Questo è previsto se è stato sostituito o rimosso/reinserito di recente.
Rilevato guasto alla ventola dell'appliance	È stato rilevato un problema relativo alla ventola dell'apparecchio.
Rilevato guasto nel Fibre Channel dell'appliance	È stato rilevato un problema di collegamento Fibre Channel tra lo storage controller dell'appliance e il controller di calcolo
Errore della porta HBA Fibre Channel dell'appliance	Una porta HBA Fibre Channel si sta guastando o si è guastata.
Unità flash cache dell'appliance non ottimali	I dischi utilizzati per la cache SSD non sono ottimali.
Interconnessione dell'appliance/contenitore della batteria rimosso	Il contenitore di interconnessione/batteria non è presente.
Porta LACP dell'appliance mancante	Una porta su un'appliance StorageGRID non partecipa al bond LACP.
Rilevato guasto alla scheda NIC dell'appliance	È stato rilevato un problema con una scheda di interfaccia di rete (NIC) nell'appliance.
Alimentatore generale dell'appliance degradato	La potenza di un'appliance StorageGRID è diversa dalla tensione di esercizio consigliata.
Avviso critico SSD dell'appliance	Un'appliance SSD sta segnalando un avviso critico.
Guasto del controller dello storage dell'appliance A.	Si è verificato un errore nel controller storage A di un'appliance StorageGRID.
Guasto del controller storage dell'appliance B.	Il controller dello storage B in un'appliance StorageGRID si è guastato.
Guasto al disco del controller dello storage dell'appliance	Uno o più dischi di un'appliance StorageGRID si sono guastati o non sono ottimali.
Problema hardware del controller dello storage dell'appliance	Il software SANtricity segnala "richiede attenzione" per un componente di un'appliance StorageGRID.
Guasto all'alimentazione Del controller dello storage dell'appliance A.	L'alimentazione A di un'appliance StorageGRID non è conforme alla tensione di esercizio consigliata.

Nome dell’avviso	Descrizione
Guasto all’alimentazione B del controller storage dell’appliance	L’alimentazione B di un apparecchio StorageGRID non è conforme alla tensione di esercizio consigliata.
Il servizio di monitoraggio hardware dello storage dell’appliance si è bloccato	Il servizio che monitora lo stato dell’hardware dello storage si è bloccato.
Gli shelf di storage delle appliance sono degradati	Lo stato di uno dei componenti dello shelf di storage di un’appliance di storage è degradato.
Temperatura dell’apparecchio superata	La temperatura nominale o massima del controller di storage dell’appliance è stata superata.
Sensore di temperatura dell’apparecchio rimosso	È stato rimosso un sensore di temperatura.
Errore di avvio protetto UEFI dell’appliance	Un’appliance non è stata avviata in modo sicuro.
L’i/o del disco è molto lento	L’i/o del disco molto lento potrebbe influire sulle prestazioni della griglia.
Rilevato guasto alla ventola dell’appliance di storage	È stato rilevato un problema con un’unità ventola nel controller di storage di un’appliance.
La connettività dello storage dell’appliance di storage è degradata	Si è verificato un problema con una o più connessioni tra il controller di calcolo e il controller dello storage.
Dispositivo di storage inaccessibile	Impossibile accedere a un dispositivo di storage.

Avvisi di audit e syslog

Nome dell’avviso	Descrizione
I registri di controllo vengono aggiunti alla coda in-memory	Il nodo non può inviare i log al server syslog locale e la coda in-memory si sta riempiendo.
Errore di inoltro del server syslog esterno	Il nodo non può inoltrare i log al server syslog esterno.
Coda di audit di grandi dimensioni	La coda dei dischi per i messaggi di controllo è piena. Se questa condizione non viene risolta, le operazioni S3 o Swift potrebbero non riuscire.
I registri vengono aggiunti alla coda su disco	Il nodo non può inoltrare i log al server syslog esterno e la coda su disco si sta riempiendo.

Avvisi bucket

Nome dell'avviso	Descrizione
Il bucket FabricPool ha un'impostazione di coerenza del bucket non supportata	Un bucket FabricPool utilizza il livello di coerenza disponibile o di sito sicuro, che non è supportato.

Avvisi Cassandra

Nome dell'avviso	Descrizione
Errore compattatore automatico Cassandra	Si è verificato un errore nel compattatore automatico Cassandra.
Metriche del compattatore automatico Cassandra non aggiornate	Le metriche che descrivono il compattatore automatico Cassandra non sono aggiornate.
Errore di comunicazione Cassandra	I nodi che eseguono il servizio Cassandra hanno problemi di comunicazione tra loro.
Le compaction di Cassandra sono sovraccaricate	Il processo di compattazione Cassandra è sovraccarico.
Errore di scrittura Cassandra oversize	Un processo StorageGRID interno ha inviato a Cassandra una richiesta di scrittura troppo grande.
Metriche di riparazione Cassandra non aggiornate	Le metriche che descrivono i lavori di riparazione Cassandra non sono aggiornate.
Il processo di riparazione di Cassandra è lento	Il progresso delle riparazioni del database Cassandra è lento.
Servizio di riparazione Cassandra non disponibile	Il servizio di riparazione Cassandra non è disponibile.
Tabella Cassandra corrotta	Cassandra ha rilevato un danneggiamento della tabella. Cassandra si riavvia automaticamente se rileva la corruzione della tabella.

Avvisi Cloud Storage Pool

Nome dell'avviso	Descrizione
Errore di connettività del pool di cloud storage	Il controllo dello stato di salute dei Cloud Storage Pools ha rilevato uno o più nuovi errori.

Avvisi di replica cross-grid

Nome dell'avviso	Descrizione
Errore permanente della replica cross-grid	Si è verificato un errore di replica cross-grid che richiede l'intervento dell'utente per la risoluzione.
Risorse di replica cross-grid non disponibili	Le richieste di replica cross-grid sono in sospeso perché una risorsa non è disponibile.

Avvisi DHCP

Nome dell'avviso	Descrizione
Lease DHCP scaduto	Il lease DHCP su un'interfaccia di rete è scaduto.
Il lease DHCP sta per scadere	Il lease DHCP su un'interfaccia di rete sta per scadere.
Server DHCP non disponibile	Il server DHCP non è disponibile.

Avvisi di debug e traccia

Nome dell'avviso	Descrizione
Impatto delle performance di debug	Quando la modalità di debug è attivata, le prestazioni del sistema potrebbero risentirne negativamente.
Configurazione traccia attivata	Quando la configurazione di trace è attivata, le prestazioni del sistema potrebbero risentire negativamente.

Avvisi e-mail e AutoSupport

Nome dell'avviso	Descrizione
Impossibile inviare il messaggio AutoSupport	Impossibile inviare il messaggio AutoSupport più recente.
Errore di notifica e-mail	Impossibile inviare la notifica via email per un avviso.

Erasure coding (EC) alerts (Avvisi di codifica di cancellazione

Nome dell'avviso	Descrizione
Errore di ribilanciamento EC	La procedura di ribilanciamento EC non è riuscita o è stata interrotta.
Errore di riparazione EC	Un intervento di riparazione per i dati EC non è riuscito o è stato interrotto.

Nome dell'avviso	Descrizione
Riparazione EC in stallo	Un intervento di riparazione per i dati EC si è bloccato.

Scadenza degli avvisi relativi ai certificati

Nome dell'avviso	Descrizione
Scadenza certificato CA proxy amministratore	Uno o più certificati nel pacchetto CA del server proxy amministratore stanno per scadere.
Scadenza del certificato client	Uno o più certificati client stanno per scadere.
Scadenza del certificato server globale per S3 e Swift	Il certificato server globale per S3 e Swift sta per scadere.
Scadenza del certificato endpoint del bilanciamento del carico	Uno o più certificati endpoint per il bilanciamento del carico stanno per scadere.
Scadenza del certificato del server per l'interfaccia di gestione	Il certificato del server utilizzato per l'interfaccia di gestione sta per scadere.
Scadenza del certificato CA syslog esterno	Il certificato dell'autorità di certificazione (CA) utilizzato per firmare il certificato del server syslog esterno sta per scadere.
Scadenza del certificato client syslog esterno	Il certificato client per un server syslog esterno sta per scadere.
Scadenza del certificato del server syslog esterno	Il certificato del server presentato dal server syslog esterno sta per scadere.

Avvisi Grid Network

Nome dell'avviso	Descrizione
Mancata corrispondenza MTU rete griglia	L'impostazione MTU per l'interfaccia Grid Network (eth0) differisce significativamente tra i nodi della griglia.

Avvisi di federazione delle griglie

Nome dell'avviso	Descrizione
Scadenza del certificato di federazione griglia	Uno o più certificati di federazione griglia stanno per scadere.
Errore di connessione alla federazione di griglie	La connessione a federazione di griglie tra la rete locale e remota non funziona.

Avvisi di utilizzo elevato o latenza elevata

Nome dell'avviso	Descrizione
Elevato utilizzo di heap Java	Viene utilizzata una percentuale elevata di spazio heap Java.
Latenza elevata per le query sui metadati	Il tempo medio per le query dei metadati Cassandra è troppo lungo.

Avvisi di Identity Federation

Nome dell'avviso	Descrizione
Errore di sincronizzazione della federazione delle identità	Impossibile sincronizzare utenti e gruppi federati dall'origine dell'identità.
Errore di sincronizzazione della federazione delle identità per un tenant	Impossibile sincronizzare utenti e gruppi federati dall'origine dell'identità configurata da un tenant.

Avvisi ILM (Information Lifecycle Management)

Nome dell'avviso	Descrizione
Posizionamento ILM non raggiungibile	Non è possibile ottenere un'istruzione di posizionamento in una regola ILM per determinati oggetti.
Periodo di scansione ILM troppo lungo	Il tempo necessario per eseguire la scansione, la valutazione e l'applicazione di ILM agli oggetti è troppo lungo.
Velocità di scansione ILM bassa	La velocità di scansione ILM è impostata su un valore inferiore a 100 oggetti/secondo.

Avvisi del server di gestione delle chiavi (KMS)

Nome dell'avviso	Descrizione
Scadenza del certificato CA KMS	Il certificato dell'autorità di certificazione (CA) utilizzato per firmare il certificato del server di gestione delle chiavi (KMS) sta per scadere.
Scadenza del certificato client KMS	Il certificato client per un server di gestione delle chiavi sta per scadere
Impossibile caricare la configurazione KMS	La configurazione per il server di gestione delle chiavi esiste ma non è riuscita a caricarsi.
Errore di connettività KMS	Un nodo appliance non è riuscito a connettersi al server di gestione delle chiavi del proprio sito.

Nome dell'avviso	Descrizione
Nome chiave di crittografia KMS non trovato	Il server di gestione delle chiavi configurato non dispone di una chiave di crittografia corrispondente al nome fornito.
Rotazione della chiave di crittografia KMS non riuscita	Tutti i volumi dell'appliance sono stati decifrati correttamente, ma uno o più volumi non sono stati ruotati sulla chiave più recente.
KMS non configurato	Non esiste alcun server di gestione delle chiavi per questo sito.
La chiave KMS non è riuscita a decrittare un volume dell'appliance	Non è stato possibile decifrare uno o più volumi su un'appliance con crittografia del nodo abilitata con la chiave KMS corrente.
Scadenza del certificato del server KMS	Il certificato del server utilizzato dal server di gestione delle chiavi (KMS) sta per scadere.

Avvisi di offset dell'orologio locale

Nome dell'avviso	Descrizione
Grande offset temporale dell'orologio locale	L'offset tra l'orologio locale e l'ora NTP (Network Time Protocol) è troppo elevato.

Avvisi di memoria insufficiente o spazio insufficiente

Nome dell'avviso	Descrizione
Bassa capacità del disco di log di audit	Lo spazio disponibile per i registri di controllo è insufficiente. Se questa condizione non viene risolta, le operazioni S3 o Swift potrebbero non riuscire.
Memoria del nodo a bassa disponibilità	La quantità di RAM disponibile su un nodo è bassa.
Spazio libero ridotto per il pool di storage	Lo spazio disponibile per memorizzare i dati dell'oggetto nel nodo di storage è basso.
Memoria del nodo installata insufficiente	La quantità di memoria installata su un nodo è bassa.
Storage dei metadati basso	Lo spazio disponibile per memorizzare i metadati degli oggetti è basso.
Capacità disco di metriche ridotte	Lo spazio disponibile per il database delle metriche è basso.
Storage dei dati a oggetti basso	Lo spazio disponibile per memorizzare i dati degli oggetti è basso.

Nome dell'avviso	Descrizione
Override del watermark di sola lettura bassa	L'override filigrana di sola lettura soft del volume di storage è inferiore al watermark ottimizzato minimo per un nodo di storage.
Bassa capacità del disco root	Lo spazio disponibile sul disco root è insufficiente.
Bassa capacità dei dati di sistema	Lo spazio disponibile per /var/local è basso. Se questa condizione non viene risolta, le operazioni S3 o Swift potrebbero non riuscire.
Spazio libero nella directory tmp basso	Lo spazio disponibile nella directory /tmp è insufficiente.

Avvisi di rete di nodi o nodi

Nome dell'avviso	Descrizione
Utilizzo ricezione rete amministratore	L'utilizzo della ricezione nella rete amministrativa è elevato.
Uso della trasmissione della rete di amministrazione	L'utilizzo della trasmissione sulla rete amministrativa è elevato.
Errore di configurazione del firewall	Impossibile applicare la configurazione del firewall.
Endpoint dell'interfaccia di gestione in modalità fallback	Tutti gli endpoint dell'interfaccia di gestione ricadono troppo a lungo sulle porte predefinite.
Errore di connettività di rete del nodo	Si sono verificati errori durante il trasferimento dei dati tra nodi.
Errore frame ricezione rete nodo	Un'elevata percentuale di frame di rete ricevuti da un nodo presenta errori.
Nodo non sincronizzato con il server NTP	Il nodo non è sincronizzato con il server NTP (Network Time Protocol).
Nodo non bloccato con server NTP	Il nodo non è bloccato su un server NTP (Network Time Protocol).
Rete del nodo non appliance non in funzione	Uno o più dispositivi di rete sono disconnessi o non attivi.
Collegamento dell'appliance di servizi alla rete di amministrazione	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.

Nome dell'avviso	Descrizione
Collegamento dell'appliance di servizi alla porta di rete dell'amministratore 1	La porta Admin Network 1 dell'appliance è inattiva o disconnessa.
Collegamento dell'appliance di servizi alla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di servizi alla porta di rete 1	La porta di rete 1 dell'appliance è inattiva o scollegata.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 2	La porta di rete 2 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 3	La porta di rete 3 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 4	La porta di rete 4 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage in Admin Network	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.
Collegamento dell'appliance di storage alla porta di rete dell'amministratore 1	La porta Admin Network 1 dell'appliance è inattiva o disconnessa.
Collegamento dell'appliance di storage alla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di storage alla porta di rete 1	La porta di rete 1 dell'appliance è inattiva o scollegata.
Collegamento dell'appliance di storage inattivo sulla porta di rete 2	La porta di rete 2 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage inattivo sulla porta di rete 3	La porta di rete 3 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage inattivo sulla porta di rete 4	La porta di rete 4 sull'apparecchio è inattiva o scollegata.

Nome dell'avviso	Descrizione
Nodo di storage non nello stato di storage desiderato	Il servizio LDR su un nodo di archiviazione non può passare allo stato desiderato a causa di un errore interno o di un problema relativo al volume
Utilizzo della connessione TCP	Il numero di connessioni TCP su questo nodo si avvicina al numero massimo che è possibile tenere traccia.
Impossibile comunicare con il nodo	Uno o più servizi non rispondono o non è possibile raggiungere il nodo.
Riavvio del nodo imprevisto	Un nodo si è riavviato inaspettatamente nelle ultime 24 ore.

Avvisi a oggetti

Nome dell'avviso	Descrizione
Controllo dell'esistenza dell'oggetto non riuscito	Il processo di controllo dell'esistenza dell'oggetto non è riuscito.
Controllo dell'esistenza dell'oggetto bloccato	Il lavoro di verifica dell'esistenza dell'oggetto si è bloccato.
Oggetti persi	Uno o più oggetti sono stati persi dalla griglia.
S3 HA POSTO la dimensione dell'oggetto troppo grande	Un client sta tentando di eseguire un'operazione PUT Object che supera i limiti di dimensione S3.
Rilevato oggetto corrotto non identificato	È stato trovato un file nello storage a oggetti replicato che non è stato possibile identificare come oggetto replicato.

Avvisi sui servizi della piattaforma

Nome dell'avviso	Descrizione
Richiesta di servizi piattaforma in sospeso capacità bassa	Il numero di richieste in sospeso di Platform Services si sta avvicinando alla capacità.
Servizi della piattaforma non disponibili	In un sito sono in esecuzione o disponibili troppi nodi di storage con il servizio RSM.

Avvisi sul volume di storage

Nome dell'avviso	Descrizione
Il volume di storage richiede attenzione	Un volume di storage è offline e richiede attenzione.

Nome dell'avviso	Descrizione
Il volume di storage deve essere ripristinato	Un volume di storage è stato ripristinato e deve essere ripristinato.
Volume di storage offline	Un volume di storage è rimasto offline per più di 5 minuti, probabilmente perché il nodo è stato riavviato durante la fase di formattazione del volume.
Ripristino volume non riuscito ad avviare la riparazione dei dati replicati	Impossibile avviare automaticamente la riparazione dei dati replicati per un volume riparato.

Avvisi dei servizi StorageGRID

Nome dell'avviso	Descrizione
servizio nginx con configurazione di backup	La configurazione del servizio nginx non è valida. È in uso la configurazione precedente.
servizio nginx-gw con configurazione di backup	La configurazione del servizio nginx-gw non è valida. È in uso la configurazione precedente.
Riavvio necessario per disattivare FIPS	Il criterio di protezione non richiede la modalità FIPS, ma il modulo di protezione crittografico NetApp è attivato.
Riavvio necessario per attivare FIPS	Il criterio di protezione richiede la modalità FIPS, ma il modulo di protezione crittografico NetApp è disattivato.
Servizio SSH con configurazione di backup	La configurazione del servizio SSH non è valida. È in uso la configurazione precedente.

Avvisi del tenant

Nome dell'avviso	Descrizione
Utilizzo elevato della quota del tenant	Viene utilizzata un'elevata percentuale di spazio di quota. Questa regola è disattivata per impostazione predefinita perché potrebbe causare un numero eccessivo di notifiche.

Metriche Prometheus comunemente utilizzate

Fare riferimento a questo elenco di metriche Prometheus comunemente utilizzate per comprendere meglio le condizioni nelle regole di avviso predefinite o per creare le condizioni per le regole di avviso personalizzate.

Puoi anche farlo ottenere un elenco completo di tutte le metriche.

Per ulteriori informazioni sulla sintassi delle query Prometheus, vedere "Interrogazione di Prometheus".

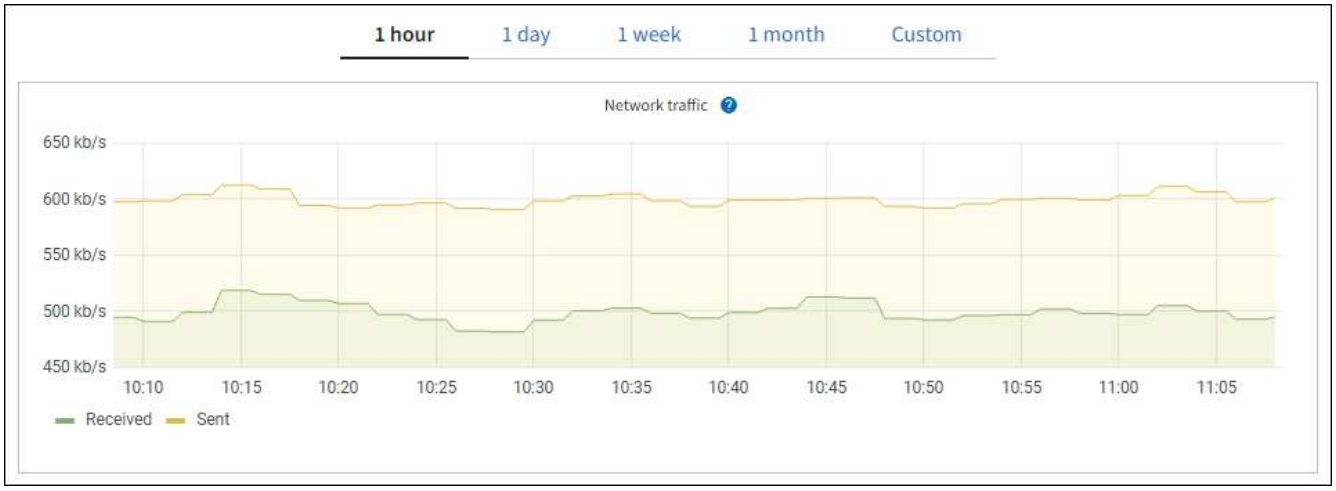
Quali sono le metriche Prometheus?

Le metriche Prometheus sono misurazioni di serie temporali. Il servizio Prometheus sui nodi di amministrazione raccoglie queste metriche dai servizi su tutti i nodi. Le metriche vengono memorizzate su ciascun nodo di amministrazione fino a quando lo spazio riservato ai dati Prometheus non è pieno. Quando il `/var/local/mysql_ibdata/` il volume raggiunge la capacità, le metriche meno recenti vengono prima eliminate.

Dove vengono utilizzate le metriche Prometheus?

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 diversi 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.

Elenco delle metriche più comuni

Il seguente elenco contiene le metriche Prometheus più comunemente utilizzate.

> Le metriche che includono *private* nei loro nomi sono solo per uso interno e sono soggette a modifiche senza preavviso tra le release di StorageGRID.

alertmanager_notifications_failed_total
Il numero totale di notifiche di avviso non riuscite.

node_filesystem_avail_bytes
La quantità di spazio del file system disponibile in byte per gli utenti non root.

Node_Memory_MemAvailable_Bytes
Campo delle informazioni sulla memoria MemAvailable_Bytes.

node_network_carrier
Valore portante di `/sys/class/net/iface`.

node_network_receive_errs_total
Statistiche sui dispositivi di rete `receive_errs`.

node_network_transmit_errs_total
Statistiche sui dispositivi di rete `transmit_errs`.

storagegrid_administively_down
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.

storagegrid_appliance_compute_controller_hardware_status
Lo stato dell'hardware del controller di calcolo in un'appliance.

storagegrid_appliance_failed_disks
Per lo storage controller di un'appliance, il numero di dischi non ottimali.

storagegrid_appliance_storage_controller_hardware_status
Lo stato generale dell'hardware dello storage controller in un'appliance.

storagegrid_content_bucket_and_containers
Il numero totale di bucket S3 e container Swift noti da questo nodo di storage.

storagegrid_content_objects
Il numero totale di oggetti dati S3 e Swift noti da questo nodo di storage. Il conteggio è valido solo per gli oggetti dati creati dalle applicazioni client che si interfacciano con il sistema tramite S3 o Swift.

storagegrid_content_objects_lost
Il numero totale di oggetti che il servizio rileva come mancanti dal sistema StorageGRID. È necessario intraprendere azioni per determinare la causa della perdita e se è possibile eseguire il ripristino.

"Risolvere i problemi relativi ai dati degli oggetti persi e mancanti"

storagegrid_http_sessions_incoming_tented

Il numero totale di sessioni HTTP che sono state tentate per un nodo di storage.

storagegrid_http_sessions_incoming_currently_established

Il numero di sessioni HTTP attualmente attive (aperte) sul nodo di storage.

storagegrid_http_sessions_incoming_failed

Il numero totale di sessioni HTTP che non sono riuscite a completare correttamente, a causa di una richiesta HTTP non valida o di un errore durante l'elaborazione di un'operazione.

storagegrid_http_sessions_incoming_successful

Il numero totale di sessioni HTTP completate correttamente.

storagegrid_ilm_waiting_background_objects

Il numero totale di oggetti su questo nodo in attesa di valutazione ILM dalla scansione.

storagegrid_ilm_waiting_client_evaluation_objects_per_second

La velocità corrente alla quale gli oggetti vengono valutati in base al criterio ILM su questo nodo.

storagegrid_ilm_waiting_client_objects

Il numero totale di oggetti su questo nodo in attesa di valutazione ILM dalle operazioni del client (ad esempio, acquisizione).

storagegrid_ilm_waiting_total_objects

Il numero totale di oggetti in attesa di valutazione ILM.

storagegrid_ilm_scan_objects_per_second

La velocità con cui gli oggetti di proprietà di questo nodo vengono sottoposti a scansione e messi in coda per ILM.

storagegrid_ilm_scan_period_estimated_minutes

Il tempo stimato per completare una scansione ILM completa su questo nodo.

Nota: Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti di proprietà di questo nodo.

storagegrid_load_balancer_endpoint_cert_expiry_time

Il tempo di scadenza del certificato endpoint del bilanciamento del carico in secondi dall'epoca.

storagegrid_metadata_queries_average_latency_millisecondi

Il tempo medio richiesto per eseguire una query sull'archivio di metadati tramite questo servizio.

storagegrid_network_received_bytes

La quantità totale di dati ricevuti dall'installazione.

storagegrid_network_transmitted_bytes

La quantità totale di dati inviati dall'installazione.

storagegrid_node_cpu_utilization_percent

La percentuale di tempo CPU disponibile attualmente utilizzata da questo servizio. Indica la disponibilità del servizio. La quantità di tempo CPU disponibile dipende dal numero di CPU del server.

storagegrid_ntp_chouged_time_source_offset_millisecondi

Offset sistematico del tempo fornito da una fonte di tempo scelta. L'offset viene introdotto quando il ritardo per raggiungere un'origine temporale non è uguale al tempo richiesto per l'origine temporale per raggiungere il client NTP.

storagegrid_ntp_locked

Il nodo non è bloccato su un server NTP (Network Time Protocol).

storagegrid_s3_data_transfers_bytes_ingested

La quantità totale di dati acquisiti dai client S3 a questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_s3_data_transfers_bytes_retrieved

La quantità totale di dati recuperati dai client S3 da questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_s3_operations_failed

Il numero totale di operazioni S3 non riuscite (codici di stato HTTP 4xx e 5xx), escluse quelle causate da un errore di autorizzazione S3.

storagegrid_s3_operations_successful

Il numero totale di operazioni S3 riuscite (codice di stato HTTP 2xx).

storagegrid_s3_operations_non autorizzato

Il numero totale di operazioni S3 non riuscite che sono il risultato di un errore di autorizzazione.

storagegrid_servercertificate_management_interface_cert_expiry_days

Il numero di giorni prima della scadenza del certificato dell'interfaccia di gestione.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

Il numero di giorni prima della scadenza del certificato API dello storage a oggetti.

storagegrid_service_cpu_seconds

La quantità di tempo cumulativa in cui la CPU è stata utilizzata da questo servizio dopo l'installazione.

storagegrid_service_memory_usage_bytes

La quantità di memoria (RAM) attualmente utilizzata da questo servizio. Questo valore è identico a quello visualizzato dall'utility principale di Linux come RES.

storagegrid_service_network_received_bytes

La quantità totale di dati ricevuti dal servizio dopo l'installazione.

storagegrid_service_network_transmitted_bytes

La quantità totale di dati inviati da questo servizio.

storagegrid_service_reavvies

Il numero totale di riavvii del servizio.

storagegrid_service_runtime_seconds

Il tempo totale di esecuzione del servizio dopo l'installazione.

storagegrid_service_uptime_seconds

Il tempo totale di esecuzione del servizio dall'ultimo riavvio.

storagegrid_storage_state_current

Lo stato corrente dei servizi di storage. I valori degli attributi sono:

- 10 = non in linea
- 15 = manutenzione
- 20 = sola lettura
- 30 = Online

storagegrid_storage_status

Lo stato corrente dei servizi di storage. I valori degli attributi sono:

- 0 = Nessun errore
- 10 = in transizione
- 20 = spazio libero insufficiente
- 30 = Volume(i) non disponibile
- 40 = errore

storagegrid_storage_utilization_data_bytes

Una stima delle dimensioni totali dei dati di oggetti replicati e con erasure coding sul nodo storage.

storagegrid_storage_utilization_metadata_allowed_bytes

Lo spazio totale sul volume 0 di ciascun nodo di storage consentito per i metadati dell'oggetto. Questo valore è sempre inferiore allo spazio effettivo riservato ai metadati su un nodo, perché una parte dello spazio riservato è necessaria per le operazioni essenziali del database (come la compattazione e la riparazione) e i futuri aggiornamenti hardware e software. Lo spazio consentito per i metadati dell'oggetto controlla la capacità complessiva degli oggetti.

storagegrid_storage_utilization_metadata_bytes

La quantità di metadati oggetto sul volume di storage 0, in byte.

storagegrid_storage_utilization_total_space_bytes

La quantità totale di spazio di storage allocato a tutti gli archivi di oggetti.

storagegrid_storage_utilization_usable_space_bytes

La quantità totale di spazio di storage a oggetti rimanente. Calcolato sommando la quantità di spazio disponibile per tutti gli archivi di oggetti sul nodo di storage.

storagegrid_swift_data_transfers_bytes_ingested

La quantità totale di dati acquisiti dai client Swift a questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_swift_data_transfers_bytes_retrieved

La quantità totale di dati recuperati dai client Swift da questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_swift_operations_failed

Il numero totale di operazioni Swift non riuscite (codici di stato HTTP 4xx e 5xx), escluse quelle causate da un errore di autorizzazione Swift.

storagegrid_swift_operations_successful

Il numero totale di operazioni Swift riuscite (codice di stato HTTP 2xx).

storagegrid_swift_operations_inhautorizzata

Il numero totale di operazioni Swift non riuscite che sono il risultato di un errore di autorizzazione (codici di stato HTTP 401, 403, 405).

storagegrid_tenant_usage_data_bytes

La dimensione logica di tutti gli oggetti per il tenant.

storagegrid_tenant_usage_object_count

Il numero di oggetti per il tenant.

storagegrid_tenant_usage_quota_byte

La quantità massima di spazio logico disponibile per gli oggetti del tenant. Se non viene fornita una metrica di quota, è disponibile una quantità illimitata di spazio.

Ottieni un elenco di tutte le metriche

per ottenere l'elenco completo delle metriche, utilizza l'API Grid Management.

1. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.
2. Individuare le operazioni **metriche**.
3. Eseguire `GET /grid/metric-names` operazione.
4. Scarica i risultati.

Gestire gli allarmi (sistema legacy)

Gestire gli allarmi (sistema legacy)

Il sistema di allarme StorageGRID è il sistema legacy utilizzato per identificare i punti di errore che talvolta si verificano durante il normale funzionamento.

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

Classi di allarme (sistema legacy)

Un allarme legacy può appartenere a una delle due classi di allarme che si escludono a vicenda.

- Gli allarmi predefiniti vengono forniti con ogni sistema StorageGRID e non possono essere modificati. Tuttavia, è possibile disattivare gli allarmi predefiniti o ignorarli definendo gli allarmi personalizzati globali.
- Gli allarmi personalizzati globali monitorano lo stato di tutti i servizi di un determinato tipo nel sistema StorageGRID. È possibile creare un allarme Global Custom per ignorare un allarme Default. È inoltre possibile creare un nuovo allarme Global Custom. Ciò può essere utile per monitorare qualsiasi condizione personalizzata del sistema StorageGRID.

Logica di attivazione degli allarmi (sistema legacy)

Un allarme legacy viene attivato quando un attributo StorageGRID raggiunge un valore di soglia che viene valutato come true rispetto a una combinazione di classe di allarme (predefinita o personalizzata globale) e livello di gravità dell'allarme.

Icona	Colore	Severità degli allarmi	Significato
	Giallo	Avviso	Il nodo è connesso alla rete, ma esiste una condizione insolita che non influisce sulle normali operazioni.
	Arancione chiaro	Minore	Il nodo è collegato alla rete, ma esiste una condizione anomala che potrebbe influire sul funzionamento in futuro. È necessario indagare per evitare l'escalation.
	Arancione scuro	Maggiore	Il nodo è collegato alla rete, ma esiste una condizione anomala che attualmente influisce sul funzionamento. Ciò richiede una rapida attenzione per evitare l'escalation.
	Rosso	Critico	Il nodo è connesso alla rete, ma esiste una condizione anomala che ha interrotto le normali operazioni. Il problema deve essere risolto immediatamente.

È possibile impostare la severità dell'allarme e il valore di soglia corrispondente per ogni attributo numerico. Il servizio NMS su ciascun nodo di amministrazione monitora continuamente i valori degli attributi correnti in base alle soglie configurate. Quando viene attivato un allarme, viene inviata una notifica a tutto il personale designato.

Si noti che un livello di severità normale non attiva un allarme.

I valori degli attributi vengono valutati in base all'elenco di allarmi abilitati definito per tale attributo. L'elenco degli allarmi viene controllato nel seguente ordine per individuare la prima classe di allarme con un allarme definito e attivato per l'attributo:

1. Allarmi personalizzati globali con livelli di interruzione degli allarmi da critici a avvisi.
2. Allarmi predefiniti con livelli di gravità degli allarmi da critico a Avviso.

Dopo che un allarme abilitato per un attributo viene trovato nella classe di allarme superiore, il servizio NMS valuta solo all'interno di tale classe. Il servizio NMS non valuterà le altre classi con priorità inferiore. In altri termini, se per un attributo è attivato un allarme Global Custom, il servizio NMS valuta solo il valore dell'attributo rispetto agli allarmi Global Custom. Gli allarmi predefiniti non vengono valutati. Pertanto, un allarme predefinito abilitato per un attributo può soddisfare i criteri necessari per attivare un allarme, ma non verrà attivato perché è attivato un allarme personalizzato globale (che non soddisfa i criteri specificati) per lo stesso attributo. Non viene attivato alcun allarme e non viene inviata alcuna notifica.

Esempio di attivazione degli allarmi

È possibile utilizzare questo esempio per comprendere come vengono attivati gli allarmi Global Custom e

Default.

Nell'esempio seguente, un attributo ha un allarme Global Custom e un allarme Default definiti e attivati come mostrato nella tabella seguente.

	Soglia di allarme Global Custom (abilitata)	**Soglia di allarme predefinita (attivata)**
Avviso	>= 1500	>= 1000
Minore	>= 15.000	>= 1000
Maggiore	>=150,000	>= 250.000

Se l'attributo viene valutato quando il suo valore è 1000, non viene attivato alcun allarme e non viene inviata alcuna notifica.

L'allarme Global Custom ha la precedenza sull'allarme Default. Un valore di 1000 non raggiunge il valore di soglia di alcun livello di severità per l'allarme Global Custom. Di conseguenza, il livello di allarme viene valutato come normale.

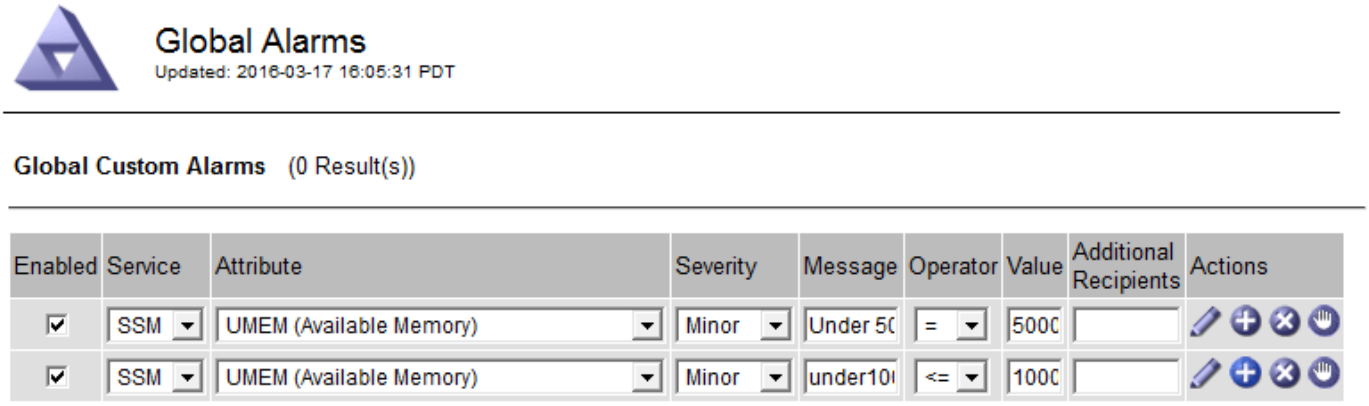
Dopo lo scenario precedente, se l'allarme Global Custom è disattivato, non cambia nulla. Il valore dell'attributo deve essere rivalutato prima che venga attivato un nuovo livello di allarme.

Se l'allarme Global Custom è disattivato, quando il valore dell'attributo viene rivalutato, il valore dell'attributo viene valutato in base ai valori di soglia per l'allarme Default. Il livello di allarme attiva un allarme di livello Notice e viene inviata una notifica via email al personale designato.

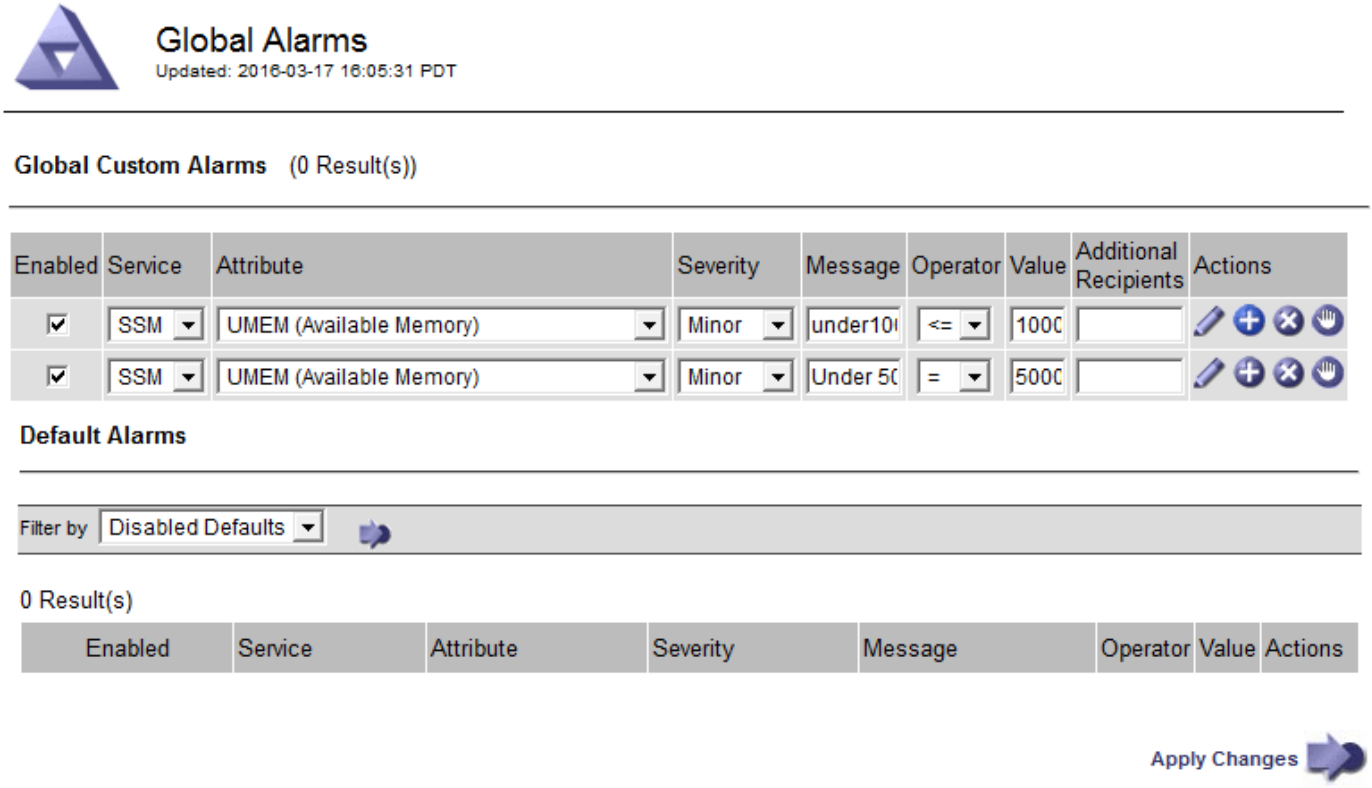
Allarmi della stessa severità

Se due allarmi personalizzati globali per lo stesso attributo hanno lo stesso livello di gravità, gli allarmi vengono valutati con una priorità "dall'alto verso il basso".

Ad esempio, se l'UMEM scende a 50 MB, viene attivato il primo allarme (= 50000000), ma non quello sottostante (⇐100000000).



Se l'ordine viene invertito, quando l'UMEM scende a 100 MB, viene attivato il primo allarme (⇐100000000), ma non quello sottostante (= 50000000).



Notifiche

Una notifica indica il verificarsi di un allarme o il cambiamento di stato di un servizio. Le notifiche di allarme possono essere inviate tramite e-mail o SNMP.

Per evitare l'invio di più allarmi e notifiche quando viene raggiunto un valore di soglia di allarme, la gravità dell'allarme viene controllata in base alla gravità corrente dell'attributo. Se non si verificano modifiche, non viene intrapresa alcuna azione. Ciò significa che mentre il servizio NMS continua a monitorare il sistema, genera un allarme e invia notifiche solo la prima volta che rileva una condizione di allarme per un attributo. Se viene raggiunta e rilevata una nuova soglia di valore per l'attributo, la gravità dell'allarme cambia e viene inviata una nuova notifica. Gli allarmi vengono cancellati quando le condizioni tornano al livello normale.

Il valore di attivazione visualizzato nella notifica di uno stato di allarme viene arrotondato a tre cifre decimali. Pertanto, un valore di attributo 1.9999 attiva un allarme la cui soglia è inferiore a (<) 2.0, anche se la notifica di allarme mostra il valore di attivazione come 2.0.

Nuovi servizi

Man mano che i nuovi servizi vengono aggiunti tramite l'aggiunta di nuovi nodi o siti della griglia, ereditano gli allarmi predefiniti e gli allarmi personalizzati globali.

Allarmi e tabelle

Gli attributi degli allarmi visualizzati nelle tabelle possono essere disattivati a livello di sistema. Non è possibile disattivare gli allarmi per singole righe di una tabella.

Ad esempio, la tabella seguente mostra due allarmi VMFI (Critical Entries Available). (Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi, selezionare ***Storage Node*** > **SSM** > **Resources**.)

È possibile disattivare l'allarme VMFI in modo che l'allarme VMFI di livello critico non venga attivato (entrambi gli allarmi attualmente critici vengono visualizzati in verde nella tabella); Tuttavia, non è possibile disattivare un

singolo allarme in una riga di tabella in modo che un allarme VMFI venga visualizzato come allarme di livello critico mentre l'altro rimane verde.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

Riconoscere gli allarmi correnti (sistema precedente)

Gli allarmi legacy vengono attivati quando gli attributi di sistema raggiungono i valori di soglia degli allarmi. Se si desidera ridurre o cancellare l'elenco degli allarmi legacy, è possibile confermarli.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- È necessario disporre dell'autorizzazione di riconoscimento degli allarmi.

A proposito di questa attività

Poiché il sistema di allarme legacy continua a essere supportato, l'elenco degli allarmi legacy nella pagina Allarmi correnti aumenta ogni volta che si verifica un nuovo allarme. In genere, è possibile ignorare gli allarmi (in quanto forniscono una migliore visualizzazione del sistema) oppure riconoscere gli allarmi.

> In alternativa, una volta eseguita la transizione completa al sistema di allerta, è possibile disattivare ciascun allarme legacy per evitare che venga attivato e aggiunto al numero di allarmi legacy.

Quando si riconosce un allarme, questo non viene più elencato nella pagina Current Alarms (Allarmi correnti) di Grid Manager, a meno che l'allarme non venga attivato al livello di severità successivo o venga risolto e riattivato.

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

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms

Last Refreshed: 2020-05-27 09:41:39 MDT

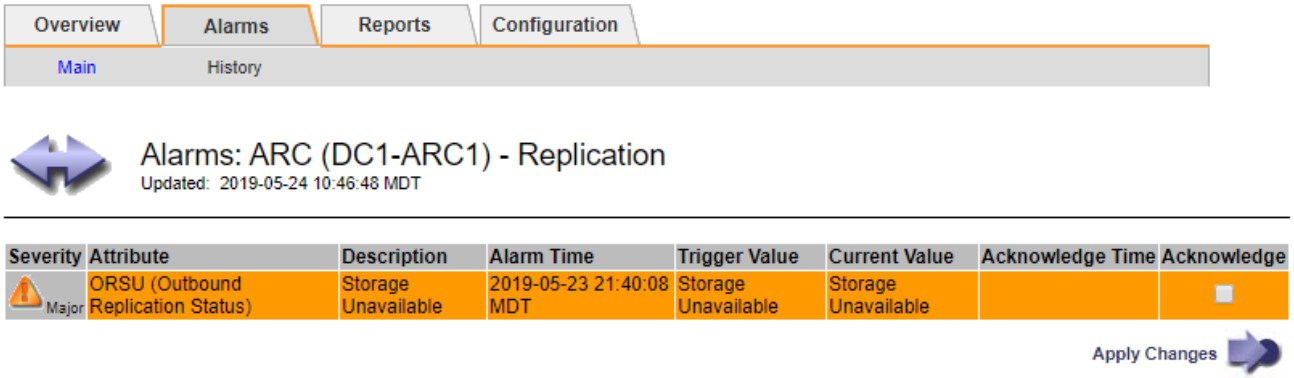
Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show 50 Records Per Page Refresh Previous « 1 » Next

2. Selezionare il nome del servizio nella tabella.

   Viene visualizzata la scheda Allarmi per il servizio selezionato (**SUPPORT** > **Tools** > **Grid topology** > ***Grid Node*** > ***Service*** > **Alarms**).



3. Selezionare la casella di controllo **Acknowledge** (Conferma) per l'allarme e fare clic su **Apply Changes** (Applica modifiche).

   L'allarme non viene più visualizzato nella dashboard o nella pagina Allarmi correnti.

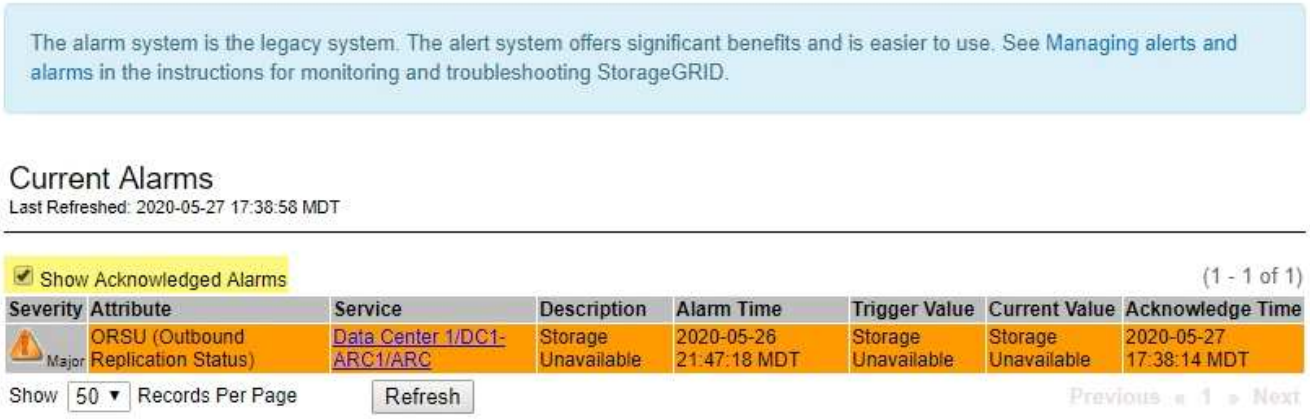
   > Quando si riconosce un allarme, la conferma non viene copiata in altri nodi di amministrazione. Per questo motivo, se si visualizza la dashboard da un altro nodo di amministrazione, è possibile continuare a visualizzare l'allarme attivo.

4. Se necessario, visualizzare gli allarmi confermati.

   a. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.

   b. Selezionare **Mostra allarmi confermati**.

      Vengono visualizzati tutti gli allarmi confermati.



Visualizza allarmi predefiniti (sistema legacy)

È possibile visualizzare l'elenco di tutti gli allarmi legacy predefiniti.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".

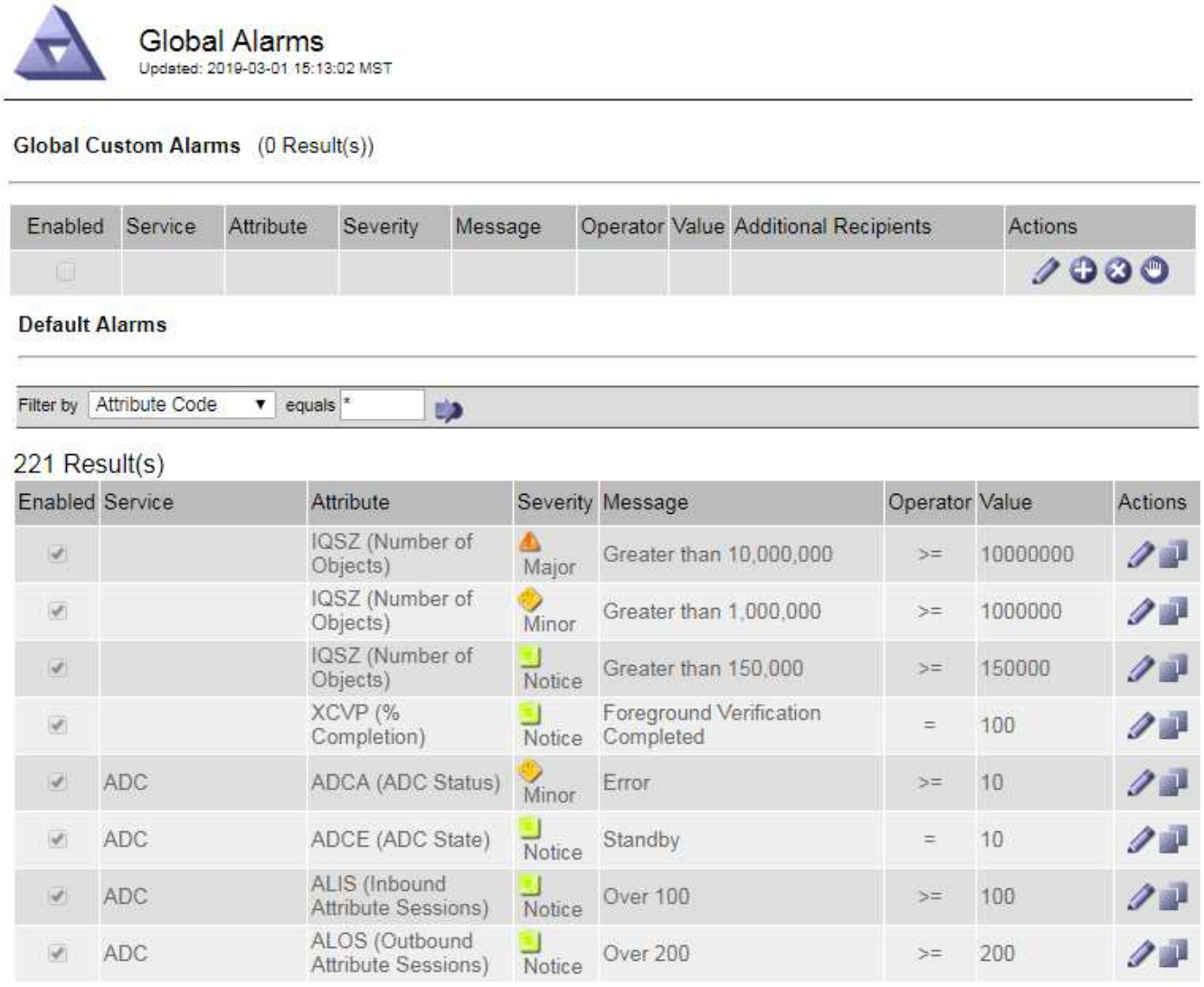
- Lo hai fatto "autorizzazioni di accesso specifiche".

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

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**.
2. Per Filtra per, selezionare **Codice attributo** o **Nome attributo**.
3. Per uguale, inserire un asterisco: *
4. Fare clic sulla freccia Oppure premere **Invio**.

   Vengono elencati tutti gli allarmi predefiniti.



Rivedere la cronologia degli allarmi e la frequenza degli allarmi (sistema precedente)

Durante la risoluzione di un problema, è possibile verificare la frequenza con cui un allarme legacy è stato attivato in passato.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

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

Fasi

1. Seguire questa procedura per ottenere un elenco di tutti gli allarmi attivati in un determinato periodo di tempo.
   a. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi storici**.
   b. Effettuare una delle seguenti operazioni:
      - Fare clic su uno dei periodi di tempo.
      - Immettere un intervallo personalizzato e fare clic su **Custom Query** (Query personalizzata).
2. Seguire questa procedura per scoprire la frequenza con cui sono stati attivati gli allarmi per un determinato attributo.
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***grid node*** > ***service o component*** > **Alarms** > **History**.
   c. Selezionare l'attributo dall'elenco.
   d. Effettuare una delle seguenti operazioni:
      - Fare clic su uno dei periodi di tempo.
      - Immettere un intervallo personalizzato e fare clic su **Custom Query** (Query personalizzata).

      Gli allarmi sono elencati in ordine cronologico inverso.
   e. Per tornare al modulo di richiesta della cronologia degli allarmi, fare clic su **Cronologia**.

Creazione di allarmi personalizzati globali (sistema legacy)

È possibile che siano stati utilizzati gli allarmi Global Custom per il sistema legacy per soddisfare specifici requisiti di monitoraggio. Gli allarmi Global Custom potrebbero avere livelli di allarme che prevalgono sugli allarmi predefiniti oppure potrebbero monitorare attributi che non hanno un allarme predefinito.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

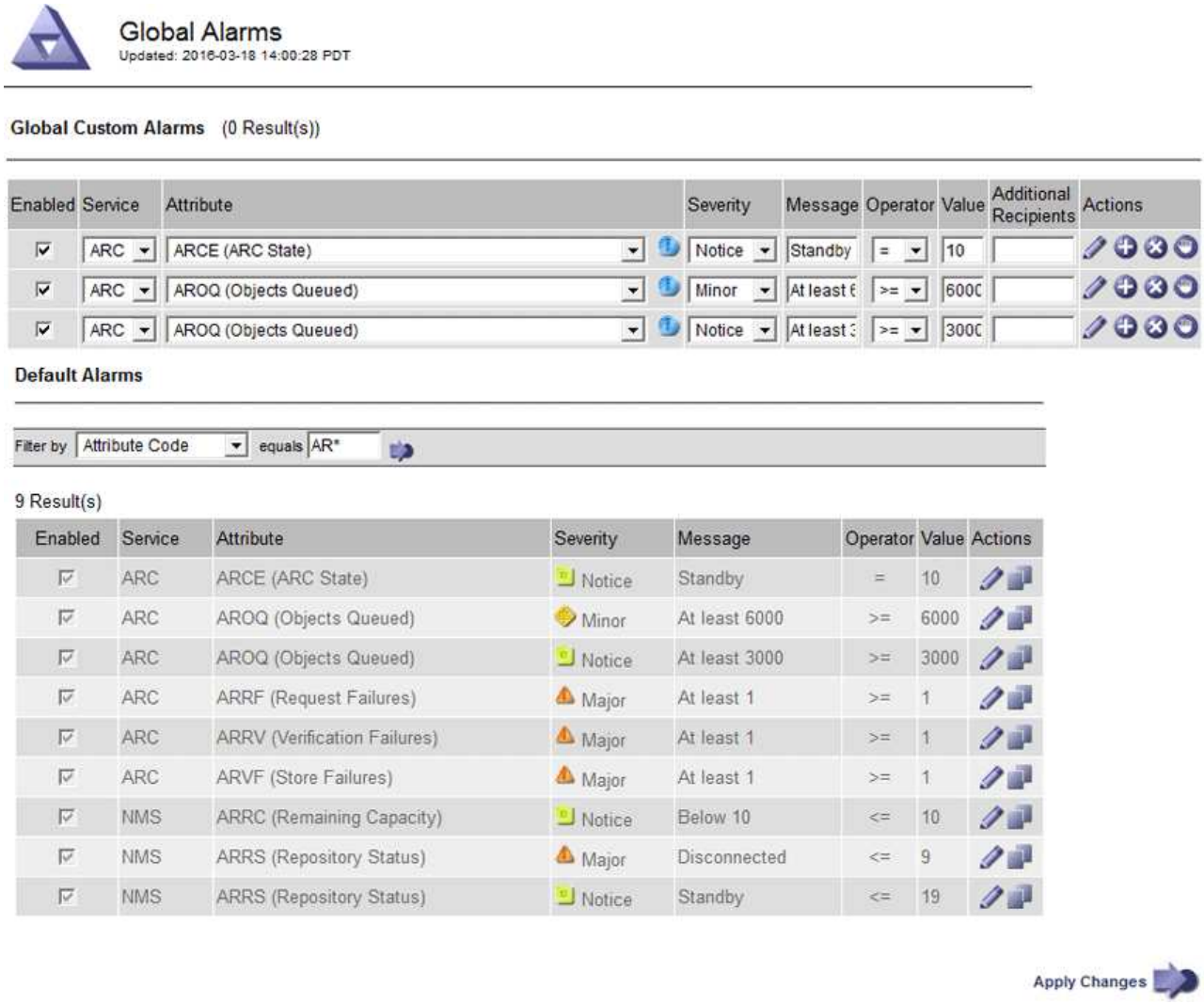
> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Gli allarmi Global Custom prevalgono sugli allarmi predefiniti. Non modificare i valori di allarme predefiniti, a meno che non sia assolutamente necessario. Modificando gli allarmi predefiniti, si corre il rischio di nascondere problemi che potrebbero altrimenti attivare un allarme.

> Prestare attenzione se si modificano le impostazioni della sveglia. Ad esempio, se si aumenta il valore di soglia per un allarme, potrebbe non essere rilevato un problema sottostante. Discutere le modifiche proposte con il supporto tecnico prima di modificare l'impostazione di un allarme.

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**.
2. Aggiungere una nuova riga alla tabella Global Custom Alarms (Allarmi personalizzati globali):
   - Per aggiungere un nuovo allarme, fare clic su **Edit** (Modifica) (Se si tratta della prima voce) o **Insert**.



   - Per modificare un allarme predefinito, cercare l'allarme predefinito.
     i. In Filtra per, selezionare **Codice attributo** o **Nome attributo**.
     ii. Digitare una stringa di ricerca.

     Specificare quattro caratteri o utilizzare caratteri jolly (Ad esempio, A???? O AB*). Gli asterischi (*) rappresentano più caratteri e punti interrogativi (?) rappresenta un singolo carattere.

     iii. Fare clic sulla freccia Oppure premere **Invio**.
     iv. Nell'elenco dei risultati, fare clic su **Copia** accanto all'allarme che si desidera modificare.

     L'allarme predefinito viene copiato nella tabella Global Custom Alarms (Allarmi personalizzati globali).
3. Apportare le modifiche necessarie alle impostazioni degli allarmi Global Custom:

Intestazione	Descrizione
Attivato	Selezionare o deselezionare la casella di controllo per attivare o disattivare l'allarme.
Attributo	Selezionare il nome e il codice dell'attributo monitorato dall'elenco di tutti gli attributi applicabili al servizio o al componente selezionato. Per visualizzare le informazioni relative all'attributo, fare clic su **Info** accanto al nome dell'attributo.
Severità	L'icona e il testo che indicano il livello dell'allarme.
Messaggio	Il motivo dell'allarme (connessione persa, spazio di storage inferiore al 10% e così via).
Operatore	Operatori per il test del valore dell'attributo corrente rispetto alla soglia del valore: • = uguale • > maggiore di • < meno di • >= maggiore o uguale a. • ⇐ minore o uguale a. • ≠ non uguale a.
Valore	Il valore di soglia dell'allarme utilizzato per eseguire il test in base al valore effettivo dell'attributo utilizzando l'operatore. La voce può essere un singolo numero, un intervallo di numeri specificato con due punti (1:3) o un elenco di numeri e intervalli delimitati da virgole.
Destinatari aggiuntivi	Un elenco supplementare di indirizzi e-mail da notificare quando viene attivato l'allarme. Oltre alla mailing list configurata nella pagina **Allarmi** > **Configurazione e-mail**. Gli elenchi sono delimitati da virgole. **Nota:** le mailing list richiedono la configurazione del server SMTP per funzionare. Prima di aggiungere mailing list, verificare che SMTP sia configurato. Le notifiche per gli allarmi personalizzati possono ignorare le notifiche degli allarmi Global Custom o Default.

Intestazione	Descrizione
Azioni	Pulsanti di controllo per: Modificare una riga + Inserire una riga + Eliminare una riga + Trascinare una riga verso l'alto o verso il basso + Copiare una riga

4. Fare clic su **Applica modifiche**.

Disattivazione degli allarmi (sistema legacy)

Gli allarmi nel sistema di allarme legacy sono attivati per impostazione predefinita, ma è possibile disattivarli che non sono necessari. È inoltre possibile disattivare gli allarmi legacy dopo la completa transizione al nuovo sistema di allerta.

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

Disattivazione di un allarme predefinito (sistema legacy)

È possibile disattivare uno degli allarmi predefiniti legacy per l'intero sistema.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

La disattivazione di un allarme per un attributo per il quale è attualmente attivato un allarme non cancella l'allarme corrente. L'allarme verrà disattivato al successivo superamento della soglia di allarme da parte dell'attributo oppure sarà possibile eliminare l'allarme attivato.

Non disattivare gli allarmi legacy fino a quando non si è passati completamente al nuovo sistema di allarme. In caso contrario, potrebbe non essere possibile rilevare un problema sottostante fino a quando non si è impedito il completamento di un'operazione critica.

Fasi

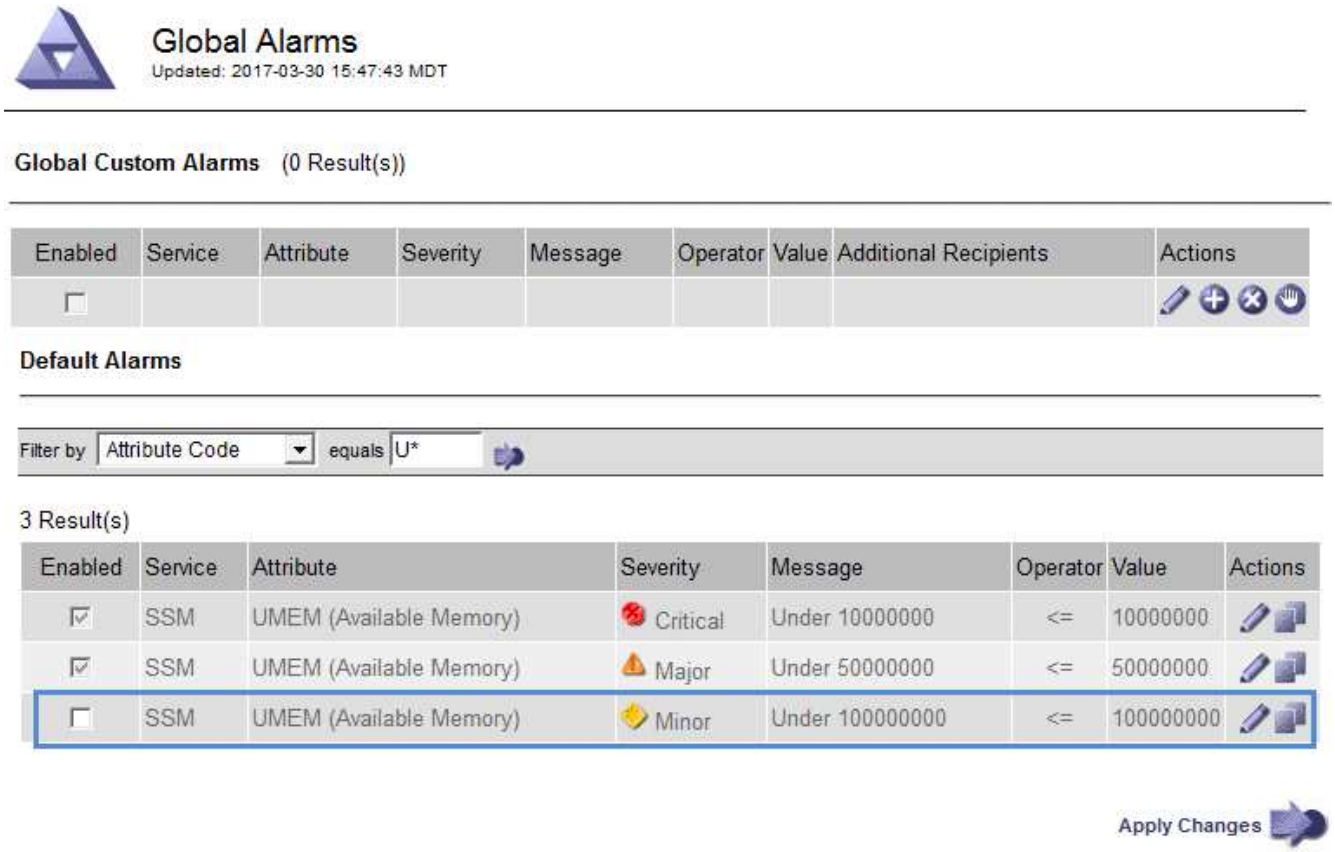
1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**.
2. Cercare l'allarme predefinito da disattivare.
   a. Nella sezione Allarmi predefiniti, selezionare **Filtra per** > **Codice attributo** o **Nome attributo**.
   b. Digitare una stringa di ricerca.

Specificare quattro caratteri o utilizzare caratteri jolly (Ad esempio, A???? O AB*). Gli asterischi (*) rappresentano più caratteri e punti interrogativi (?) rappresenta un singolo carattere.

c. Fare clic sulla freccia Oppure premere **Invio**.

> Selezionando **Disabled Defaults** (Impostazioni predefinite disabilitate) viene visualizzato un elenco di tutti gli allarmi predefiniti attualmente disattivati.

3. Nella tabella dei risultati della ricerca, fare clic sull'icona Modifica per la sveglia che si desidera disattivare.



La casella di controllo **Enabled** dell'allarme selezionato diventa attiva.

4. Deselezionare la casella di controllo **Enabled**.
5. Fare clic su **Applica modifiche**.

L'allarme predefinito è disattivato.

Disattiva allarmi Global Custom (sistema legacy)

È possibile disattivare un allarme Global Custom legacy per l'intero sistema.

Prima di iniziare

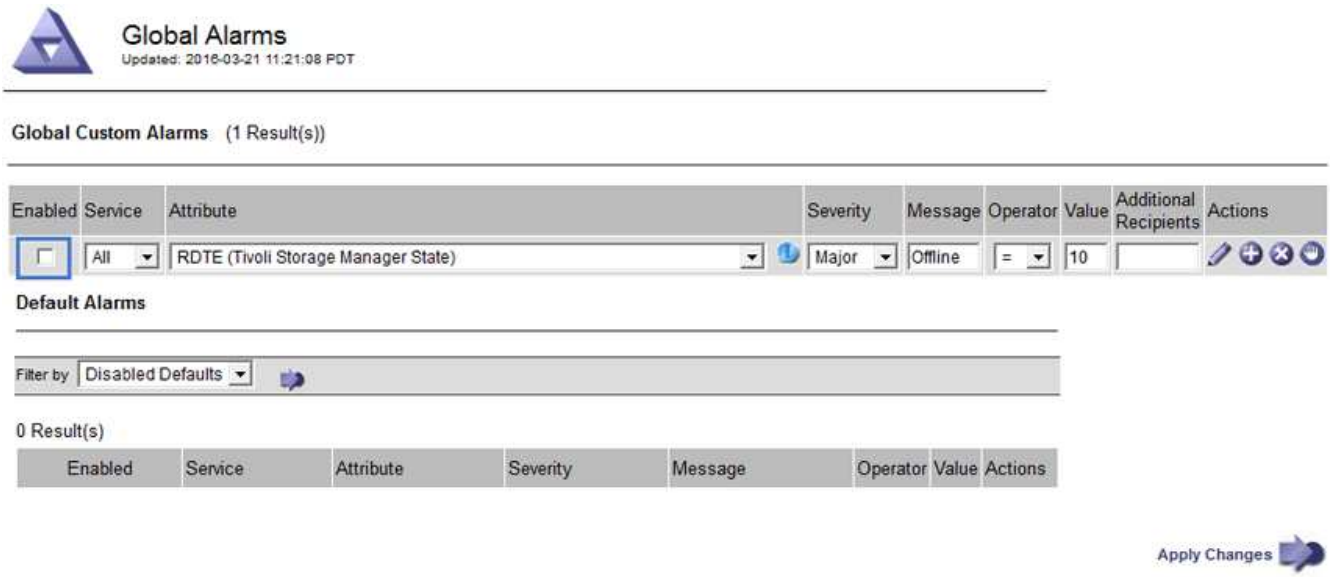
- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

La disattivazione di un allarme per un attributo per il quale è attualmente attivato un allarme non cancella l'allarme corrente. L'allarme verrà disattivato al successivo superamento della soglia di allarme da parte dell'attributo oppure sarà possibile eliminare l'allarme attivato.

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**.
2. Nella tabella Global Custom Alarms (Allarmi personalizzati globali), fare clic su **Edit** (Modifica) accanto all'allarme che si desidera disattivare.
3. Deselezionare la casella di controllo **Enabled**.



4. Fare clic su **Applica modifiche**.

   L'allarme Global Custom è disattivato.

Cancellazione degli allarmi attivati (sistema precedente)

Se viene attivato un allarme legacy, è possibile cancellarlo invece di confermarlo.

Prima di iniziare

- È necessario disporre di `Passwords.txt` file.

La disattivazione di un allarme per un attributo per il quale è attualmente attivato un allarme non cancella l'allarme. L'allarme verrà disattivato alla successiva modifica dell'attributo. È possibile riconoscere l'allarme oppure, se si desidera annullare immediatamente l'allarme anziché attendere la modifica del valore dell'attributo (con conseguente modifica dello stato dell'allarme), è possibile annullare l'allarme attivato. Questa operazione potrebbe essere utile se si desidera eliminare immediatamente un allarme in relazione a un attributo il cui valore non cambia spesso (ad esempio, gli attributi di stato).

1. Disattiva l'allarme.
2. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: *`ssh admin@primary_Admin_Node_IP`*
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`

d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

3. Riavviare il servizio NMS: `service nms restart`
4. Disconnettersi dal nodo di amministrazione: `exit`

   L'allarme viene cancellato.

Configurazione delle notifiche per gli allarmi (sistema legacy)

Il sistema StorageGRID può inviare automaticamente e-mail e. "Notifiche SNMP" quando viene attivato un allarme o quando cambia lo stato di servizio.

Per impostazione predefinita, le notifiche e-mail di allarme non vengono inviate. Per le notifiche e-mail, è necessario configurare il server e-mail e specificare i destinatari. Per le notifiche SNMP, è necessario configurare l'agente SNMP.

Tipi di notifiche di allarme (sistema legacy)

Quando viene attivato un allarme legacy, il sistema StorageGRID invia due tipi di notifiche di allarme: Livello di severità e stato del servizio.

Notifiche del livello di severità

Quando viene attivato un allarme legacy a un livello di severità selezionato, viene inviata una notifica via email:

- Avviso
- Minore
- Maggiore
- Critico

Una mailing list riceve tutte le notifiche relative all'allarme per la severità selezionata. Quando l'allarme esce dal livello di allarme, viene inviata una notifica tramite risoluzione o immissione di un livello di gravità diverso.

Notifiche dello stato del servizio

Viene inviata una notifica dello stato del servizio quando un servizio (ad esempio, il servizio LDR o il servizio NMS) entra nello stato del servizio selezionato e lascia lo stato del servizio selezionato. Le notifiche dello stato del servizio vengono inviate quando un servizio entra o lascia uno dei seguenti stati del servizio:

- Sconosciuto
- Amministrazione non disponibile

Una mailing list riceve tutte le notifiche relative ai cambiamenti nello stato selezionato.

Configurare le impostazioni del server di posta elettronica per gli allarmi (sistema legacy)

Se si desidera che StorageGRID invii notifiche e-mail quando viene attivato un allarme legacy, è necessario specificare le impostazioni del server di posta SMTP. Il sistema StorageGRID invia solo e-mail; non può ricevere e-mail.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Utilizzare queste impostazioni per definire il server SMTP utilizzato per le notifiche e-mail di allarme legacy e i messaggi e-mail AutoSupport. Queste impostazioni non vengono utilizzate per le notifiche degli avvisi.

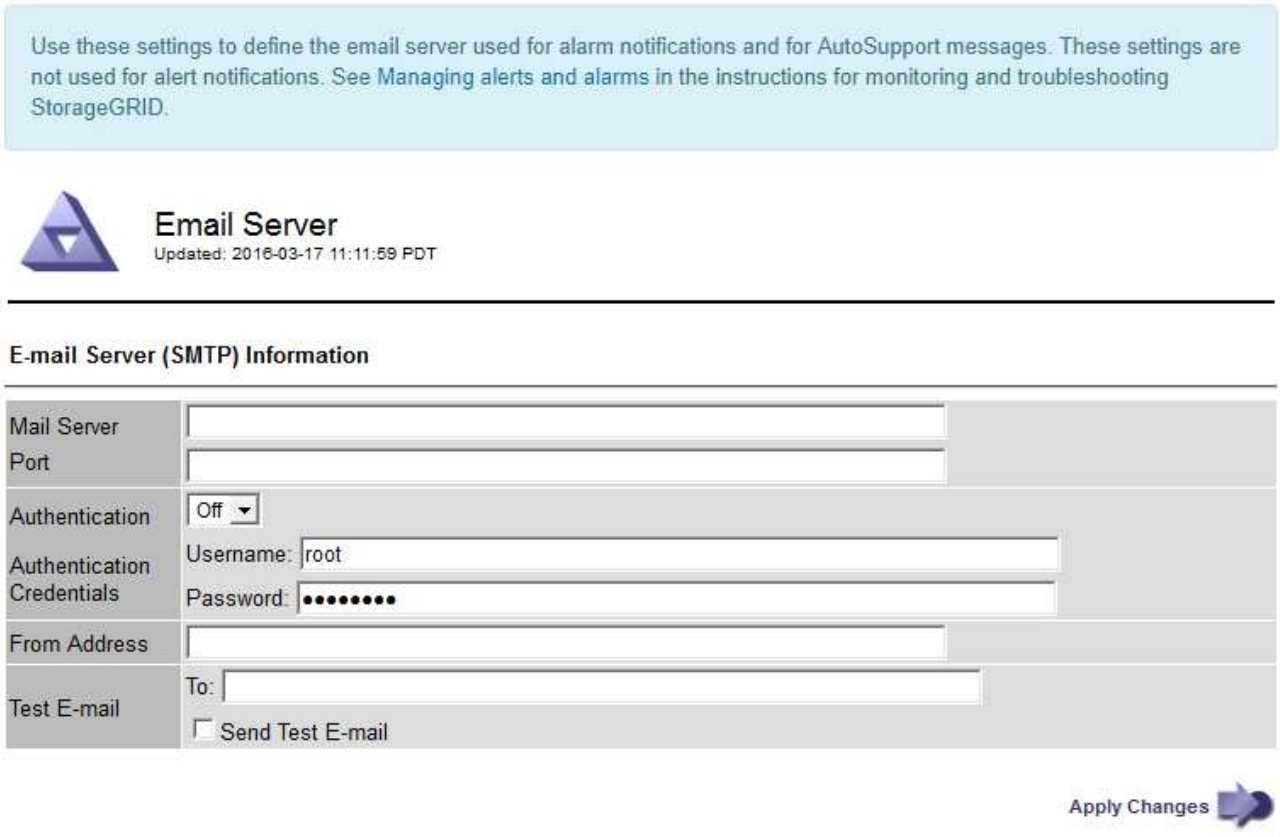
> Se si utilizza SMTP come protocollo per i pacchetti AutoSupport, è possibile che sia già stato configurato un server di posta SMTP. Lo stesso server SMTP viene utilizzato per le notifiche e-mail di allarme, pertanto è possibile saltare questa procedura. Vedere "Istruzioni per l'amministrazione di StorageGRID".

SMTP è l'unico protocollo supportato per l'invio di e-mail.

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **Server**.

   Viene visualizzata la pagina Server di posta elettronica. Questa pagina viene utilizzata anche per configurare il server di posta elettronica per i pacchetti AutoSupport.



3. Aggiungere le seguenti impostazioni del server di posta SMTP:

Elemento	Descrizione
Server di posta	Indirizzo IP del server di posta SMTP. È possibile inserire un nome host anziché un indirizzo IP se in precedenza sono state configurate le impostazioni DNS nel nodo di amministrazione.
Porta	Numero di porta per accedere al server di posta SMTP.
Autenticazione	Consente l'autenticazione del server di posta SMTP. Per impostazione predefinita, l'autenticazione è disattivata.
Credenziali di autenticazione	Nome utente e password del server di posta SMTP. Se l'opzione Authentication (autenticazione) è impostata su on, è necessario fornire un nome utente e una password per accedere al server di posta SMTP.

4. Sotto **Indirizzo mittente**, immettere un indirizzo e-mail valido che il server SMTP riconoscerà come indirizzo e-mail di invio. Indirizzo e-mail ufficiale da cui viene inviato il messaggio e-mail.
5. Facoltativamente, inviare un'e-mail di prova per confermare che le impostazioni del server di posta SMTP sono corrette.
   a. Nella casella **e-mail di prova** > **a**, aggiungere uno o più indirizzi ai quali è possibile accedere.

      È possibile inserire un singolo indirizzo e-mail o un elenco di indirizzi e-mail delimitati da virgole. Poiché il servizio NMS non conferma l'esito positivo o negativo dell'invio di un'e-mail di prova, è necessario controllare la posta in arrivo del destinatario del test.

   b. Selezionare **Invia e-mail di prova**.
6. Fare clic su **Applica modifiche**.

   Le impostazioni del server di posta SMTP vengono salvate. Se sono state inserite informazioni per un'e-mail di prova, tale e-mail viene inviata. I messaggi di posta elettronica di prova vengono inviati immediatamente al server di posta e non attraverso la coda delle notifiche. In un sistema con più nodi di amministrazione, ogni nodo di amministrazione invia un'email. La ricezione dell'email di prova conferma che le impostazioni del server di posta SMTP sono corrette e che il servizio NMS si sta connettendo correttamente al server di posta. Un problema di connessione tra il servizio NMS e il server di posta attiva l'allarme MIN legacy (NMS Notification Status) al livello di gravità minore.

Creazione di modelli e-mail di allarme (sistema legacy)

I modelli e-mail consentono di personalizzare l'intestazione, il piè di pagina e l'oggetto di una notifica e-mail di allarme legacy. È possibile utilizzare i modelli e-mail per inviare notifiche univoche contenenti lo stesso corpo del testo a diverse mailing list.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

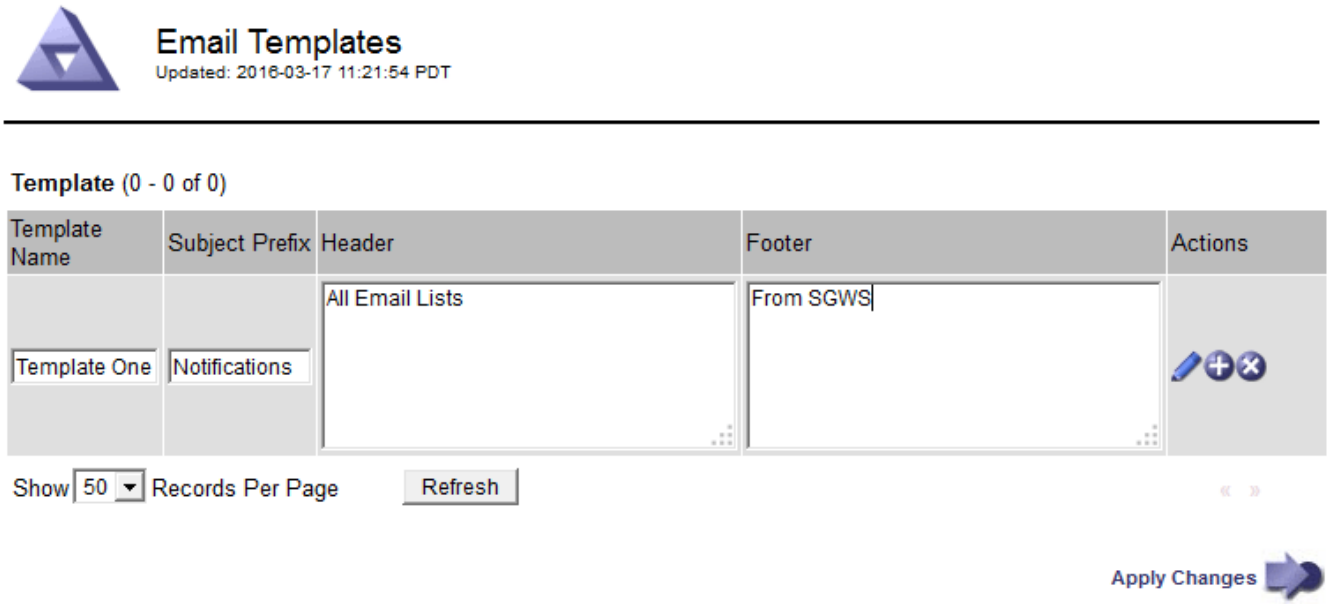
A proposito di questa attività

Utilizzare queste impostazioni per definire i modelli e-mail utilizzati per le notifiche di allarme legacy. Queste impostazioni non vengono utilizzate per le notifiche degli avvisi.

Diverse mailing list potrebbero richiedere informazioni di contatto diverse. I modelli non includono il corpo del messaggio e-mail.

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **modelli**.
3. Fare clic su **Edit** (Modifica) (O **Inserisci** se questo non è il primo modello).



4. Nella nuova riga aggiungere quanto segue:

Elemento	Descrizione
Nome modello	Nome univoco utilizzato per identificare il modello. I nomi dei modelli non possono essere duplicati.
Prefisso soggetto	Opzionale. Prefisso che verrà visualizzato all'inizio dell'oggetto dell'e-mail. I prefissi possono essere utilizzati per configurare facilmente i filtri e-mail e organizzare le notifiche.
Intestazione	Opzionale. Testo dell'intestazione visualizzato all'inizio del corpo del messaggio di posta elettronica. Il testo dell'intestazione può essere utilizzato per anteporre al contenuto del messaggio di posta elettronica informazioni quali nome e indirizzo della società.
Piè di pagina	Opzionale. Testo a piè di pagina visualizzato alla fine del corpo del messaggio di posta elettronica. Il testo a piè di pagina può essere utilizzato per chiudere il messaggio e-mail con informazioni di promemoria come un numero di telefono di un contatto o un collegamento a un sito Web.

5. Fare clic su **Applica modifiche**.

   Viene aggiunto un nuovo modello per le notifiche.

Creare mailing list per le notifiche di allarme (sistema legacy)

Le mailing list consentono di notificare ai destinatari quando viene attivato un allarme legacy o quando cambia lo stato di un servizio. È necessario creare almeno una mailing list prima di poter inviare notifiche di allarme via email. Per inviare una notifica a un singolo destinatario, creare una mailing list con un indirizzo e-mail.

Prima di iniziare

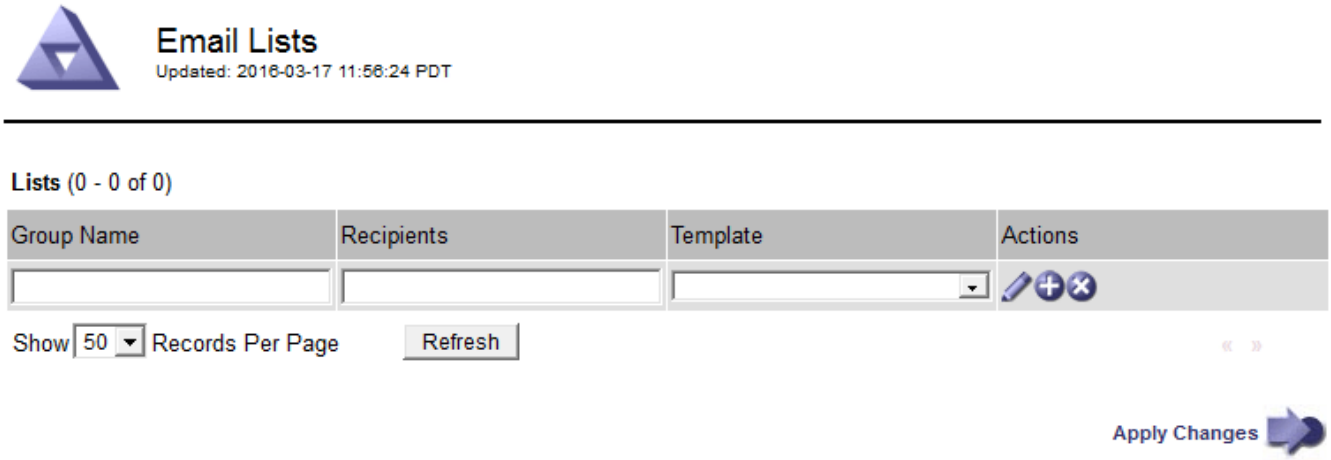
- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Se si desidera specificare un modello e-mail per la mailing list (intestazione personalizzata, piè di pagina e oggetto), è necessario aver già creato il modello.

A proposito di questa attività

Utilizzare queste impostazioni per definire le mailing list utilizzate per le notifiche e-mail di allarme legacy. Queste impostazioni non vengono utilizzate per le notifiche degli avvisi.

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **Liste**.
3. Fare clic su **Edit** (Modifica) (O *Inserisci* se questa non è la prima mailing list).



4. Nella nuova riga, aggiungere quanto segue:

Elemento	Descrizione
Nome gruppo	Nome univoco utilizzato per identificare la mailing list. I nomi delle mailing list non possono essere duplicati. **Nota:** se si modifica il nome di una mailing list, la modifica non viene propagata alle altre posizioni che utilizzano il nome della mailing list. È necessario aggiornare manualmente tutte le notifiche configurate per utilizzare il nuovo nome della mailing list.

Elemento	Descrizione
Destinatari	Singolo indirizzo e-mail, una mailing list precedentemente configurata o un elenco di indirizzi e-mail e mailing list delimitati da virgole a cui verranno inviate le notifiche. **Nota:** se un indirizzo e-mail appartiene a più mailing list, viene inviata solo una notifica e-mail quando si verifica un evento di attivazione della notifica.
Modello	Se si desidera, selezionare un modello e-mail per aggiungere un'intestazione, un piè di pagina e una riga dell'oggetto univoci alle notifiche inviate a tutti i destinatari della mailing list.

5. Fare clic su **Applica modifiche**.

   Viene creata una nuova mailing list.

Configurazione delle notifiche e-mail per gli allarmi (sistema legacy)

Per ricevere notifiche via email per il sistema di allarme legacy, i destinatari devono essere membri di una mailing list e tale elenco deve essere aggiunto alla pagina Notifiche. Le notifiche sono configurate in modo da inviare e-mail ai destinatari solo quando viene attivato un allarme con un livello di gravità specificato o quando cambia lo stato di un servizio. Pertanto, i destinatari ricevono solo le notifiche necessarie.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- È necessario aver configurato un elenco e-mail.

A proposito di questa attività

Utilizzare queste impostazioni per configurare le notifiche per gli allarmi legacy. Queste impostazioni non vengono utilizzate per le notifiche degli avvisi.

Se un indirizzo e-mail (o un elenco) appartiene a più mailing list, viene inviata una sola notifica e-mail quando si verifica un evento di attivazione della notifica. Ad esempio, un gruppo di amministratori all'interno dell'organizzazione può essere configurato per ricevere notifiche per tutti gli allarmi, indipendentemente dalla gravità. Un altro gruppo potrebbe richiedere notifiche solo per gli allarmi con un livello di gravità critico. È possibile appartenere a entrambi gli elenchi. Se viene attivato un allarme critico, si riceve una sola notifica.

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **Notifiche**.
3. Fare clic su **Edit** (Modifica) (O *Inserisci* se questa non è la prima notifica).
4. In elenco e-mail, selezionare la mailing list.
5. Selezionare uno o più livelli di severità degli allarmi e stati del servizio.
6. Fare clic su **Applica modifiche**.

   Le notifiche vengono inviate alla mailing list quando vengono attivati o modificati gli allarmi con il livello di

gravità dell'allarme o lo stato di servizio selezionato.

Eliminazione delle notifiche di allarme per una mailing list (sistema legacy)

È possibile eliminare le notifiche di allarme per una mailing list quando non si desidera più ricevere le notifiche relative agli allarmi. Ad esempio, è possibile eliminare le notifiche relative agli allarmi legacy dopo la transizione all'utilizzo delle notifiche e-mail di avviso.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Utilizzare queste impostazioni per eliminare le notifiche e-mail per il sistema di allarme legacy. Queste impostazioni non si applicano alle notifiche e-mail di avviso.

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

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **Notifiche**.
3. Fare clic su **Edit** (Modifica) accanto alla mailing list per la quale si desidera eliminare le notifiche.
4. In Sospendi, selezionare la casella di controllo accanto alla mailing list che si desidera sospendere oppure selezionare **Sospendi** nella parte superiore della colonna per eliminare tutte le mailing list.
5. Fare clic su **Applica modifiche**.

   Le notifiche di allarme legacy vengono soppresse per le mailing list selezionate.

Visualizzare gli allarmi legacy

Gli allarmi (sistema legacy) vengono attivati quando gli attributi di sistema raggiungono i valori di soglia degli allarmi. È possibile visualizzare gli allarmi attualmente attivi dalla pagina Allarmi correnti.

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

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".

Fasi

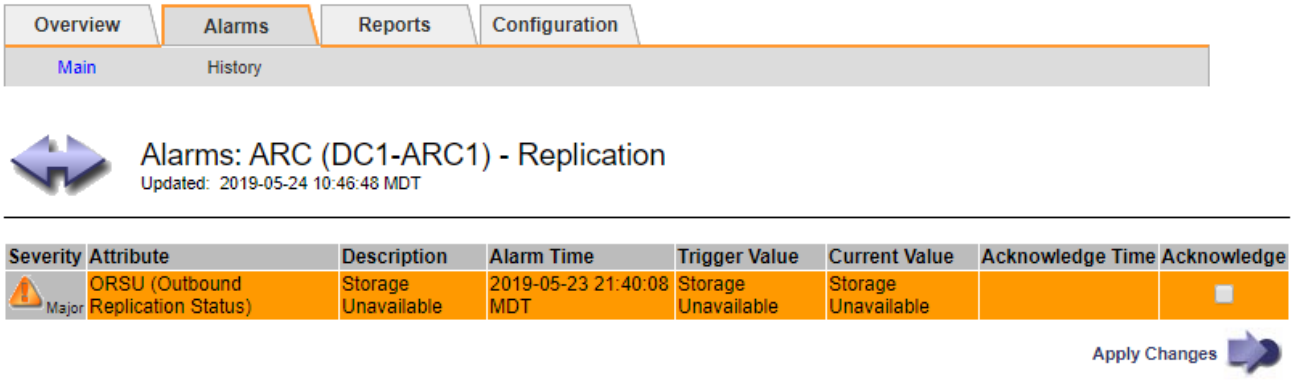
1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.

L'icona di allarme indica la gravità di ciascun allarme, come indicato di seguito:

Icona	Colore	Severità degli allarmi	Significato
	Giallo	Avviso	Il nodo è connesso alla rete, ma esiste una condizione insolita che non influisce sulle normali operazioni.
	Arancione chiaro	Minore	Il nodo è collegato alla rete, ma esiste una condizione anomala che potrebbe influire sul funzionamento in futuro. È necessario indagare per evitare l'escalation.
	Arancione scuro	Maggiore	Il nodo è collegato alla rete, ma esiste una condizione anomala che attualmente influisce sul funzionamento. Ciò richiede una rapida attenzione per evitare l'escalation.
	Rosso	Critico	Il nodo è connesso alla rete, ma esiste una condizione anomala che ha interrotto le normali operazioni. Il problema deve essere risolto immediatamente.

2. Per informazioni sull'attributo che ha causato l'attivazione dell'allarme, fare clic con il pulsante destro del mouse sul nome dell'attributo nella tabella.
3. Per visualizzare ulteriori dettagli su un allarme, fare clic sul nome del servizio nella tabella.

   Viene visualizzata la scheda Allarmi per il servizio selezionato (**SUPPORT** > **Tools** > **Grid topology** > ***Grid Node*** > ***Service*** > **Alarms**).



4. Se si desidera azzerare il conteggio degli allarmi correnti, è possibile eseguire le seguenti operazioni:
   - Riconoscere l'allarme. Un allarme confermato non viene più incluso nel conteggio degli allarmi legacy a meno che non venga attivato al livello di severità successivo o venga risolto e si verifichi di nuovo.
   - Disattivare un particolare allarme predefinito o Global Custom per l'intero sistema per evitare che venga attivato nuovamente.

Informazioni correlate

"Riferimento allarmi (sistema legacy)"

"Riconoscere gli allarmi correnti (sistema precedente)"

"Disattivazione degli allarmi (sistema legacy)"

Riferimento allarmi (sistema legacy)

La tabella seguente elenca tutti gli allarmi predefiniti legacy. Se viene attivato un allarme, è possibile cercare il codice di allarme in questa tabella per individuare le azioni consigliate.

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

Codice	Nome	Servizio	Azione consigliata
ABRL	Relè attributi disponibili	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Ripristinare la connettività a un servizio (un servizio ADC) che esegue un Attribute Relay Service il prima possibile. Se non sono presenti relay di attributi connessi, il nodo della griglia non può riportare i valori di attributo al servizio NMS. Pertanto, il servizio NMS non può più monitorare lo stato del servizio o aggiornare gli attributi del servizio. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
ACMS	Servizi metadati disponibili	BARC, BLDR, BCMN	Viene attivato un allarme quando un servizio LDR o ARC perde la connessione a un servizio DDS. In questo caso, le transazioni di acquisizione o recupero non possono essere elaborate. Se l'indisponibilità dei servizi DDS è solo un breve problema transitorio, le transazioni possono essere ritardate. Controllare e ripristinare le connessioni a un servizio DDS per annullare questo allarme e ripristinare il servizio alla funzionalità completa.
ATTI	Stato del servizio di tiering cloud	ARCO	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Cloud Tiering - Simple Storage Service (S3). Se l'attributo ACTS per il nodo di archiviazione è impostato su sola lettura abilitata o lettura/scrittura disabilitata, è necessario impostare l'attributo su lettura/scrittura abilitata. Se viene attivato un allarme grave a causa di un errore di autenticazione, verificare le credenziali associate al bucket di destinazione e aggiornare i valori, se necessario. Se viene attivato un allarme grave per qualsiasi altro motivo, contattare il supporto tecnico.
ADCA	Stato ADC	ADC	Se viene attivato un allarme, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Grid node*** > **ADC** > **Overview** > **Main** e **ADC** > **Alarms** > **Main** per determinare la causa dell'allarme. Se il problema persiste, contattare il supporto tecnico.
ADCE	Stato ADC	ADC	Se il valore di ADC state (Stato ADC) è Standby, continuare il monitoraggio del servizio e, se il problema persiste, contattare il supporto tecnico. Se il valore di Stato ADC è offline, riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
AITE	Recupera stato	BARC	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Tivoli Storage Manager (TSM). Se il valore Retrieve state (Stato recupero) è Waiting for Target (in attesa di destinazione), controllare il server middleware TSM e assicurarsi che funzioni correttamente. Se il nodo di archiviazione è stato appena aggiunto al sistema StorageGRID, assicurarsi che la connessione del nodo di archiviazione al sistema di archiviazione esterno di destinazione sia configurata correttamente. Se il valore di Archive Retrieve state (Stato recupero archivio) è Offline (non in linea), provare ad aggiornare lo stato in Online. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Grid node*** > **ARC** > **Recupera** > **Configurazione** > **principale**, selezionare **Archive Retrieve state** > **Online** e fare clic su **Apply Changes**. Se il problema persiste, contattare il supporto tecnico.
AITU	Recupera stato	BARC	Se il valore di Recupera stato è Target Error (errore di destinazione), verificare la presenza di errori nel sistema di storage di archiviazione esterno di destinazione. Se il valore di Archive Retrieve Status (Stato recupero archivio) è Session Lost (sessione persa), controllare il sistema di storage di archiviazione esterno di destinazione per assicurarsi che sia online e funzioni correttamente. Verificare la connessione di rete con la destinazione. Se il valore di Archive Retrieve Status (Stato recupero archivio) è Unknown Error (errore sconosciuto), contattare il supporto tecnico.
ALIS	Sessioni di attributi inbound	ADC	Se il numero di sessioni di attributi in entrata su un relay di attributi aumenta troppo, può essere un'indicazione che il sistema StorageGRID è diventato sbilanciato. In condizioni normali, le sessioni degli attributi devono essere distribuite uniformemente tra i servizi ADC. Uno squilibrio può causare problemi di performance. Se il problema persiste, contattare il supporto tecnico.
ALOS	Sessioni di attributi in uscita	ADC	Il servizio ADC ha un numero elevato di sessioni di attributi e sta diventando sovraccarico. Se questo allarme viene attivato, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
ALUR	Repository di attributi non raggiungibili	ADC	Verificare la connettività di rete con il servizio NMS per assicurarsi che il servizio possa contattare il repository degli attributi. Se questo allarme viene attivato e la connettività di rete è buona, contattare il supporto tecnico.
AMQS	Messaggi di controllo in coda	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Se i messaggi di audit non possono essere inoltrati immediatamente a un relay di audit o a un repository, i messaggi vengono memorizzati in una coda di dischi. Se la coda dei dischi si esaurisce, possono verificarsi interruzioni. Per consentire di rispondere in tempo per evitare un'interruzione, gli allarmi AMQS vengono attivati quando il numero di messaggi nella coda del disco raggiunge le seguenti soglie: • Avviso: Più di 100,000 messaggi • Minore: Almeno 500,000 messaggi • Maggiore: Almeno 2,000,000 messaggi • Critico: Almeno 5,000,000 messaggi Se viene attivato un allarme AMQS, controllare il carico sul sistema. Se si è verificato un numero significativo di transazioni, l'allarme dovrebbe risolversi automaticamente nel tempo. In questo caso, è possibile ignorare l'allarme. Se l'allarme persiste e aumenta di severità, visualizzare un grafico delle dimensioni della coda. Se il numero aumenta costantemente nel corso di ore o giorni, il carico di audit ha probabilmente superato la capacità di audit del sistema. Ridurre la velocità operativa del client o diminuire il numero di messaggi di audit registrati cambiando il livello di audit in Error (errore) o Off (Disattivato). Vedere "Configurare i messaggi di audit e le destinazioni dei log".

Codice	Nome	Servizio	Azione consigliata
AOTE	Store state (Stato archiviazione)	BARC	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Tivoli Storage Manager (TSM). Se il valore di Store state è in attesa di Target, controllare il sistema di storage di archiviazione esterno e assicurarsi che funzioni correttamente. Se il nodo di archiviazione è stato appena aggiunto al sistema StorageGRID, assicurarsi che la connessione del nodo di archiviazione al sistema di archiviazione esterno di destinazione sia configurata correttamente. Se il valore di Store state è offline, controlla il valore di Store Status. Correggere eventuali problemi prima di riportare lo stato dello store in linea.
AOTU	Stato del negozio	BARC	Se il valore di Store Status (Stato negozio) è Session Lost (sessione persa), verificare che il sistema di storage di archiviazione esterno sia connesso e online. Se il valore di Target Error (errore di destinazione), verificare la presenza di errori nel sistema di storage di archiviazione esterno. Se il valore di Stato negozio è Unknown Error, contattare il supporto tecnico.
APM	Connettività storage multipath	SSM	Se l'allarme di stato multipercorso viene visualizzato come "danneggiato" (selezionare **SUPPORTO** > **Strumenti** > **topologia griglia**, quindi selezionare ***sito*** > ***nodo griglia*** > **SSM** > **Eventi**), procedere come segue: 1. Collegare o sostituire il cavo che non visualizza spie luminose. 2. Attendere da uno a cinque minuti. Non scollegare l'altro cavo fino a cinque minuti dopo aver collegato il primo cavo. Se si scollega troppo presto, il volume root può diventare di sola lettura, il che richiede il riavvio dell'hardware. 3. Tornare alla pagina **SSM** > **risorse** e verificare che lo stato del multipath "degradato" sia stato modificato in "nominale" nella sezione hardware di archiviazione.

Codice	Nome	Servizio	Azione consigliata
ARCE	ARC state (Stato ARCO)	ARCO	Il servizio ARC ha uno stato di standby fino all'avvio di tutti i componenti ARC (Replication, Store, Retrieve, Target). Passa quindi a Online. Se il valore dello stato ARC non passa da Standby a Online, controllare lo stato dei componenti ARC. Se il valore di ARC state (Stato arco) è Offline (non in linea), riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
AROQ	Oggetti in coda	ARCO	Questo allarme può essere attivato se il dispositivo di storage rimovibile è lento a causa di problemi con il sistema di storage di archiviazione esterno di destinazione o se si verificano errori di lettura multipli. Verificare la presenza di errori nel sistema di storage di archiviazione esterno e assicurarsi che funzioni correttamente. In alcuni casi, questo errore può verificarsi a causa di un elevato numero di richieste di dati. Monitorare il numero di oggetti accodati quando l'attività di sistema diminuisce.

Codice	Nome	Servizio	Azione consigliata
ARRF	Errori della richiesta	ARCO	Se un recupero dal sistema di storage di archiviazione esterno di destinazione non riesce, il nodo di archiviazione tenta di nuovo il recupero in quanto l'errore può essere dovuto a un problema transitorio. Tuttavia, se i dati dell'oggetto sono corrotti o sono stati contrassegnati come indisponibili in modo permanente, il recupero non avrà esito negativo. Invece, il nodo di archiviazione tenta continuamente il recupero e il valore di Request Failures continua ad aumentare. Questo allarme può indicare che il supporto di memorizzazione contenente i dati richiesti è corrotto. Controllare il sistema di storage di archiviazione esterno per diagnosticare ulteriormente il problema. Se si determina che i dati dell'oggetto non sono più presenti nell'archivio, l'oggetto dovrà essere rimosso dal sistema StorageGRID. Per ulteriori informazioni, contatta il supporto tecnico. Una volta risolto il problema che ha attivato questo allarme, ripristinare il conteggio degli errori. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Grid node*** > **ARC** > **Recupera** > **Configurazione** > **principale**, selezionare **Reset Request Failure Count** e fare clic su **Apply Changes**.
ARRV	Errori di verifica	ARCO	Per diagnosticare e correggere questo problema, contattare il supporto tecnico. Dopo aver risolto il problema che ha generato questo allarme, azzerare il conteggio dei guasti. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **ARC** > **Recupera** > **Configurazione** > **principale**, selezionare **Reset Verification Failure Count** e fare clic su **Apply Changes**.

Codice	Nome	Servizio	Azione consigliata
ARVF	Guasti del negozio	ARCO	Questo allarme può verificarsi in seguito a errori del sistema di storage di archiviazione esterno di destinazione. Verificare la presenza di errori nel sistema di storage di archiviazione esterno e assicurarsi che funzioni correttamente. Una volta risolto il problema che ha attivato questo allarme, ripristinare il conteggio degli errori. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **ARC** > **Recupera** > **Configurazione** > **principale**, selezionare **Reset Store Failure Count** e fare clic su **Apply Changes**.
ASXP	Controlla le condivisioni	AMS	Viene attivato un allarme se il valore di Audit shares è Unknown (Sconosciuto). Questo allarme può indicare un problema con l'installazione o la configurazione del nodo di amministrazione. Se il problema persiste, contattare il supporto tecnico.
AUMA	Stato AMS	AMS	Se il valore di AMS Status (Stato AMS) è DB Connectivity Error (errore di connettività DB), riavviare il nodo Grid. Se il problema persiste, contattare il supporto tecnico.
AUME	Stato AMS	AMS	Se il valore di AMS state (Stato AMS) è Standby, continuare il monitoraggio del sistema StorageGRID. Se il problema persiste, contattare il supporto tecnico. Se il valore di AMS state è Offline, riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
AUXS	Audit Export Status (Stato esportazione audit)	AMS	Se viene attivato un allarme, correggere il problema sottostante, quindi riavviare il servizio AMS. Se il problema persiste, contattare il supporto tecnico.
BADD	Storage Controller Failed Drive Count (Conteggio dischi guasto	SSM	Questo allarme viene attivato quando uno o più dischi di un'appliance StorageGRID si sono guastati o non sono ottimali. Sostituire le unità secondo necessità.

Codice	Nome	Servizio	Azione consigliata
BASE	Identificatori di oggetti disponibili	CMN	Quando viene eseguito il provisioning di un sistema StorageGRID, al servizio CMN viene assegnato un numero fisso di identificatori di oggetti. Questo allarme viene attivato quando il sistema StorageGRID inizia a esaurire la fornitura di identificatori di oggetti. Per assegnare altri identificatori, contattare il supporto tecnico.
BASSI	Stato allocazione blocco identificatore	CMN	Per impostazione predefinita, viene attivato un allarme quando non è possibile allocare gli identificatori degli oggetti perché non è possibile raggiungere il quorum ADC. L'allocazione del blocco di identificatori sul servizio CMN richiede che un quorum (50% + 1) dei servizi ADC sia online e connesso. Se il quorum non è disponibile, il servizio CMN non è in grado di allocare nuovi blocchi identificatori fino a quando non viene ristabilita il quorum ADC. In caso di perdita del quorum ADC, in genere non vi è alcun impatto immediato sul sistema StorageGRID (i client possono ancora acquisire e recuperare il contenuto), in quanto circa un mese di fornitura di identificatori viene memorizzato nella cache altrove nella griglia; Tuttavia, se la condizione persiste, il sistema StorageGRID perderà la capacità di acquisire nuovi contenuti. Se viene attivato un allarme, esaminare il motivo della perdita del quorum ADC (ad esempio, potrebbe trattarsi di un guasto di rete o del nodo di storage) e intraprendere un'azione correttiva. Se il problema persiste, contattare il supporto tecnico.
BRDT	Temperatura dello chassis del controller di calcolo	SSM	Viene attivato un allarme se la temperatura del controller di calcolo in un'appliance StorageGRID supera una soglia nominale. Controllare i componenti hardware e i problemi ambientali per verificare la presenza di condizioni di surriscaldamento. Se necessario, sostituire il componente.

Codice	Nome	Servizio	Azione consigliata
BTOF	Offset	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Viene attivato un allarme se il tempo di servizio (secondi) differisce significativamente dall'ora del sistema operativo. In condizioni normali, il servizio dovrebbe risincronizzarsi. Se il tempo di servizio è troppo lontano dall'ora del sistema operativo, le operazioni del sistema potrebbero risentirne. Verificare che l'origine dell'ora del sistema StorageGRID sia corretta. Se il problema persiste, contattare il supporto tecnico.
BTSE	Stato del clock	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Viene attivato un allarme se l'ora del servizio non è sincronizzata con l'ora tracciata dal sistema operativo. In condizioni normali, il servizio dovrebbe risincronizzarsi. Se il tempo si disasse troppo dall'ora del sistema operativo, le operazioni del sistema potrebbero risentirne. Verificare che l'origine dell'ora del sistema StorageGRID sia corretta. Se il problema persiste, contattare il supporto tecnico.
CAHP	Percentuale di utilizzo di Java Heap	DDS	Viene attivato un allarme se Java non è in grado di eseguire la garbage collection a una velocità tale da consentire al sistema di funzionare correttamente. Un allarme potrebbe indicare un carico di lavoro dell'utente che supera le risorse disponibili nel sistema per l'archivio di metadati DDS. Controllare l'attività ILM nella dashboard oppure selezionare **SUPPORT** > **Tools** > **Grid topology**, quindi selezionare ***site*** > ***grid node*** > **DDS** > **Resources** > **Overview** > **Main**. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
CASA	Data Store Status (Stato archivio dati)	DDS	Viene generato un allarme se l'archivio di metadati Cassandra non è più disponibile. Controllare lo stato di Cassandra: 1. Nel nodo di storage, accedere come admin e. `su` Per eseguire l'root utilizzando la password elencata nel file Passwords.txt. 2. Inserire: `service cassandra status` 3. Se Cassandra non è in esecuzione, riavviarlo: `service cassandra restart` Questo allarme potrebbe anche indicare che l'archivio di metadati (database Cassandra) per un nodo di storage deve essere ricostruito. Consultare le informazioni relative alla risoluzione dei problemi relativi all'allarme Services: Status - Cassandra (SVST) in "Risolvere i problemi relativi ai metadati". Se il problema persiste, contattare il supporto tecnico.
CASO	Data Store state (Stato archivio dati)	DDS	Questo allarme viene attivato durante l'installazione o l'espansione per indicare che un nuovo archivio di dati si sta unendo alla griglia.
CCNA	Hardware di calcolo	SSM	Questo allarme viene attivato se lo stato dell'hardware del controller di calcolo in un'appliance StorageGRID richiede attenzione.

Codice	Nome	Servizio	Azione consigliata
CDLP	Spazio utilizzato metadati (percentuale)	DDS	Questo allarme viene attivato quando lo spazio effettivo dei metadati (CEMS) raggiunge il 70% di pieno (allarme minore), il 90% di pieno (allarme maggiore) e il 100% di pieno (allarme critico). Se questo allarme raggiunge la soglia del 90%, viene visualizzato un avviso sul dashboard in Grid Manager. È necessario eseguire una procedura di espansione per aggiungere nuovi nodi di storage il prima possibile. Vedere "Espandere una griglia". Se questo allarme raggiunge la soglia del 100%, è necessario interrompere l'acquisizione di oggetti e aggiungere nodi di storage immediatamente. Cassandra richiede una certa quantità di spazio per eseguire operazioni essenziali come la compattazione e la riparazione. Queste operazioni saranno influenzate se i metadati dell'oggetto utilizzano più del 100% dello spazio consentito. Possono verificarsi risultati indesiderati. **Nota**: Se non si riesce ad aggiungere nodi di storage, contattare il supporto tecnico. Una volta aggiunti nuovi nodi di storage, il sistema ribilancia automaticamente i metadati degli oggetti in tutti i nodi di storage e l'allarme viene cancellato. Inoltre, consultare le informazioni sulla risoluzione dei problemi relativi all'avviso di storage con metadati bassi in "Risolvere i problemi relativi ai metadati". Se il problema persiste, contattare il supporto tecnico.
CMNA	Stato CMN	CMN	Se il valore di CMN Status (Stato CMN) è Error (errore), selezionare **SUPPORT** > **Tools** > **Grid topology**, quindi selezionare ***Site*** > ***Grid node*** > **CMN** > **Overview** > **Main** e **CMN** > **Alarms** > **Main** per determinare la causa dell'errore e risolvere il problema. Viene attivato un allarme e il valore di CMN Status (Stato CMN) è No Online CMN (Nessuna CMN online) durante un aggiornamento hardware del nodo di amministrazione primario quando vengono commutate le CMN (il valore del vecchio stato CMN è Standby e il nuovo è Online). Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
CPRC	Capacità rimanente	NMS	Viene attivato un allarme se la capacità rimanente (numero di connessioni disponibili che è possibile aprire nel database NMS) scende al di sotto della gravità dell'allarme configurata. Se viene attivato un allarme, contattare il supporto tecnico.
CPSA	Alimentatore a del controller di calcolo	SSM	Viene attivato un allarme in caso di problemi con l'alimentazione A nel controller di calcolo di un'appliance StorageGRID. Se necessario, sostituire il componente.
CPSB	Alimentatore del controller di calcolo B	SSM	Viene attivato un allarme in caso di problemi con l'alimentazione B nel controller di calcolo di un'appliance StorageGRID. Se necessario, sostituire il componente.
CPUT	Temperatura CPU del controller di calcolo	SSM	Viene attivato un allarme se la temperatura della CPU nel controller di calcolo di un'appliance StorageGRID supera una soglia nominale. Se il nodo di storage è un'appliance StorageGRID, il sistema StorageGRID indica che il controller richiede attenzione. Controllare i componenti hardware e i problemi ambientali per verificare la presenza di condizioni di surriscaldamento. Se necessario, sostituire il componente.
DNST	DNS Status (Stato DNS)	SSM	Al termine dell'installazione, viene attivato un allarme DNST nel servizio SSM. Una volta configurato il DNS e le nuove informazioni sul server raggiungono tutti i nodi della griglia, l'allarme viene annullato.

Codice	Nome	Servizio	Azione consigliata
ECCD	Rilevati frammenti corrotti	LDR	Un allarme viene attivato quando il processo di verifica in background rileva un frammento danneggiato sottoposto a erasure coding. Se viene rilevato un frammento corrotto, si tenta di ricostruire il frammento. Ripristinare i frammenti danneggiati rilevati e copiare gli attributi Lost su zero e monitorarli per verificare se i conteggi si rialzano. Se il numero aumenta, potrebbe esserci un problema con lo storage sottostante del nodo di storage. Una copia dei dati oggetto sottoposti a erasure coding non viene considerata mancante fino a quando il numero di frammenti persi o corrotti non viola la tolleranza di errore del codice di cancellazione; pertanto, è possibile avere un frammento corrotto e poter recuperare l'oggetto. Se il problema persiste, contattare il supporto tecnico.
ECST	Stato di verifica	LDR	Questo allarme indica lo stato corrente del processo di verifica in background per i dati oggetto con erasure coding su questo nodo di storage. In caso di errore nel processo di verifica in background, viene attivato un allarme grave.
FOPN	Aprire file Descriptor	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Il FOPN può diventare grande durante le attività di picco. Se non diminuisce durante i periodi di attività lenta, contattare il supporto tecnico.
HSTE	HTTP state (Stato HTTP)	BLDR	Consultare le azioni consigliate per HSTU.

Codice	Nome	Servizio	Azione consigliata
HSTU	HTTP Status (Stato HTTP)	BLDR	HSTE e HSTU sono correlati a HTTP per tutto il traffico LDR, inclusi S3, Swift e altro traffico StorageGRID interno. Un allarme indica che si è verificata una delle seguenti situazioni: • HTTP è stato portato offline manualmente. • L'attributo HTTP Auto-Start è stato disattivato. • Chiusura del servizio LDR in corso. L'attributo HTTP Auto-Start è attivato per impostazione predefinita. Se questa impostazione viene modificata, HTTP potrebbe rimanere offline dopo un riavvio. Se necessario, attendere il riavvio del servizio LDR. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Storage Node*** > **LDR** > **Configuration**. Se HTTP non è in linea, metterlo in linea. Verificare che l'attributo Avvio automatico HTTP sia attivato. Se HTTP rimane offline, contattare il supporto tecnico.
HTA	Avvio automatico HTTP	LDR	Specifica se avviare automaticamente i servizi HTTP all'avvio. Questa è un'opzione di configurazione specificata dall'utente.
IRSU	Stato della replica in entrata	BLDR, BARC	Un allarme indica che la replica in entrata è stata disattivata. Confermare le impostazioni di configurazione: Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **Main**.
LATA	Latenza media	NMS	Verificare la presenza di problemi di connettività. Controllare l'attività del sistema per verificare che l'attività del sistema aumenti. Un aumento dell'attività di sistema determinerà un aumento dell'attributo dell'attività dei dati. L'aumento dell'attività comporterà un ritardo nell'elaborazione dei dati degli attributi. Si tratta di un'attività normale del sistema che verrà a trovarsi in una posizione secondaria. Verificare la presenza di più allarmi. Un aumento dei tempi di latenza medi può essere indicato da un numero eccessivo di allarmi attivati. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
DRE	Stato LDR	LDR	Se il valore dello stato LDR è Standby, continuare a monitorare la situazione e, se il problema persiste, contattare il supporto tecnico. Se il valore di stato LDR è Offline, riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
PERSO	Oggetti persi	DDS, LDR	Viene attivato quando il sistema StorageGRID non riesce a recuperare una copia dell'oggetto richiesto da qualsiasi punto del sistema. Prima che venga attivato un allarme LOST (Lost Objects), il sistema tenta di recuperare e sostituire un oggetto mancante da un'altra parte del sistema. Gli oggetti persi rappresentano una perdita di dati. L'attributo Lost Objects viene incrementato ogni volta che il numero di posizioni di un oggetto scende a zero senza che il servizio DDS purifichi intenzionalmente il contenuto per soddisfare la policy ILM. Esaminare immediatamente gli allarmi PERSI (oggetti SMARRITI). Se il problema persiste, contattare il supporto tecnico. "Risolvere i problemi relativi ai dati degli oggetti persi e mancanti"
MCEP	Scadenza del certificato dell'interfaccia di gestione	CMN	Viene attivato quando il certificato utilizzato per accedere all'interfaccia di gestione sta per scadere. 1. Da Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**. 2. Nella scheda **Global**, selezionare **Management interface certificate**. 3. "Caricare un nuovo certificato dell'interfaccia di gestione."
MINQ	Notifiche e-mail in coda	NMS	Controllare le connessioni di rete dei server che ospitano il servizio NMS e il server di posta esterno. Verificare inoltre che la configurazione del server di posta elettronica sia corretta. "Configurare le impostazioni del server di posta elettronica per gli allarmi (sistema legacy)"

Codice	Nome	Servizio	Azione consigliata
MIN	Email Notifications Status (Stato notifiche e-mail)	BNMS	Se il servizio NMS non riesce a connettersi al server di posta, viene attivato un allarme minore. Controllare le connessioni di rete dei server che ospitano il servizio NMS e il server di posta esterno. Verificare inoltre che la configurazione del server di posta elettronica sia corretta. "Configurare le impostazioni del server di posta elettronica per gli allarmi (sistema legacy)"
SIG.NA	Stato del motore di interfaccia NMS	BNMS	Viene attivato un allarme se il motore di interfaccia NMS sul nodo di amministrazione che raccoglie e genera il contenuto dell'interfaccia viene disconnesso dal sistema. Controllare Server Manager per determinare se la singola applicazione del server non è disponibile.
NANG	Network Auto Negotiate (negoziazione automatica di rete	SSM	Controllare la configurazione della scheda di rete. L'impostazione deve corrispondere alle preferenze dei router e degli switch di rete. Un'impostazione errata può avere un impatto grave sulle prestazioni del sistema.
NUP	Impostazione fronte/retro di rete	SSM	Controllare la configurazione della scheda di rete. L'impostazione deve corrispondere alle preferenze dei router e degli switch di rete. Un'impostazione errata può avere un impatto grave sulle prestazioni del sistema.
NLNK	Network link Detect (rilevamento collegamento di rete	SSM	Controllare i collegamenti dei cavi di rete sulla porta e sullo switch. Controllare le configurazioni di router, switch e adattatori di rete. Riavviare il server. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
NRER	Errori di ricezione	SSM	Di seguito sono riportate le cause degli allarmi NRER: • Mancata corrispondenza FEC (Forward Error Correction) • Mancata corrispondenza tra porta dello switch e MTU della scheda NIC • Elevati tassi di errore di collegamento • Buffer di anello NIC scaduto Consultare le informazioni relative alla risoluzione dei problemi relativi all'allarme NRER (Network Receive Error) in "Risolvere i problemi di rete, hardware e piattaforma".
NRLY	Relè di audit disponibili	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Se i relè di audit non sono connessi ai servizi ADC, non è possibile segnalare gli eventi di audit. Vengono messi in coda e non disponibili per gli utenti fino al ripristino della connessione. Ripristinare la connettività a un servizio ADC il prima possibile. Se il problema persiste, contattare il supporto tecnico.
NSCA	Stato NMS	NMS	Se il valore di NMS Status (Stato NMS) è DB Connectivity Error (errore di connettività DB), riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
NSCE	Stato NMS	NMS	Se il valore di NMS state (Stato NMS) è Standby, continuare il monitoraggio e, se il problema persiste, contattare il supporto tecnico. Se il valore di NMS state (Stato NMS) è Offline, riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
NSPD	Velocità	SSM	Ciò può essere causato da problemi di connettività di rete o di compatibilità dei driver. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
NTBR	Spazio tabella libero	NMS	Se viene attivato un allarme, verificare la velocità di modifica dell'utilizzo del database. Un calo improvviso (invece di un cambiamento graduale nel tempo) indica una condizione di errore. Se il problema persiste, contattare il supporto tecnico. La regolazione della soglia di allarme consente di gestire in modo proattivo quando è necessario allocare ulteriore storage. Se lo spazio disponibile raggiunge una soglia bassa (vedere soglia di allarme), contattare il supporto tecnico per modificare l'allocazione del database.
NTER.A.	Errori di trasmissione	SSM	Questi errori possono essere azzerati senza essere reimpostati manualmente. In caso contrario, controllare l'hardware di rete. Verificare che l'hardware e il driver della scheda siano installati e configurati correttamente per funzionare con i router e gli switch di rete. Una volta risolto il problema sottostante, azzerare il contatore. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **Main**, selezionare **Reset Transmit Error Count** e fare clic su **Apply Changes**.
NTFQ	Offset frequenza NTP	SSM	Se l'offset di frequenza supera la soglia configurata, è probabile che si sia verificato un problema hardware con l'orologio locale. Se il problema persiste, contattare il supporto tecnico per richiedere la sostituzione.
NTLK	Blocco NTP	SSM	Se il daemon NTP non è bloccato su una fonte di tempo esterna, controllare la connettività di rete alle fonti di tempo esterne designate, la loro disponibilità e la loro stabilità.
NTOF	Offset ora NTP	SSM	Se l'offset temporale supera la soglia configurata, è probabile che si sia verificato un problema hardware con l'oscillatore del clock locale. Se il problema persiste, contattare il supporto tecnico per richiedere la sostituzione.

Codice	Nome	Servizio	Azione consigliata
NTSJ	Jitter di origine temporale selezionato	SSM	Questo valore indica l'affidabilità e la stabilità dell'origine temporale utilizzata da NTP sul server locale come riferimento. Se viene attivato un allarme, può essere un'indicazione che l'oscillatore dell'origine del tempo è difettoso o che si è verificato un problema con il collegamento WAN all'origine del tempo.
NTSU	NTP Status (Stato NTP)	SSM	Se il valore NTP Status (Stato NTP) non è in esecuzione, contattare il supporto tecnico.
OPST	Stato generale dell'alimentazione	SSM	Viene attivato un allarme se l'alimentazione di un apparecchio StorageGRID non rientra nella tensione di esercizio consigliata. Controllare lo stato dell'alimentatore A o B per determinare quale alimentatore funziona in modo anomalo. Se necessario, sostituire l'alimentatore.
OQRT	Oggetti in quarantena	LDR	Dopo il ripristino automatico degli oggetti da parte del sistema StorageGRID, è possibile rimuovere gli oggetti in quarantena dalla directory di quarantena. 1. Selezionare **SUPPORT** > **Tools** > **Grid topology**. 2. Selezionare **sito** > **nodo di storage** > **LDR** > **verifica** > **Configurazione** > **principale**. 3. Selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena). 4. Fare clic su **Applica modifiche**. Gli oggetti in quarantena vengono rimossi e il conteggio viene azzerato.
ORSU	Stato della replica in uscita	BLDR, BARC	Un allarme indica che la replica in uscita non è possibile: Lo storage si trova in uno stato in cui gli oggetti non possono essere recuperati. Viene attivato un allarme se la replica in uscita viene disattivata manualmente. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration**. Viene attivato un allarme se il servizio LDR non è disponibile per la replica. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Storage**.

Codice	Nome	Servizio	Azione consigliata
OSLF	Stato dello shelf	SSM	Viene attivato un allarme se lo stato di uno dei componenti dello shelf di storage di un'appliance di storage è degradato. I componenti dello shelf di storage includono gli IOM, le ventole, gli alimentatori e i cassetti delle unità. Se viene attivato questo allarme, consultare le istruzioni di manutenzione dell'apparecchio.
PMEM	Utilizzo della memoria di servizio (percentuale)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Può avere un valore superiore a Y% di RAM, dove Y rappresenta la percentuale di memoria utilizzata dal server. I valori inferiori al 80% sono normali. Oltre il 90% è considerato un problema. Se l'utilizzo della memoria è elevato per un singolo servizio, monitorare la situazione e analizzare. Se il problema persiste, contattare il supporto tecnico.
PSA	Power Supply A Status (Stato alimentatore A)	SSM	Viene attivato un allarme se l'alimentazione A di un apparecchio StorageGRID non rientra nella tensione di esercizio consigliata. Se necessario, sostituire l'alimentatore A.
PSB	Stato dell'alimentatore B.	SSM	Viene attivato un allarme se l'alimentazione B di un apparecchio StorageGRID si discosta dalla tensione di esercizio consigliata. Se necessario, sostituire l'alimentatore B.
RDTE	Stato di Tivoli Storage Manager	BARC	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Tivoli Storage Manager (TSM). Se il valore di Tivoli Storage Manager state (Stato di Tivoli Storage Manager) è offline, controllare lo stato di Tivoli Storage Manager e risolvere eventuali problemi. Riportare il componente online. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **ARC** > **Target** > **Configuration** > **Main**, selezionare **Tivoli Storage Manager state** > **Online** e fare clic su **Apply Changes**.

Codice	Nome	Servizio	Azione consigliata
RDTU	Stato di Tivoli Storage Manager	BARC	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Tivoli Storage Manager (TSM). Se il valore dello stato di Tivoli Storage Manager è errore di configurazione e il nodo di archiviazione è stato appena aggiunto al sistema StorageGRID, assicurarsi che il server middleware TSM sia configurato correttamente. Se il valore di Stato di Tivoli Storage Manager è errore di connessione o errore di connessione, Riprova, controllare la configurazione di rete sul server middleware TSM e la connessione di rete tra il server middleware TSM e il sistema StorageGRID. Se il valore di Stato di Tivoli Storage Manager è errore di autenticazione o errore di autenticazione, riconnessione, il sistema StorageGRID può connettersi al server middleware TSM, ma non può autenticare la connessione. Verificare che il server middleware TSM sia configurato con l'utente, la password e le autorizzazioni corretti, quindi riavviare il servizio. Se il valore di Tivoli Storage Manager Status (Stato di Tivoli Storage Manager) è Session Failure (errore di sessione), una sessione stabilita è stata persa inaspettatamente. Verificare la connessione di rete tra il server middleware TSM e il sistema StorageGRID. Verificare la presenza di errori nel server middleware. Se il valore di Tivoli Storage Manager Status (Stato di Tivoli Storage Manager) è Unknown Error (errore sconosciuto), contattare il supporto tecnico.
RRF	Repliche in entrata — non riuscite	BLDR, BARC	Un allarme Inbound Replications — Failed (repliche in entrata) può verificarsi in periodi di carico elevato o interruzioni temporanee della rete. Una volta ridotta l'attività del sistema, questo allarme dovrebbe essere disattivato. Se il numero di repliche non riuscite continua ad aumentare, cercare i problemi di rete e verificare che i servizi LDR e ARC di origine e destinazione siano online e disponibili. Per azzerare il conteggio, selezionare **SUPPORT** > **Tools** > **Grid topology**, quindi selezionare ***Site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **Main**. Selezionare **Reset Inbound Replication Failure Count**, quindi fare clic su **Apply Changes** (Applica modifiche).

Codice	Nome	Servizio	Azione consigliata
RIRQ	Repliche inbound — in coda	BLDR, BARC	Gli allarmi possono verificarsi in periodi di carico elevato o interruzione temporanea della rete. Una volta ridotta l'attività del sistema, questo allarme dovrebbe essere disattivato. Se il numero di repliche in coda continua ad aumentare, cercare i problemi di rete e verificare che i servizi LDR e ARC di origine e destinazione siano online e disponibili.
RORQ	Repliche in uscita — in coda	BLDR, BARC	La coda di replica in uscita contiene i dati oggetto copiati per soddisfare le regole ILM e gli oggetti richiesti dai client. Un allarme può verificarsi in seguito a un sovraccarico del sistema. Attendere per verificare se l'allarme viene cancellato quando l'attività del sistema diminuisce. Se l'allarme si ripete, aggiungere capacità aggiungendo nodi di storage.
SAVP	Spazio totale utilizzabile (percentuale)	LDR	Se lo spazio utilizzabile raggiunge una soglia bassa, le opzioni includono l'espansione del sistema StorageGRID o lo spostamento dei dati dell'oggetto nell'archivio attraverso un nodo di archiviazione.
SCA	Stato	CMN	Se il valore di Status (Stato) per l'attività della griglia attiva è Error (errore), cercare il messaggio Grid task (attività griglia). Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Grid node*** > **CMN** > **Grid Tasks** > **Overview** > **Main**. Il messaggio dell'attività griglia visualizza informazioni sull'errore (ad esempio, "controllo non riuscito sul nodo 12130011"). Dopo aver esaminato e corretto il problema, riavviare l'attività Grid. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Configuration** > **Main** e selezionare **Actions** > **Run**. Se il valore Stato per un'attività di griglia interrotta è Error, riprovare a terminare l'attività di griglia. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
SCEP	Scadenza del certificato per gli endpoint del servizio API di storage	CMN	Viene attivato quando il certificato utilizzato per l'accesso agli endpoint API dello storage sta per scadere. 1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**. 2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**. 3. "Caricare un nuovo certificato API S3 e Swift."
SCHR	Stato	CMN	Se il valore di Status (Stato) per l'attività della griglia storica viene interrotto, esaminare il motivo ed eseguire nuovamente l'attività, se necessario. Se il problema persiste, contattare il supporto tecnico.
SCSA	Controller dello storage A	SSM	Viene attivato un allarme in caso di problemi con lo storage controller A in un'appliance StorageGRID. Se necessario, sostituire il componente.
SCSB	Controller dello storage B	SSM	Viene attivato un allarme in caso di problemi con lo storage controller B in un'appliance StorageGRID. Se necessario, sostituire il componente. Alcuni modelli di appliance non dispongono di un controller di storage B.
SHLH	Salute	LDR	Se il valore di Health per un archivio di oggetti è Error (errore), controllare e correggere: • problemi con il volume montato • errori del file system
SLSA	Media carico CPU	SSM	Maggiore è il valore, maggiore è il numero di componenti del sistema. Se la media del carico della CPU persiste a un valore elevato, è necessario esaminare il numero di transazioni nel sistema per determinare se ciò sia dovuto a un carico pesante in quel momento. Visualizza un grafico della media di carico della CPU: Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **SSM** > **Resources** > **Reports** > **Charts**. Se il carico sul sistema non è elevato e il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
SMST	Log Monitor state (Stato monitoraggio registro) non è connesso per un periodo di tempo persistente, contattare il supporto tecnico.	SSM	Se il valore Log Monitor state (Stato monitoraggio registro) non è connesso per un periodo di tempo persistente, contattare il supporto tecnico.
SMTT	Eventi totali	SSM	Se il valore di Total Events (Eventi totali) è maggiore di zero, controllare se la causa può essere la presenza di eventi noti (come gli errori di rete). A meno che questi errori non siano stati cancellati (ovvero, il conteggio è stato reimpostato su 0), possono essere attivati gli allarmi Total Events (Eventi totali). Una volta risolto il problema, azzerare il contatore per eliminare l'allarme. Selezionare **NODI** > ***sito*** > ***nodo griglia*** > **Eventi** > **Ripristina conteggi eventi**. Per reimpostare i conteggi degli eventi, è necessario disporre dell'autorizzazione di configurazione della pagina topologia griglia. Se il valore di Total Events (Eventi totali) è zero o il numero aumenta e il problema persiste, contattare il supporto tecnico.
SNST	Stato	CMN	Un allarme indica che si è verificato un problema nella memorizzazione dei bundle di attività della griglia. Se il valore Stato è errore del punto di controllo o quorum non raggiunto, verificare che la maggior parte dei servizi ADC sia connessa al sistema StorageGRID (50% più uno), quindi attendere alcuni minuti. Se il problema persiste, contattare il supporto tecnico.
SOSS	Stato del sistema operativo per lo storage	SSM	Un allarme viene attivato se SANtricity OS indica che un componente di un'apparecchiatura StorageGRID presenta un problema di "intervento richiesto". Selezionare **NODI**. Quindi selezionare **Appliance Storage Node** > **hardware**. Scorrere verso il basso per visualizzare lo stato di ciascun componente. In SANtricity OS, controllare gli altri componenti dell'appliance per isolare il problema.

Codice	Nome	Servizio	Azione consigliata
SSMA	Stato SSM	SSM	Se il valore di SSM Status (Stato SSM) è Error (errore), selezionare **SUPPORT** > **Tools** > **Grid topology**, quindi selezionare ***Site*** > ***Grid node*** > **SSM** > **Overview** > **Main** e **SSM** > **Overview** > **Alarms** per determinare la causa dell'allarme. Se il problema persiste, contattare il supporto tecnico.
SSME	Stato SSM	SSM	Se il valore di SSM state (Stato SSM) è Standby, continuare il monitoraggio e, se il problema persiste, contattare il supporto tecnico. Se il valore di SSM state (Stato SSM) è Offline (non in linea), riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
SST	Stato dello storage	BLDR	Se il valore di Storage Status (Stato storage) è Insufficient usable Space (spazio utilizzabile insufficiente), lo storage disponibile sul nodo di storage non è più disponibile e i dati acquisiti vengono reindirizzati ad altri nodi di storage disponibili. Le richieste di recupero possono continuare ad essere inviate da questo nodo della griglia. È necessario aggiungere ulteriore storage. Non influisce sulla funzionalità dell'utente finale, ma l'allarme persiste fino a quando non viene aggiunto ulteriore storage. Se il valore di Storage Status (Stato storage) è Volume(i) Unavailable (volumi non disponibili), una parte dello storage non è disponibile. Lo storage e il recupero da questi volumi non sono possibili. Per ulteriori informazioni, controllare lo stato di salute del volume: Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**. Lo stato di salute del volume è elencato in archivi di oggetti. Se il valore dello stato dello storage è Error (errore), contattare il supporto tecnico. "Risolvere i problemi relativi all'allarme Storage Status (SST)"

Codice	Nome	Servizio	Azione consigliata
SVST	Stato	SSM	Questo allarme viene cancellato quando vengono risolti altri allarmi relativi a un servizio non in esecuzione. Tenere traccia degli allarmi di manutenzione della sorgente per ripristinare il funzionamento. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **SSM** > **servizi** > **Panoramica** > **principale**. Quando lo stato di un servizio viene visualizzato come non in esecuzione, il suo stato è amministrativamente inattivo. Lo stato del servizio può essere indicato come non in esecuzione per i seguenti motivi: • Il servizio è stato arrestato manualmente (`/etc/init.d/<service\> stop`). • Si è verificato un problema con il database MySQL e Server Manager arresta IL servizio MI. • È stato aggiunto un nodo Grid, ma non è stato avviato. • Durante l'installazione, un nodo Grid non è ancora connesso al nodo Admin. Se un servizio viene visualizzato come non in esecuzione, riavviarlo (`/etc/init.d/<service\> restart`). Questo allarme potrebbe anche indicare che l'archivio di metadati (database Cassandra) per un nodo di storage deve essere ricostruito. Se il problema persiste, contattare il supporto tecnico. "Risolvere i problemi relativi all'allarme Services: Status - Cassandra (SVST)"
TMEM	Memoria installata	SSM	I nodi in esecuzione con meno di 24 GB di memoria installata possono causare problemi di performance e instabilità del sistema. La quantità di memoria installata nel sistema deve essere aumentata ad almeno 24 GiB.
TPOP	Operazioni in sospeso	ADC	Una coda di messaggi può indicare che il servizio ADC è sovraccarico. È possibile collegare al sistema StorageGRID un numero troppo basso di servizi ADC. In un'implementazione di grandi dimensioni, il servizio ADC può richiedere l'aggiunta di risorse di calcolo oppure il sistema può richiedere servizi ADC aggiuntivi.

Codice	Nome	Servizio	Azione consigliata
UMEM	Memoria disponibile	SSM	Se la RAM disponibile si sta esaurendo, determinare se si tratta di un problema hardware o software. Se non si tratta di un problema hardware o se la memoria disponibile scende al di sotto di 50 MB (soglia di allarme predefinita), contattare il supporto tecnico.
VMFI	Voci disponibili	SSM	Ciò indica che è necessario uno storage aggiuntivo. Contattare il supporto tecnico.
VMFR	Spazio disponibile	SSM	Se il valore di spazio disponibile diventa troppo basso (vedi soglie di allarme), occorre verificare se ci sono file di log che crescono fuori proporzione o oggetti che occupano troppo spazio su disco (vedi soglie di allarme) che devono essere ridotti o cancellati. Se il problema persiste, contattare il supporto tecnico.
VMST	Stato	SSM	Viene attivato un allarme se il valore di Status (Stato) per il volume montato è Unknown (Sconosciuto). Il valore Unknown (Sconosciuto) o Offline (non in linea) indica che non è possibile montare o accedere al volume a causa di un problema con il dispositivo di storage sottostante.
VPRI	Priorità di verifica	BLDR, BARC	Per impostazione predefinita, il valore della priorità di verifica è Adaptive. Se la priorità di verifica è impostata su alta, viene attivato un allarme perché la verifica dello storage può rallentare le normali operazioni del servizio.
VSTU	Stato di verifica dell'oggetto	BLDR	Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**. Controllare il sistema operativo per verificare la presenza di eventuali errori relativi a dispositivi a blocchi o file system. Se il valore di Stato verifica oggetto è Unknown Error (errore sconosciuto), di solito indica un problema di file system o hardware di basso livello (errore i/o) che impedisce all'attività di verifica dello storage di accedere al contenuto memorizzato. Contattare il supporto tecnico.
XAMS	Repository di audit non raggiungibili	BADC, BARC, BCLB, BCMN, BLDR, BNMS	Verificare la connettività di rete al server che ospita il nodo di amministrazione. Se il problema persiste, contattare il supporto tecnico.

Riferimenti ai file di log

Riferimento ai file di log: Panoramica

StorageGRID fornisce registri utilizzati per acquisire eventi, messaggi di diagnostica e condizioni di errore. Potrebbe essere richiesto di raccogliere i file di log e inoltrarli al supporto tecnico per agevolare la risoluzione dei problemi.

I log sono classificati come segue:

- "Log del software StorageGRID"
- "Log di implementazione e manutenzione"
- "Registri per software di terze parti"
- "A proposito di bycast.log"

> I dettagli forniti per ciascun tipo di registro sono solo a scopo di riferimento. I registri sono destinati al troubleshooting avanzato da parte del supporto tecnico. Le tecniche avanzate che implicano la ricostruzione della cronologia dei problemi utilizzando i registri di controllo e i file di log dell'applicazione esulano dall'ambito di queste istruzioni.

Accedere ai registri

Per accedere ai registri, è possibile "raccogliere i file di log e i dati di sistema" da uno o più nodi come singolo archivio di file di log. In alternativa, se il nodo di amministrazione primario non è disponibile o non è in grado di raggiungere un nodo specifico, è possibile accedere ai singoli file di registro per ciascun nodo della griglia come segue:

1. Immettere il seguente comando: `ssh admin@grid_node_IP`
2. Immettere la password elencata in `Passwords.txt` file.
3. Immettere il seguente comando per passare a root: `su -`
4. Immettere la password elencata in `Passwords.txt` file.

Categorie di file di log

L'archivio del file di log di StorageGRID contiene i log descritti per ciascuna categoria e i file aggiuntivi che contengono metriche e output dei comandi di debug.

Percorso di archiviazione	Descrizione
audit	Messaggi di audit generati durante il normale funzionamento del sistema.
log-sistema-di-base	Informazioni di base sul sistema operativo, incluse le versioni delle immagini StorageGRID.
bundle	Informazioni sulla configurazione globale (bundle).
cassandra	Informazioni sul database Cassandra e registri di riparazione Reaper.

Percorso di archiviazione	Descrizione
ce	Informazioni sui VCSs relative al nodo corrente e informazioni sul gruppo EC in base all'ID del profilo.
griglia	Log di griglia generali, incluso il debug (`bycast.log`) e. `servermanager` registri.
grid.xml	File di configurazione della griglia condiviso tra tutti i nodi.
hagroup	Metriche e registri dei gruppi ad alta disponibilità.
installare	`Gdu-server` e installare i log.
lumberjack.log	Messaggi di debug relativi alla raccolta dei log.
Arbitro lambda	Registri relativi alla richiesta del proxy S3 Select.
Metriche	Log di servizio per Grafana, Jaeger, node esporter e Prometheus.
errore	Accesso Miscd e log degli errori.
mysql	La configurazione del database MariaDB e i relativi log.
netto	Log generati da script correlati alla rete e dal servizio Dynip.
nginx	File e log di configurazione del bilanciamento del carico e della federazione di griglie. Include anche i log di traffico di Grid Manager e Tenant Manager.
nginx-gw	File e log di configurazione del bilanciamento del carico e della federazione di griglie.
ntp	File di configurazione NTP e registri.
sistema operativo	File di stato del nodo e della griglia, inclusi i servizi `pid`.
altro	File di log in `/var/local/log` che non vengono raccolte in altre cartelle.
perf	Informazioni sulle prestazioni per CPU, rete e i/o del disco
prometheus-data	Metriche Prometheus correnti, se la raccolta di log include i dati Prometheus.
provisioning	Log relativi al processo di provisioning della griglia.

Percorso di archiviazione	Descrizione
zattera	Log dal cluster Raft utilizzato nei servizi della piattaforma.
ssh	Registri relativi alla configurazione e al servizio SSH.
snmp	Configurazione dell'agente SNMP e elenchi di allow/deny degli allarmi utilizzati per l'invio di notifiche SNMP.
socket-dati	Dati socket per il debug di rete.
system-commands.txt	Output dei comandi del container StorageGRID. Contiene informazioni di sistema, ad esempio le reti e l'utilizzo del disco.

Log del software StorageGRID

È possibile utilizzare i registri di StorageGRID per risolvere i problemi.

> Se si desidera inviare i registri a un server syslog esterno o modificare la destinazione delle informazioni di controllo, ad esempio `bycast.log` e. `nms.log`, vedere "Configurare i messaggi di audit e le destinazioni dei log".

Log StorageGRID generali

Nome del file	Note	Trovato in
/var/local/log/bycast.log	Il file primario per la risoluzione dei problemi di StorageGRID. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Node*** > **SSM** > **Events**.	Tutti i nodi
/var/local/log/bycast-err.log	Contiene un sottoinsieme di `bycast.log` (Messaggi con ERRORI di severità e CRITICI). I messaggi CRITICI vengono visualizzati anche nel sistema. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Node*** > **SSM** > **Events**.	Tutti i nodi

Nome del file	Note	Trovato in
/var/local/core/	Contiene tutti i file core dump creati se il programma termina in modo anomalo. Le possibili cause includono errori di asserzione, violazioni o timeout di thread. **Nota**: Il file `/var/local/core/kexec_cmd` di solito esiste sui nodi appliance e non indica un errore.	Tutti i nodi

Log relativi alla crittografia

Nome del file	Note	Trovato in
/var/local/log/ssh-config-generation.log	Contiene i log relativi alla generazione delle configurazioni SSH e al ricaricamento dei servizi SSH.	Tutti i nodi
/var/local/log/nginx/config-generation.log	Contiene i log relativi alla generazione di configurazioni nginx e al ricaricamento dei servizi nginx.	Tutti i nodi
/var/local/log/nginx-gw/config-generation.log	Contiene i log relativi alla generazione di configurazioni nginx-gw (e al ricaricamento dei servizi nginx-gw).	Nodi Admin e Gateway
/var/local/log/update-cipher-configurations.log	Contiene i registri relativi alla configurazione dei criteri TLS e SSH.	Tutti i nodi

Log della federazione di griglie

Nome del file	Note	Trovato in
/var/local/log/update_grid_federation_config.log	Contiene i log relativi alla generazione di configurazioni nginx e nginx-gw per le connessioni di federazione di griglie.	Tutti i nodi

Registri NMS

Nome del file	Note	Trovato in
/var/local/log/nms.log	• Acquisisce le notifiche da Grid Manager e Tenant Manager. • Acquisisce gli eventi correlati al funzionamento del servizio NMS, ad esempio l'elaborazione degli allarmi, le notifiche e-mail e le modifiche alla configurazione. • Contiene gli aggiornamenti del bundle XML risultanti dalle modifiche di configurazione apportate nel sistema. • Contiene messaggi di errore relativi al downsampling degli attributi eseguito una volta al giorno. • Contiene messaggi di errore del server Web Java, ad esempio errori di generazione pagina e errori HTTP Status 500.	Nodi di amministrazione
/var/local/log/nms.errlog	Contiene messaggi di errore relativi agli aggiornamenti del database MySQL. Contiene il flusso standard di errore (stderr) dei servizi corrispondenti. Esiste un file di log per servizio. Questi file sono generalmente vuoti, a meno che non si verifichino problemi con il servizio.	Nodi di amministrazione
/var/local/log/nms.requestlog	Contiene informazioni sulle connessioni in uscita dall'API di gestione ai servizi StorageGRID interni.	Nodi di amministrazione

Log di Server Manager

Nome del file	Note	Trovato in
/var/local/log/servermanager.log	File di log per l'applicazione Server Manager in esecuzione sul server.	Tutti i nodi
/Var/local/log/GridstatBackend.errlog	File di log per l'applicazione backend della GUI di Server Manager.	Tutti i nodi
/var/local/log/gridstat.errlog	File di log per la GUI di Server Manager.	Tutti i nodi

Log dei servizi StorageGRID

Nome del file	Note	Trovato in
/var/local/log/acct.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/adc.errlog	Contiene il flusso standard di errore (stderr) dei servizi corrispondenti. Esiste un file di log per servizio. Questi file sono generalmente vuoti, a meno che non si verifichino problemi con il servizio.	Nodi di storage che eseguono il servizio ADC
/var/local/log/ams.errlog		Nodi di amministrazione
/var/local/log/arc.errlog		Nodi di archiviazione
/var/local/log/cassandra/system.log	Informazioni per l'archivio di metadati (database Cassandra) che possono essere utilizzate se si verificano problemi durante l'aggiunta di nuovi nodi di storage o se l'attività di riparazione nodetool si blocca.	Nodi di storage
/var/local/log/cassandra-reaper.log	Informazioni per il servizio Cassandra Reaper, che esegue la riparazione dei dati nel database Cassandra.	Nodi di storage
/var/local/log/cassandra-reaper.errlog	Informazioni sugli errori per il servizio Cassandra Reaper.	Nodi di storage
/var/local/log/chunk.errlog		Nodi di storage
/var/local/log/cmn.errlog		Nodi di amministrazione
/var/local/log/cms.errlog	Questo file di log potrebbe essere presente sui sistemi che sono stati aggiornati da una versione precedente di StorageGRID. Contiene informazioni legacy.	Nodi di storage
/var/local/log/cts.errlog	Questo file di log viene creato solo se il tipo di destinazione è **Cloud Tiering - Simple Storage Service (S3).**	Nodi di archiviazione
/var/local/log/dds.errlog		Nodi di storage
/var/local/log/dmv.errlog		Nodi di storage

Nome del file	Note	Trovato in
/var/local/log/dynip*	Contiene i registri relativi al servizio di dinip, che monitora la griglia per rilevare le modifiche dell'IP dinamico e aggiorna la configurazione locale.	Tutti i nodi
/var/local/log/grafana.log	Log associato al servizio Grafana, utilizzato per la visualizzazione delle metriche in Grid Manager.	Nodi di amministrazione
/var/local/log/hagroups.log	Log associato ai gruppi ad alta disponibilità.	Nodi di amministrazione e nodi gateway
/var/local/log/hagroups_events.log	Tiene traccia delle modifiche di stato, come la transizione da BACKUP a MASTER o FAULT.	Nodi di amministrazione e nodi gateway
/var/local/log/idnt.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/jaeger.log	Log associato al servizio jaeger, utilizzato per la raccolta delle tracce.	Tutti i nodi
/var/local/log/kstn.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/lambda*	Contiene i registri per il servizio S3 Select.	Nodi Admin e Gateway Solo alcuni nodi Admin e Gateway contengono questo log. Vedere "S3 selezionare requisiti e limitazioni per i nodi Admin e Gateway".
/var/local/log/ldr.errlog		Nodi di storage
/var/local/log/miscd/*.log	Contiene i log per il servizio MISCd (Information Service Control Daemon), che 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.	Tutti i nodi

Nome del file	Note	Trovato in
/var/local/log/nginx/*.log	Contiene i log per il servizio nginx, che funge da meccanismo di autenticazione e comunicazione sicura per diversi servizi grid (come Prometheus e Dynip) per poter comunicare con servizi su altri nodi tramite API HTTPS.	Tutti i nodi
/var/local/log/nginx-gw/*.log	Contiene i log generali relativi al servizio nginx-gw, inclusi i log degli errori e i log per le porte amministrative limitate sui nodi di amministrazione.	Nodi di amministrazione e nodi gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contiene log di accesso relativi al traffico di replica cross-grid.	Nodi di amministrazione, nodi gateway o entrambi, in base alla configurazione della federazione di griglie. Trovato solo nella griglia di destinazione per la replica cross-grid.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contiene i log di accesso per il servizio Load Balancer, che fornisce il bilanciamento del carico del traffico S3 e Swift dai client ai nodi di storage.	Nodi di amministrazione e nodi gateway
/var/local/log/persistence*	Contiene i log per il servizio di persistenza, che gestisce i file sul disco root che devono persistere durante un riavvio.	Tutti i nodi
/var/local/log/prometheus.log	Per tutti i nodi, contiene il log del servizio dell'esportatore di nodi e il log del servizio di metriche dell'esportatore. Per i nodi di amministrazione, contiene anche i registri per i servizi Prometheus e Alert Manager.	Tutti i nodi
/var/local/log/raft.log	Contiene l'output della libreria utilizzata dal servizio RSM per il protocollo Raft.	Nodi storage con servizio RSM
/var/local/log/rms.errlog	Contiene i registri per il servizio RSM (Replicated state Machine Service), utilizzato per i servizi della piattaforma S3.	Nodi storage con servizio RSM
/var/local/log/ssm.errlog		Tutti i nodi

Nome del file	Note	Trovato in
/var/local/log/update-s3vs-domains.log	Contiene i registri relativi all'elaborazione degli aggiornamenti per la configurazione dei nomi di dominio host virtuali S3.vedere le istruzioni per l'implementazione delle applicazioni client S3.	Nodi Admin e Gateway
/var/local/log/update-snmp-firewall.*	Contiene i registri relativi alle porte firewall gestite per SNMP.	Tutti i nodi
/var/local/log/update-sysl.log	Contiene i registri relativi alle modifiche apportate alla configurazione syslog del sistema.	Tutti i nodi
/var/local/log/update-traffic-classes.log	Contiene i registri relativi alle modifiche apportate alla configurazione dei classificatori del traffico.	Nodi Admin e Gateway
/var/local/log/update-utcn.log	Contiene i registri relativi alla modalità di rete client non attendibile su questo nodo.	Tutti i nodi

Informazioni correlate

"A proposito di bycast.log"

"UTILIZZARE L'API REST S3"

Log di implementazione e manutenzione

È possibile utilizzare i registri di implementazione e manutenzione per risolvere i problemi.

Nome del file	Note	Trovato in
/var/local/log/install.log	Creato durante l'installazione del software. Contiene un record degli eventi di installazione.	Tutti i nodi
/var/local/log/expansion-progress.log	Creato durante le operazioni di espansione. Contiene un record degli eventi di espansione.	Nodi di storage
/var/local/log/pa-move.log	Creato durante l'esecuzione di `pa-move.sh` script.	Nodo amministratore primario
/var/local/log/pa-move-new_pa.log	Creato durante l'esecuzione di `pa-move.sh` script.	Nodo amministratore primario

Nome del file	Note	Trovato in
/var/local/log/pa-move-old_pa.log	Creato durante l'esecuzione di `pa-move.sh` script.	Nodo amministratore primario
/var/local/log/gdu-server.log	Creato dal servizio GDU. Contiene eventi correlati alle procedure di provisioning e manutenzione gestite dal nodo di amministrazione primario.	Nodo amministratore primario
/var/local/log/send_admin_hw.log	Creato durante l'installazione. Contiene informazioni di debug relative alle comunicazioni di un nodo con il nodo di amministrazione primario.	Tutti i nodi
/var/local/log/upgrade.log	Creato durante l'aggiornamento del software. Contiene un record degli eventi di aggiornamento software.	Tutti i nodi

Registri per software di terze parti

È possibile utilizzare i registri del software di terze parti per risolvere i problemi.

Categoria	Nome del file	Note	Trovato in
Archiviazione	/var/local/log/dsierror.log	Informazioni sugli errori per le API del client TSM.	Nodi di archiviazione
MySQL	/var/local/log/mysql.err /var/local/log/mysql-slow.log	File di log generati da MySQL. `mysql.err` acquisisce errori e eventi del database, come avvii e arresti. `mysql-slow.log` (Log di query lento) acquisisce le istruzioni SQL che hanno richiesto più di 10 secondi per l'esecuzione.	Nodi di amministrazione
Sistema operativo	/var/local/log/messages	Questa directory contiene i file di log per il sistema operativo. Gli errori contenuti in questi log vengono visualizzati anche in Grid Manager. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare **topologia** > ***Sito*** > ***nodo*** > **SSM** > **Eventi**.	Tutti i nodi

Categoria	Nome del file	Note	Trovato in
NTP	/var/local/log/ntp.log /var/lib/ntp/var/log/ntpstats/	`/var/local/log/ntp.log` Contiene il file di log per i messaggi di errore NTP. `/var/lib/ntp/var/log/ntpstats/` La directory contiene le statistiche di tempo NTP. `loopstats` registra le informazioni statistiche del filtro loop. `peerstats` registra le informazioni delle statistiche peer.	Tutti i nodi

A proposito di bycast.log

Il file `/var/local/log/bycast.log` È il file principale per la risoluzione dei problemi del software StorageGRID. Esiste un `bycast.log` file per ogni nodo della griglia. Il file contiene messaggi specifici del nodo della griglia.

Il file `/var/local/log/bycast-err.log` è un sottoinsieme di `bycast.log`. Contiene messaggi di errore di severità e CRITICI.

In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno. Vedere "Configurare i messaggi di audit e le destinazioni dei log".

Rotazione del file per bycast.log

Quando il `bycast.log` Il file raggiunge 1 GB, il file esistente viene salvato e viene avviato un nuovo file di log.

Il file salvato viene rinominato `bycast.log.1`e il nuovo file viene denominato `bycast.log`. Quando il nuovo `bycast.log` Raggiunge 1 GB, `bycast.log.1` viene rinominato e compresso come `bycast.log.2.gz`, e. `bycast.log` viene rinominato `bycast.log.1`.

Il limite di rotazione per `bycast.log` è di 21 file. Quando la ventiduesima versione di `bycast.log` il file viene creato, il file meno recente viene cancellato.

Il limite di rotazione per `bycast-err.log` sono sette file.

> Se un file di log è stato compresso, non è necessario decomprimerlo nella stessa posizione in cui è stato scritto. La decompressione del file nella stessa posizione può interferire con gli script di rotazione del log.

In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno. Vedere "Configurare i messaggi di audit e le destinazioni dei log".

Informazioni correlate

"Raccogliere i file di log e i dati di sistema"

Messaggi nel bycast.log

Messaggi in `bycast.log` Sono scritti da ADE (Asynchronous Distributed Environment). ADE è l'ambiente di runtime utilizzato dai servizi di ciascun nodo di rete.

Esempio di messaggio ADE:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

I messaggi ADE contengono le seguenti informazioni:

Segmento di messaggio	Valore nell'esempio
ID nodo	12455685
ID processo ADE	0357819531
Nome del modulo	SVMR
Identificatore del messaggio	EVHR
Ora di sistema UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDGH:MM:SS.UUUUUUUU)
Livello di severità	ERRORE
Numero di tracking interno	0906
Messaggio	SVMR: Controllo dello stato di salute sul volume 3 non riuscito con motivo 'TOUT'

Severità dei messaggi nel bycast.log

I messaggi in `bycast.log` sono assegnati livelli di severità.

Ad esempio:

- **NOTA** — si è verificato un evento da registrare. La maggior parte dei messaggi di log è a questo livello.
- **ATTENZIONE** — si è verificata una condizione imprevista.
- **ERRORE** — si è verificato un errore grave che ha un impatto sulle operazioni.
- **CRITICO** — si è verificata una condizione anomala che ha interrotto le normali operazioni. È necessario risolvere immediatamente la condizione sottostante. I messaggi critici vengono visualizzati anche in Grid Manager. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare **Sito** > **nodo** > **SSM** > **Eventi**.

Codici di errore in `bycast.log`

La maggior parte dei messaggi di errore in `bycast.log` contiene codici di errore.

La seguente tabella elenca i codici non numerici comuni in `bycast.log`. Il significato esatto di un codice non numerico dipende dal contesto in cui viene riportato.

Codice di errore	Significato
SUC	Nessun errore
GERR	Sconosciuto
CANC	Annullato
ABRT	Interrotto
TOUT	Timeout
INVL	Non valido
NFND	Non trovato
VERS	Versione
CONF	Configurazione
NON RIUSCITO	Non riuscito
ICPL	Incompleto
FATTO	Fatto
SUNV	Servizio non disponibile

La seguente tabella elenca i codici di errore numerici in `bycast.log`.

Numero di errore	Codice di errore	Significato
001	EPER	Operazione non consentita
002	ENOENT	Nessun file o directory di questo tipo
003	ESRCH	Nessun processo di questo tipo
004	EINTR	Chiamata di sistema interrotta

Numero di errore	Codice di errore	Significato
005	EIO	Errore i/O.
006	ENXIO	Nessun dispositivo o indirizzo di questo tipo
007	E2BIG	Elenco di argomenti troppo lungo
008	ENOEXEC	Errore di formato Exec
009	EBADF	Numero di file errato
010	ECHILD	Nessun processo figlio
011	EAGAIN	Riprovare
012	ENOMEM	Memoria esaurita
013	EACCES	Permesso negato
014	EFAULT	Indirizzo non valido
015	ENOTBLK	Dispositivo a blocchi richiesto
016	EBUSY	Periferica o risorsa occupata
017	EEXIST	Il file esiste
018	ESCLUDI	Collegamento tra dispositivi
019	ENODEV	Nessun dispositivo di questo tipo
020	ENOTDIR	Non una directory
021	EISDIR	È una directory
022	EINVAL	Argomento non valido
023	ENFILE	Overflow della tabella dei file
024	EMFILE	Troppi file aperti
025	ENOTTY	Non è una macchina da scrivere

Numero di errore	Codice di errore	Significato
026	ETXTBSY	File di testo occupato
027	EFBIG	File troppo grande
028	ENOSPC	Spazio non disponibile sul dispositivo
029	ESPIPE	Ricerca illegale
030	EROFS	File system di sola lettura
031	EMSINK	Troppi collegamenti
032	EPIPE	Tubo rotto
033	EDOM	Argomento matematico fuori dominio della funzione
034	ERANGE	Risultato matematico non rappresentabile
035	EDEADLK	Si verificherebbe un deadlock delle risorse
036	ENAMETOLONG	Nome file troppo lungo
037	ENOLCK	Nessun blocco di record disponibile
038	ENOSYS	Funzione non implementata
039	ENOTEMPTY	Directory non vuota
040	ELOOP	Sono stati rilevati troppi collegamenti simbolici
041		
042	ENOMSG	Nessun messaggio del tipo desiderato
043	EIDRM	Identificatore rimosso
044	ECHRNG	Numero di canale fuori intervallo
045	EL2NSYNC	Livello 2 non sincronizzato
046	EL3HLT	Livello 3 interrotto

Numero di errore	Codice di errore	Significato
047	EL3RST	Ripristino livello 3
048	ELNRNG	Numero di collegamento fuori intervallo
049	EUNATCH	Driver del protocollo non collegato
050	ENOCSI	Nessuna struttura CSI disponibile
051	EL2HLT	Livello 2 arrestato
052	EBADE	Scambio non valido
053	EBADR	Descrittore della richiesta non valido
054	ESCLUDI	Exchange pieno
055	ENOANO	Nessun anodo
056	EBADRQC	Codice di richiesta non valido
057	EBADSLT	Slot non valido
058		
059	EBFONT	Formato del file di font non valido
060	ENOSTR	Il dispositivo non è un flusso
061	ENODATA	Nessun dato disponibile
062	ETIME	Timer scaduto
063	ENOSR	Risorse out of Streams
064	ENONET	La macchina non è in rete
065	ENOPKG	Pacchetto non installato
066	EREMOTE	L'oggetto è remoto
067	ENOLINK	Il collegamento è stato separato

Numero di errore	Codice di errore	Significato
068	EADV	Errore di pubblicità
069	ESRMNT	Errore Srmount
070	ECOMM	Errore di comunicazione durante l'invio
071	PRONTO	Errore di protocollo
072	EMULTIHOP	Tentativo di multihop
073	EDOTDOT	Errore specifico RFS
074	EBADMSG	Non è un messaggio dati
075	EOVERFLOW	Valore troppo grande per il tipo di dati definito
076	ENOTUNIQ	Nome non univoco sulla rete
077	EBADFD	Descrittore del file in stato non valido
078	EREMCHG	Indirizzo remoto modificato
079	ELIBACC	Impossibile accedere a una libreria condivisa necessaria
080	ELIBBAD	Accesso a una libreria condivisa danneggiata
081	ELIBSCN	
082	ELIBMAX	Tentativo di collegamento in troppe librerie condivise
083	ELIBEXEC	Impossibile eseguire direttamente una libreria condivisa
084	EILSEQ	Sequenza di byte non valida
085	ERESTART	La chiamata di sistema interrotta deve essere riavviata
086	ESTRPIPE	Errore pipe flussi
087	EUSERS	Troppi utenti

Numero di errore	Codice di errore	Significato
088	ENOTSOCK	Funzionamento socket su non socket
089	EDESTADDRREQ	Indirizzo di destinazione obbligatorio
090	EMSGSIZE	Messaggio troppo lungo
091	EPROTOTYPE	Tipo di protocollo errato per il socket
092	ENOPROTOOPT	Protocollo non disponibile
093	EPROTONOSUPPORT	Protocollo non supportato
094	SESOCKTNOSUPPORT	Tipo di socket non supportato
095	EOPNOTSUPP	Operazione non supportata sull'endpoint di trasporto
096	EPFNOSUPPORT	Famiglia di protocolli non supportata
097	EAFNOSUPPORT	Famiglia di indirizzi non supportata dal protocollo
098	EADDRINUSE	Indirizzo già in uso
099	EADDRNOTAVAIL	Impossibile assegnare l'indirizzo richiesto
100	ENETDOWN	La rete non è disponibile
101	ENETUNREACH	La rete non è raggiungibile
102	ENETRESET	Connessione di rete interrotta a causa del ripristino
103	PRONTO	Il software ha causato l'interruzione della connessione
104	ECONNRESET	Connessione ripristinata da peer
105	ENOBUFS	Spazio buffer non disponibile
106	EISCONN	Endpoint di trasporto già connesso
107	ENOTCONN	Endpoint di trasporto non connesso
108	ESHUTDOWN	Impossibile inviare dopo l'arresto dell'endpoint di trasporto

Numero di errore	Codice di errore	Significato
109	ETOOMANYREFS	Troppi riferimenti: Impossibile unire
110	ETIMEDOUT	Timeout della connessione
111	ECONNREFUSED	Connessione rifiutata
112	EHOSTDOWN	Host non attivo
113	EHOSTUNREACH	Nessun percorso verso l'host
114	EALREADY	Operazione già in corso
115	EINPROGRESS	Operazione in corso
116		
117	EUCLEAN	La struttura deve essere pulita
118	ENOTNAM	Non è un file XENIX denominato
119	ENAVAIL	Nessun semaphore XENIX disponibile
120	EISNAM	È un file di tipo denominato
121	EREMOTEIO	Errore i/o remoto
122	EDQUOT	Quota superata
123	ENOMEDIUM	Nessun supporto trovato
124	EMPDIUMTYPE	Tipo di supporto errato
125	LED ECANCELED	Operazione annullata
126	ENOKEY	Chiave richiesta non disponibile
127	EKEYEXPIRED	Chiave scaduta
128	EKEYREVOKED	Chiave revocata
129	EKEYREJECTED	Chiave rifiutata dal servizio

Numero di errore	Codice di errore	Significato
130	EOWNERDEAD	Per i mutex più forti: Il proprietario è morto
131	ENOTRECOVERABILE	Per mutex affidabili: Stato non ripristinabile

Configurare le destinazioni dei messaggi di controllo e del registro

Considerazioni sull'utilizzo di un server syslog esterno

Un server syslog esterno è un server esterno a StorageGRID che può essere utilizzato per raccogliere informazioni di controllo del sistema in una singola posizione. L'utilizzo di un server syslog esterno consente di ridurre il traffico di rete sui nodi Admin e di gestire le informazioni in modo più efficiente. Per StorageGRID, il formato del pacchetto di messaggi syslog in uscita è conforme con RFC 3164.

I tipi di informazioni di controllo che è possibile inviare al server syslog esterno includono:

- Registri di audit contenenti i messaggi di audit generati durante il normale funzionamento del sistema
- Eventi correlati alla sicurezza, come accessi ed escalation a root
- Log delle applicazioni che potrebbero essere richiesti se è necessario aprire un caso di supporto per risolvere un problema riscontrato

Quando utilizzare un server syslog esterno

Un server syslog esterno è particolarmente utile se si dispone di un grid di grandi dimensioni, se si utilizzano più tipi di applicazioni S3 o se si desidera mantenere tutti i dati di revisione. L'invio di informazioni di audit a un server syslog esterno consente di:

- Raccogliere e gestire in modo più efficiente le informazioni di audit come messaggi di audit, registri delle applicazioni ed eventi di sicurezza.
- Riduci il traffico di rete sui nodi amministrativi, perché le informazioni di audit vengono trasferite direttamente dai vari nodi storage al server syslog esterno, senza dover passare attraverso un nodo amministrativo.

> Quando i log vengono inviati a un server syslog esterno, i log singoli superiori a 8.192 byte vengono troncati alla fine del messaggio in conformità con le limitazioni comuni nelle implementazioni del server syslog esterno.

> Per massimizzare le opzioni per il recovery completo dei dati in caso di guasto del server syslog esterno, fino a 20 GB di registri locali di record di revisione (`localaudit.log`) sono mantenuti su ogni nodo.

Come configurare un server syslog esterno

Per informazioni su come configurare un server syslog esterno, vedere "Configurare i messaggi di controllo e il server syslog esterno".

Se si intende configurare l'utilizzo del protocollo TLS o RELP/TLS, è necessario disporre dei seguenti certificati:

- **Certificati CA del server**: Uno o più certificati CA attendibili per la verifica del server syslog esterno nella codifica PEM. Se omesso, verrà utilizzato il certificato Grid CA predefinito.
- **Certificato client**: Certificato client per l'autenticazione al server syslog esterno nella codifica PEM.
- **Chiave privata client**: Chiave privata per il certificato client nella codifica PEM.

> Se si utilizza un certificato client, è necessario utilizzare anche una chiave privata client. Se si fornisce una chiave privata crittografata, è necessario fornire anche la passphrase. L'utilizzo di una chiave privata crittografata non offre alcun vantaggio significativo in termini di sicurezza, in quanto è necessario memorizzare la chiave e la passphrase; per semplicità, si consiglia di utilizzare una chiave privata non crittografata, se disponibile.

Come valutare le dimensioni del server syslog esterno

Normalmente, il tuo grid è dimensionato per ottenere un throughput richiesto, definito in termini di operazioni S3 al secondo o byte al secondo. Ad esempio, potrebbe essere necessario che la griglia gestisca 1,000 operazioni S3 al secondo, o 2,000 MB al secondo, di acquisizione e recupero di oggetti. È necessario dimensionare il server syslog esterno in base ai requisiti dei dati del grid.

Questa sezione fornisce alcune formule euristiche che consentono di stimare la velocità e la dimensione media dei messaggi di log di vari tipi che il server syslog esterno deve gestire, espresse in termini di caratteristiche di performance note o desiderate della griglia (operazioni S3 al secondo).

Utilizzare le operazioni S3 al secondo nelle formule di stima

Se la griglia è stata dimensionata per un throughput espresso in byte al secondo, è necessario convertire questo dimensionamento in operazioni S3 al secondo per utilizzare le formule di stima. Per convertire il throughput della griglia, è necessario innanzitutto determinare la dimensione media degli oggetti, che è possibile utilizzare utilizzando le informazioni contenute nei registri di audit e nelle metriche esistenti (se presenti), oppure utilizzando la conoscenza delle applicazioni che utilizzeranno StorageGRID. Ad esempio, se la griglia è stata dimensionata per ottenere un throughput di 2,000 MB/secondo e la dimensione media dell'oggetto è di 2 MB, la griglia è stata dimensionata in modo da poter gestire 1,000 operazioni S3 al secondo (2,000 MB/2 MB).

> Le formule per il dimensionamento del server syslog esterno nelle sezioni seguenti forniscono stime dei casi comuni (piuttosto che stime dei casi peggiori). A seconda della configurazione e del carico di lavoro, è possibile che venga visualizzata una velocità di messaggi syslog o un volume di dati syslog superiore o inferiore rispetto a quanto previsto dalle formule. Le formule devono essere utilizzate solo come linee guida.

Formule di stima per i log di audit

Se non si dispone di informazioni sul carico di lavoro S3 diverse dal numero di operazioni S3 al secondo supportate dal grid, è possibile stimare il volume dei registri di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule: Presupponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie sono impostate su normale, ad eccezione dello storage, che è impostato su errore):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Ad esempio, se la griglia è dimensionata per 1,000 operazioni S3 al secondo, il server syslog esterno deve essere dimensionato in modo da supportare 2,000 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere memorizzare) i dati del registro di controllo a una velocità di 1.6 MB al secondo.

Se conosci meglio il tuo carico di lavoro, puoi effettuare stime più accurate. Per i registri di audit, le variabili aggiuntive più importanti sono la percentuale di operazioni S3 che vengono messe (rispetto a. GETS) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni a 4 caratteri utilizzate nella tabella sono i nomi dei campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Tasto S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.

Utilizziamo P per rappresentare la percentuale di operazioni S3 che vengono messe, dove 0 ≤ P ≤ 1 (quindi per un carico di lavoro PUT del 100%, P = 1 e per un carico DI lavoro GET del 100%, P = 0).

Utilizzare K per rappresentare la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi il valore di K è 90 (13+13+28+36).

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei registri di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule, presupponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie sono impostate su normale, ad eccezione di Storage, Che è impostato su Error):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Ad esempio, se il tuo grid è dimensionato per 1,000 operazioni S3 al secondo, il tuo carico di lavoro è pari al 50% di put e i tuoi nomi account S3, nomi bucket, E i nomi degli oggetti hanno una media di 90 byte, il server

syslog esterno deve essere dimensionato per supportare 1,500 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere memorizzare) i dati del registro di controllo a una velocità di circa 1 MB al secondo.

Formule di stima per livelli di audit non predefiniti

Le formule fornite per i registri di controllo presuppongono l'utilizzo delle impostazioni predefinite del livello di controllo (tutte le categorie sono impostate su normale, ad eccezione dello storage, che è impostato su errore). Non sono disponibili formule dettagliate per la stima del tasso e della dimensione media dei messaggi di audit per le impostazioni del livello di audit non predefinite. Tuttavia, la seguente tabella può essere utilizzata per effettuare una stima approssimativa del tasso; è possibile utilizzare la formula delle dimensioni medie fornita per i registri di controllo, ma è probabile che si verifichi una sovrastima perché i messaggi di controllo "extra" sono, in media, più piccoli dei messaggi di controllo predefiniti.

Condizione	Formula
Replica: Tutti i livelli di controllo sono impostati su Debug o Normal	Tasso del registro di controllo = 8 x S3 tasso di operazioni
Erasure coding (codifica erasure): I livelli di audit sono tutti impostati su Debug o Normal (normale)	Utilizzare la stessa formula utilizzata per le impostazioni predefinite

Formule di stima per gli eventi di sicurezza

Gli eventi di sicurezza non sono correlati con le operazioni S3 e in genere producono un volume trascurabile di log e dati. Per questi motivi, non vengono fornite formule di stima.

Formule di stima per i log delle applicazioni

Se non si dispone di informazioni sul carico di lavoro S3 diverse dal numero di operazioni S3 al secondo supportate dal grid, è possibile stimare il volume di log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Ad esempio, se il grid è dimensionato per 1,000 operazioni S3 al secondo, il server syslog esterno deve essere dimensionato in modo da supportare 3,300 log delle applicazioni al secondo ed essere in grado di ricevere (e memorizzare) i dati del log delle applicazioni a una velocità di circa 1.2 MB al secondo.

Se conosci meglio il tuo carico di lavoro, puoi effettuare stime più accurate. Per i log delle applicazioni, le variabili aggiuntive più importanti sono la strategia di protezione dei dati (replica vs Erasure coding), la percentuale di operazioni S3 che vengono messe (rispetto a. Gets/Other) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni a 4 caratteri utilizzate nella tabella sono i nomi dei campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Tasto S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.

Stime di dimensionamento di esempio

In questa sezione vengono illustrati esempi di utilizzo delle formule di stima per le griglie con i seguenti metodi di protezione dei dati:

- Replica
- Erasure coding

Se si utilizza la replica per la protezione dei dati

Sia P la percentuale di operazioni S3 che vengono messe, dove 0 ≤ P ≤ 1 (quindi per un carico di lavoro PUT del 100%, P = 1 e per un carico DI lavoro GET del 100%, P = 0).

Sia K la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi K ha un valore di 90 (13+13+28+36).

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

Ad esempio, se il grid è dimensionato per 1,000 operazioni S3 al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket e i nomi degli oggetti sono in media di 90 byte, il server syslog esterno deve essere dimensionato in modo da supportare 1800 log delle applicazioni al secondo, E riceverà (e in genere memorizzerà) i dati delle applicazioni a una velocità di 0.5 MB al secondo.

Se si utilizza l'erasure coding per la protezione dei dati

Sia P la percentuale di operazioni S3 che vengono messe, dove 0 ≤ P ≤ 1 (quindi per un carico di lavoro PUT del 100%, P = 1 e per un carico DI lavoro GET del 100%, P = 0).

Sia K la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi K ha un valore di 90 (13+13+28+36).

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

Ad esempio, se il grid è dimensionato per 1.000 S3 operazioni al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket mentre i nomi degli oggetti hanno una media di 90 byte, il server syslog esterno dovrebbe essere dimensionato in modo da supportare 2.250 registri delle applicazioni al secondo e dovrebbe essere in grado di ricevere (e generalmente archiviare) dati delle applicazioni a una velocità di 0,6 MB al secondo.

Configurare i messaggi di controllo e il server syslog esterno

È possibile configurare una serie di impostazioni relative ai messaggi di controllo. È possibile regolare il numero di messaggi di controllo registrati, definire eventuali intestazioni di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client, configurare un server syslog esterno e specificare dove vengono inviati i registri di controllo, i registri degli eventi di protezione e i registri del software StorageGRID.

I messaggi e i registri di audit registrano le attività del sistema e gli eventi di sicurezza e sono strumenti essenziali per il monitoraggio e la risoluzione dei problemi. Tutti i nodi StorageGRID generano messaggi di audit e registri per tenere traccia dell'attività e degli eventi del sistema.

In alternativa, è possibile configurare un server syslog esterno per salvare le informazioni di revisione in remoto. L'utilizzo di un server esterno riduce al minimo l'impatto delle prestazioni della registrazione dei messaggi di controllo senza ridurre la completezza dei dati di controllo. Un server syslog esterno è particolarmente utile se si dispone di un grid di grandi dimensioni, se si utilizzano più tipi di applicazioni S3 o se si desidera mantenere tutti i dati di revisione. Vedere "Considerazioni sul server syslog esterno" per ulteriori informazioni.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Se si prevede di configurare un server syslog esterno, è stata esaminata la "considerazioni sull'utilizzo di un server syslog esterno" e ha assicurato che il server abbia capacità sufficiente per ricevere e memorizzare i file di registro.

- Se si intende configurare un server syslog esterno utilizzando il protocollo TLS o RELP/TLS, si dispone della CA del server e dei certificati client richiesti e della chiave privata del client.

Modificare i livelli dei messaggi di controllo

È possibile impostare un livello di audit diverso per ciascuna delle seguenti categorie di messaggi nel registro di audit:

Categoria di audit	Impostazione predefinita	Ulteriori informazioni
Sistema	Normale	"Messaggi di audit del sistema"
Storage	Errore	"Messaggi di audit dello storage a oggetti"
Gestione	Normale	"Messaggio di audit della gestione"
Letture del client	Normale	"Messaggi di audit in lettura del client"
Il client scrive	Normale	"Messaggi di audit di scrittura del client"
ILM	Normale	"Messaggi di controllo ILM"
Replica cross-grid	Errore	"CGRR: Richiesta di replica cross-grid"

Queste impostazioni predefinite si applicano se StorageGRID è stato installato inizialmente utilizzando la versione 10.3 o successiva. Se inizialmente è stata utilizzata una versione precedente di StorageGRID, l'impostazione predefinita per tutte le categorie è normale.

Durante gli aggiornamenti, le configurazioni a livello di audit non saranno effettive immediatamente.

Fasi

1. Selezionare **CONFIGURATION** > **Monitoring** > **Audit and syslog server**.
2. Per ciascuna categoria di messaggi di audit, selezionare un livello di audit dall'elenco a discesa:

Livello di audit	Descrizione
Spento	Non vengono registrati messaggi di audit della categoria.
Errore	Vengono registrati solo messaggi di errore - messaggi di audit per i quali il codice risultato non è stato "riuscito" (SUCS).
Normale	Vengono registrati i messaggi transazionali standard, ovvero i messaggi elencati in queste istruzioni per la categoria.

Livello di audit	Descrizione
Debug	Obsoleto. Questo livello si comporta come il livello di audit normale.

I messaggi inclusi per qualsiasi livello specifico includono quelli che verrebbero registrati ai livelli superiori. Ad esempio, il livello normale include tutti i messaggi di errore.

> Se non si richiede un record dettagliato delle operazioni di lettura del client per le applicazioni S3, modificare l'impostazione **letture del client** su **errore** per ridurre il numero di messaggi di audit registrati nel registro di audit.

3. Selezionare **Salva**.

   Un banner verde indica che la configurazione è stata salvata.

Definire le intestazioni delle richieste HTTP

Facoltativamente, è possibile definire qualsiasi intestazione di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client. Queste intestazioni di protocollo si applicano solo alle richieste S3 e Swift.

Fasi

1. Nella sezione **Audit Protocol headers**, definire le intestazioni di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client.

   Utilizzare un asterisco (**) come carattere jolly per far corrispondere zero o più caratteri. Utilizzare la sequenza escape (**) per far corrispondere un asterisco letterale.

2. Selezionare **Add another header** (Aggiungi un'altra intestazione) per creare altre intestazioni, se necessario.

   Quando le intestazioni HTTP vengono trovate in una richiesta, vengono incluse nel messaggio di audit nel campo HTRH.

   > Le intestazioni delle richieste del protocollo di audit vengono registrate solo se il livello di audit per **letture client** o **scritture client** non è **disattivato**.

3. Selezionare **Salva**

   Un banner verde indica che la configurazione è stata salvata.

Usa un server syslog esterno

In alternativa, è possibile configurare un server syslog esterno per salvare registri di controllo, registri delle applicazioni e registri di eventi di sicurezza in una posizione esterna alla griglia.

> Se non si desidera utilizzare un server syslog esterno, ignorare questo passaggio e andare a Selezionare le destinazioni delle informazioni di audit.

Se le opzioni di configurazione disponibili in questa procedura non sono sufficientemente flessibili da soddisfare le proprie esigenze, è possibile applicare ulteriori opzioni di configurazione utilizzando `audit-destinations` Endpoint, che si trovano nella sezione API privata di "API di Grid Management". Ad esempio, è possibile utilizzare l'API se si desidera utilizzare server syslog diversi per diversi gruppi di nodi.

Inserire le informazioni di syslog

Accedere alla procedura guidata Configura server syslog esterno e fornire le informazioni di cui StorageGRID ha bisogno per accedere al server syslog esterno.

Fasi

1. Dalla pagina Audit and syslog server (controllo e server syslog), selezionare **Configure external syslog server** (Configura server syslog esterno Oppure, se è stato precedentemente configurato un server syslog esterno, selezionare **Modifica server syslog esterno**.

   Viene visualizzata la procedura guidata Configura server syslog esterno.

2. Per la fase **inserire le informazioni syslog** della procedura guidata, immettere un nome di dominio completo valido o un indirizzo IPv4 o IPv6 per il server syslog esterno nel campo **host**.
3. Inserire la porta di destinazione sul server syslog esterno (deve essere un numero intero compreso tra 1 e 65535). La porta predefinita è 514.
4. Selezionare il protocollo utilizzato per inviare le informazioni di audit al server syslog esterno.

   Si consiglia di utilizzare **TLS** o **RELP/TLS**. Per utilizzare una di queste opzioni, è necessario caricare un certificato del server. L'utilizzo dei certificati consente di proteggere le connessioni tra la griglia e il server syslog esterno. Per ulteriori informazioni, vedere "Gestire i certificati di sicurezza".

   Tutte le opzioni del protocollo richiedono il supporto e la configurazione del server syslog esterno. È necessario scegliere un'opzione compatibile con il server syslog esterno.

   Il protocollo RELP (Reliable Event Logging Protocol) estende le funzionalità del protocollo syslog per fornire un'erogazione affidabile dei messaggi di evento. L'utilizzo di RELP può contribuire a prevenire la perdita di informazioni di controllo nel caso in cui il server syslog esterno debba essere riavviato.

5. Selezionare **continua**.
6. se si seleziona **TLS** o **RELP/TLS**, caricare i certificati CA del server, il certificato client e la chiave privata del client.
   a. Selezionare **Sfoglia** per il certificato o la chiave che si desidera utilizzare.
   b. Selezionare il certificato o il file della chiave.
   c. Selezionare **Open** per caricare il file.

      Accanto al nome del certificato o del file della chiave viene visualizzato un segno di spunta verde che indica che il caricamento è stato eseguito correttamente.

7. Selezionare **continua**.

Gestire il contenuto syslog

È possibile selezionare le informazioni da inviare al server syslog esterno.

Fasi

1. Per la fase **Gestisci contenuto syslog** della procedura guidata, selezionare ogni tipo di informazione di audit che si desidera inviare al server syslog esterno.
   - **Invia log di audit**: Invia eventi StorageGRID e attività di sistema
   - **Invia eventi di sicurezza**: Invia eventi di sicurezza, ad esempio quando un utente non autorizzato tenta di effettuare l'accesso o un utente accede come root
   - **Send application logs**: Invia file di log utili per la risoluzione dei problemi, tra cui:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (Solo nodi di amministrazione)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`

   Per informazioni sui registri del software StorageGRID, vedere "Log del software StorageGRID".

2. Utilizzare i menu a discesa per selezionare la gravità e la struttura (tipo di messaggio) per ciascuna categoria di informazioni di controllo che si desidera inviare.

   L'impostazione dei valori di gravità e struttura consente di aggregare i registri in modo personalizzabile per semplificare l'analisi.

   a. Per **gravità**, selezionare **Passthrough** oppure selezionare un valore di gravità compreso tra 0 e 7.

      Se si seleziona un valore, il valore selezionato verrà applicato a tutti i messaggi di questo tipo. Le informazioni sui diversi livelli di gravità andranno perse se si sovrascrive la gravità con un valore fisso.

Severità	Descrizione
Passthrough	Ogni messaggio inviato al syslog esterno per avere lo stesso valore di gravità di quando è stato registrato localmente sul nodo: • Per i registri di controllo, la gravità è "info". • Per gli eventi di sicurezza, i valori di gravità sono generati dalla distribuzione Linux sui nodi. • Per i registri delle applicazioni, i livelli di gravità variano tra "info" e "avviso", a seconda del problema. Ad esempio, aggiungendo un server NTP e configurando un gruppo ha si ottiene il valore "info", mentre arrestando intenzionalmente il servizio SSM o RSM si ottiene il valore "avviso".
0	Emergenza: Il sistema non è utilizzabile

Severità	Descrizione
1	Attenzione: L'azione deve essere eseguita immediatamente
2	Critico: Condizioni critiche
3	Errore: Condizioni di errore
4	Avvertenza: Condizioni di avviso
5	Avviso: Condizione normale ma significativa
6	Informativo: Messaggi informativi
7	Debug: Messaggi a livello di debug

b. Per **Facilty**, selezionare **Passthrough** o selezionare un valore di struttura compreso tra 0 e 23.

Se si seleziona un valore, questo verrà applicato a tutti i messaggi di questo tipo. Le informazioni sulle diverse strutture andranno perse se si sostituisce la struttura con un valore fisso.

Struttura	Descrizione
Passthrough	Ogni messaggio inviato al syslog esterno per avere lo stesso valore di struttura di quando è stato collegato localmente al nodo: • Per i registri di controllo, la struttura inviata al server syslog esterno è "local7". • Per gli eventi di sicurezza, i valori della struttura vengono generati dalla distribuzione linux sui nodi. • Per i registri delle applicazioni, i registri delle applicazioni inviati al server syslog esterno presentano i seguenti valori di struttura: ◦ `bycast.log`: utente o daemon ◦ `bycast-err.log`: utente, daemon, local3 o local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6
0	kern (messaggi kernel)
1	utente (messaggi a livello utente)

Struttura	Descrizione
2	mail
3	daemon (daemon di sistema)
4	auth (messaggi di sicurezza/autorizzazione)
5	syslog (messaggi generati internamente da syslogd)
6	lpr (sottosistema di stampanti di linea)
7	news (sottosistema notizie di rete)
8	UUCP
9	cron (daemon di clock)
10	sicurezza (messaggi di sicurezza/autorizzazione)
11	FTP
12	NTP
13	logaudit (audit del log)
14	logalert (avviso di log)
15	clock (daemon di clock)
16	local0
17	locale1
18	locale2
19	locale3
20	locale4
21	locale5
22	locale6
23	locale7

3. Selezionare **continua**.

Inviare messaggi di test

Prima di iniziare a utilizzare un server syslog esterno, è necessario richiedere a tutti i nodi della griglia di inviare messaggi di test al server syslog esterno. È necessario utilizzare questi messaggi di test per convalidare l'intera infrastruttura di raccolta dei log prima di inviare i dati al server syslog esterno.

> Non utilizzare la configurazione del server syslog esterno fino a quando non si conferma che il server syslog esterno ha ricevuto un messaggio di test da ciascun nodo della griglia e che il messaggio è stato elaborato come previsto.

Fasi

1. Se non si desidera inviare messaggi di test perché si è certi che il server syslog esterno sia configurato correttamente e che sia in grado di ricevere informazioni di controllo da tutti i nodi della griglia, selezionare **Ignora e termina**.

   Un banner verde indica che la configurazione è stata salvata.

2. In caso contrario, selezionare **Invia messaggi di prova** (scelta consigliata).

   I risultati del test vengono visualizzati continuamente sulla pagina fino a quando non si interrompe il test. Mentre il test è in corso, i messaggi di controllo continuano a essere inviati alle destinazioni precedentemente configurate.

3. Se si verificano errori durante la configurazione del server syslog o in fase di esecuzione, correggerli e selezionare nuovamente **Invia messaggi di prova**.

   Vedere "Risolvere i problemi di un server syslog esterno" per risolvere eventuali errori.

4. Attendere che venga visualizzato un banner verde che indica che tutti i nodi hanno superato il test.
5. Controllare il server syslog per determinare se i messaggi di test vengono ricevuti ed elaborati come previsto.

   > Se si utilizza UDP, controllare l'intera infrastruttura di raccolta dei log. Il protocollo UDP non consente un rilevamento degli errori rigoroso come l'altro protocolli.

6. Selezionare **Stop and Finish** (Interrompi e termina).

   Viene nuovamente visualizzata la pagina **Audit and syslog server**. Un banner verde indica che la configurazione del server syslog è stata salvata.

   > Le informazioni di audit StorageGRID non vengono inviate al server syslog esterno finché non si seleziona una destinazione che include il server syslog esterno.

Selezionare le destinazioni delle informazioni di audit

È possibile specificare la posizione dei registri di controllo, dei registri eventi di protezione e. "Log del software StorageGRID" vengono inviati.

StorageGRID utilizza per impostazione predefinita le destinazioni di controllo dei nodi locali e memorizza le informazioni di controllo in `/var/local/log/localaudit.log`.

Quando si utilizza `/var/local/log/localaudit.log`, le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di archiviazione. È possibile individuare il nodo con le voci più recenti utilizzando il `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` comando.

Alcune destinazioni sono disponibili solo se è stato configurato un server syslog esterno.

Fasi

1. Nella pagina Audit and syslog server (Server audit e syslog), selezionare la destinazione per le informazioni di audit.

Solo nodi locali e **Server syslog esterno** in genere offrono prestazioni migliori.

Opzione	Descrizione
Solo nodi locali (impostazione predefinita)	I messaggi di controllo, i registri degli eventi di protezione e i registri delle applicazioni non vengono inviati ai nodi amministrativi. Vengono invece salvati solo sui nodi che li hanno generati ("nodo locale"). Le informazioni di controllo generate su ogni nodo locale sono memorizzate in `/var/local/log/localaudit.log`. **Nota**: StorageGRID rimuove periodicamente i log locali in una rotazione per liberare spazio. Quando il file di log di un nodo raggiunge 1 GB, il file esistente viene salvato e viene avviato un nuovo file di log. Il limite di rotazione per il log è di 21 file. Quando viene creata la ventiduesima versione del file di log, il file di log più vecchio viene cancellato. In media, su ciascun nodo vengono memorizzati circa 20 GB di dati di log.
Nodi amministrativi/nodi locali	I messaggi di controllo vengono inviati al registro di controllo sui nodi Admin, mentre i registri degli eventi di protezione e i registri delle applicazioni vengono memorizzati sui nodi che li hanno generati. Le informazioni di controllo sono memorizzate nei seguenti file: • Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante. Potrebbe contenere informazioni secondarie, ad esempio una copia aggiuntiva di alcuni messaggi.
Server syslog esterno	Le informazioni di controllo vengono inviate a un server syslog esterno e salvate sui nodi locali (`/var/local/log/localaudit.log`). Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.

Opzione	Descrizione
Nodo di amministrazione e server syslog esterno	I messaggi di controllo vengono inviati al registro di controllo (`/var/local/audit/export/audit.log`) sui nodi Admin e le informazioni di controllo vengono inviate al server syslog esterno e salvate sul nodo locale (`/var/local/log/localaudit.log`. Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.

2. Selezionare **Salva**.

   Viene visualizzato un messaggio di avviso.

3. Selezionare **OK** per confermare che si desidera modificare la destinazione per le informazioni di controllo.

   Un banner verde indica che la configurazione di controllo è stata salvata.

   I nuovi registri vengono inviati alle destinazioni selezionate. I registri esistenti rimangono nella posizione corrente.

Utilizzare il monitoraggio SNMP

USA monitoraggio SNMP: Panoramica

Se si desidera monitorare StorageGRID utilizzando il protocollo SNMP (Simple Network Management Protocol), è necessario configurare l'agente SNMP incluso in StorageGRID.

- "Configurare l'agente SNMP"
- "Aggiornare l'agente SNMP"

Funzionalità

Ogni nodo StorageGRID esegue un agente SNMP, o daemon, che fornisce un MIB. Il MIB StorageGRID contiene definizioni di tabella e notifica per avvisi e allarmi. Il MIB contiene anche informazioni sulla descrizione del sistema, come il numero di piattaforma e il numero di modello per ciascun nodo. Ogni nodo StorageGRID supporta anche un sottoinsieme di oggetti MIB-II.

Vedere "Accedere ai file MIB" Se si desidera scaricare i file MIB sui nodi della griglia.

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. Fornisce accesso MIB di sola lettura per le query e può inviare due tipi di notifiche basate sugli eventi a un sistema di gestione:

Trappole

I 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.

Informa

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 tentativi.

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 "Nodo Admin mittente preferito".

  Ogni avviso viene associato a uno dei tre tipi di trap in base al livello di gravità dell'avviso: ActiveMinorAlert, activeMajorAlert e activeCriticalAlert. Per un elenco degli avvisi che possono attivare questi trap, vedere "Riferimenti agli avvisi".

- Certo "allarmi (sistema legacy)" vengono attivati a livelli di gravità specificati o superiori.

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

Supporto della versione SNMP

La tabella fornisce un riepilogo generale dei contenuti supportati per ciascuna versione SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Query (GET e GETNEXT)	Query MIB di sola lettura	Query MIB di sola lettura	Query MIB di sola lettura
Autenticazione delle query	Stringa di comunità	Stringa di comunità	Utente del modello di sicurezza basato sull'utente (USM)
Notifiche (INTRAPPOLARE e INFORMARE)	Solo trap	Trap e informa	Trap e informa
Autenticazione delle notifiche	Community trap predefinita o stringa di comunità personalizzata per ciascuna destinazione trap	Community trap predefinita o stringa di comunità personalizzata per ciascuna destinazione trap	Utente USM per ciascuna destinazione trap

Limitazioni

- StorageGRID supporta l'accesso MIB di sola lettura. L'accesso in lettura/scrittura non è supportato.

- Tutti i nodi della griglia ricevono la stessa configurazione.
- SNMPv3: StorageGRID non supporta la modalità di supporto per il trasporto (TSM).
- SNMPv3: L'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).
- SNMPv3: L'unico protocollo per la privacy supportato è AES.

Configurare l'agente SNMP

È possibile configurare l'agente SNMP StorageGRID in modo che utilizzi un sistema di gestione SNMP di terze parti per l'accesso MIB di sola lettura e le notifiche.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

L'agente SNMP di StorageGRID supporta SNMPv1, SNMPv2c e SNMPv3. È possibile configurare l'agente per una o più versioni.
Per SNMPv3, è supportata solo l'autenticazione del modello di sicurezza utente (USM).

Tutti i nodi nella griglia utilizzano la stessa configurazione SNMP.

Specificare la configurazione di base

Come prima fase, attivare l'agente SMNP StorageGRID e fornire informazioni di base.

Fasi

1. Selezionare **CONFIGURATION** > **Monitoring** > **SNMP Agent**.

   Viene visualizzata la pagina SNMP Agent.

2. Per attivare l'agente SNMP su tutti i nodi della griglia, selezionare la casella di controllo **Enable SNMP** (attiva SNMP).
3. Inserire le seguenti informazioni nella sezione Configurazione di base.

Campo	Descrizione
Contatto per il sistema	Opzionale. Il contatto principale per il sistema StorageGRID, che viene restituito nei messaggi SNMP come sysContact. In genere, il contatto di sistema è un indirizzo e-mail. Questo valore si applica a tutti i nodi nel sistema StorageGRID. **Il contatto di sistema** può contenere al massimo 255 caratteri.

Campo	Descrizione
Ubicazione del sistema	Opzionale. La posizione del sistema StorageGRID, che viene restituita nei messaggi SNMP come sysLocation. La posizione del sistema può essere una qualsiasi informazione utile per identificare la posizione del sistema StorageGRID. Ad esempio, è possibile utilizzare l'indirizzo di una struttura. Questo valore si applica a tutti i nodi nel sistema StorageGRID. **La posizione del sistema** può contenere al massimo 255 caratteri.
Attivare le notifiche dell'agente SNMP	• Se selezionata, l'agente SNMP StorageGRID invia notifiche trap e inform. • Se questa opzione non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.
Abilita trap di autenticazione	Se selezionata, l'agente SNMP StorageGRID invia trap di autenticazione se riceve messaggi di protocollo autenticati in modo errato.

Immettere le stringhe di comunità

Se si utilizza SNMPv1 o SNMPv2c, completare la sezione Community Strings (stringhe comunità).

Quando il sistema di gestione interroga il MIB StorageGRID, invia una stringa di comunità. Se la stringa di comunità corrisponde a uno dei valori specificati, l'agente SNMP invia una risposta al sistema di gestione.

Fasi

1. Per **comunità di sola lettura**, è possibile immettere una stringa di comunità per consentire l'accesso MIB di sola lettura agli indirizzi di agenti IPv4 e IPv6.

   Per garantire la sicurezza del sistema StorageGRID, non utilizzare "public" come stringa di comunità. Se questo campo viene lasciato vuoto, l'agente SNMP utilizza l'ID griglia del sistema StorageGRID come stringa di comunità.

   Ogni stringa di community può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

2. Selezionare **Aggiungi un'altra stringa di comunità** per aggiungere altre stringhe.

   Sono consentite fino a cinque stringhe.

creare destinazioni trap

Utilizzare la scheda destinazioni trap nella sezione altre configurazioni per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

Fasi

1. Per il campo **Comunità trap predefinita**, è possibile immettere la stringa di comunità predefinita che si desidera utilizzare per le destinazioni trap SNMPv1 o SNMPv2.

Se necessario, è possibile fornire una stringa di comunità diversa ("personalizzata") quando si definisce una destinazione trap specifica.

La comunità trap predefinita può contenere al massimo 32 caratteri e non può contenere spazi vuoti.

2. Per aggiungere una destinazione trap, selezionare **Crea**.
3. Selezionare la versione SNMP che verrà utilizzata per la destinazione trap.
4. Completare il modulo Crea destinazione trap per la versione selezionata.

SNMPv1

Se si seleziona SNMPv1 come versione, completare questi campi.

Campo	Descrizione
Tipo	Deve essere trap per SNMPv1.
Host	Un indirizzo IPv4 o IPv6 o un nome di dominio completo (FQDN) per ricevere il trap.
Porta	Utilizzare 162, quale porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv2c

Se si seleziona SNMPv2c come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv3

Se si seleziona SNMPv3 come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Utente USM	L'utente USM che verrà utilizzato per l'autenticazione. • Se si seleziona **Trap**, vengono visualizzati solo gli utenti USM senza ID motore autorevoli. • Se si seleziona **inform**, vengono visualizzati solo gli utenti USM con ID motore autorevoli. • Se non viene visualizzato alcun utente: i. Creare e salvare la destinazione trap. ii. Passare a. Creare utenti USM e creare l'utente. iii. Tornare alla scheda Destinazioni trap, selezionare la destinazione salvata dalla tabella e selezionare **Modifica**. iv. Selezionare l'utente.

5. Selezionare **Crea**.

   La destinazione trap viene creata e aggiunta alla tabella.

Creare gli indirizzi degli agenti

Facoltativamente, utilizzare la scheda indirizzi agente nella sezione altre configurazioni per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

Se non si configura un indirizzo dell'agente, l'indirizzo di ascolto predefinito è la porta UDP 161 su tutte le reti StorageGRID.

Fasi

1. Selezionare **Crea**.
2. Inserire le seguenti informazioni.

Campo	Descrizione
Protocollo Internet	Se questo indirizzo utilizzerà IPv4 o IPv6. Per impostazione predefinita, SNMP utilizza IPv4.

Campo	Descrizione
Protocollo di trasporto	Se questo indirizzo utilizza UDP o TCP. Per impostazione predefinita, SNMP utilizza UDP.
Rete StorageGRID	La rete StorageGRID su cui l'agente ascolta. • Grid, Admin e Client Networks (reti Grid, Admin e Client): L'agente SNMP è in attesa di query su tutte e tre le reti. • Grid Network • Admin Network (rete amministrativa) • Rete client **Nota**: Se si utilizza la rete client per i dati non protetti e si crea un indirizzo agente per la rete client, tenere presente che anche il traffico SNMP non sarà sicuro.
Porta	Facoltativamente, il numero di porta su cui l'agente SNMP deve essere in attesa. La porta UDP predefinita per un agente SNMP è 161, ma è possibile immettere qualsiasi numero di porta inutilizzato. **Nota**: Quando si salva l'agente SNMP, StorageGRID apre automaticamente le porte degli indirizzi dell'agente sul firewall interno. È necessario assicurarsi che tutti i firewall esterni consentano l'accesso a queste porte.

3. Selezionare **Crea**.

   L'indirizzo dell'agente viene creato e aggiunto alla tabella.

creare utenti USM

Se si utilizza SNMPv3, utilizzare la scheda utenti USM nella sezione altre configurazioni per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

> SNMPv3 *inform* le destinazioni devono avere utenti con ID motore. SNMPv3 la destinazione *trap* non può avere utenti con ID motore.

Questi passaggi non si applicano solo se si utilizza SNMPv1 o SNMPv2c.

Fasi

1. Selezionare **Crea**.
2. Inserire le seguenti informazioni.

Campo	Descrizione
Nome utente	Un nome univoco per questo utente USM. I nomi utente possono avere un massimo di 32 caratteri e non possono contenere spazi vuoti. Il nome utente non può essere modificato dopo la creazione dell'utente.
Accesso MIB di sola lettura	Se selezionata, l'opzione consente all'utente di accedere in sola lettura al MIB.
ID motore autorevole	Se l'utente verrà utilizzato in una destinazione inform, l'ID motore autorevole per questo utente. Inserire da 10 a 64 caratteri esadecimali (da 5 a 32 byte) senza spazi. Questo valore è necessario per gli utenti USM che verranno selezionati nelle destinazioni trap per gli informa. Questo valore non è consentito per gli utenti USM che verranno selezionati nelle destinazioni trap per trap. **Nota**: Questo campo non viene visualizzato se si seleziona **accesso MIB di sola lettura** perché gli utenti USM che hanno accesso MIB di sola lettura non possono avere ID motore.
Livello di sicurezza	Il livello di sicurezza per l'utente USM: • **Authprim**: Questo utente comunica con autenticazione e privacy (crittografia). È necessario specificare un protocollo di autenticazione e una password, nonché un protocollo e una password per la privacy. • **AuthNoPriv**: Questo utente comunica con autenticazione e senza privacy (senza crittografia). Specificare un protocollo di autenticazione e una password.
Protocollo di autenticazione	Impostare sempre su SHA, che è l'unico protocollo supportato (HMAC-SHA-96).
Password	La password che l'utente utilizzerà per l'autenticazione.
Protocollo di privacy	Visualizzato solo se si seleziona **authviv** e si imposta sempre su AES, che è l'unico protocollo di privacy supportato.
Password	Visualizzato solo se è stato selezionato **authviv**. La password che l'utente utilizzerà per la privacy.

3. Selezionare **Crea**.

   L'utente USM viene creato e aggiunto alla tabella.

4. Una volta completata la configurazione dell'agente SNMP, selezionare **Salva**.

La nuova configurazione dell'agente SNMP diventa attiva.

Aggiornare l'agente SNMP

È possibile disattivare le notifiche SNMP, aggiornare le stringhe di comunità o aggiungere o rimuovere indirizzi di agenti, utenti USM e destinazioni trap.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

Vedere "Configurare l'agente SNMP" Per informazioni dettagliate su ciascun campo nella pagina dell'agente SNMP. È necessario selezionare **Salva** nella parte inferiore della pagina per confermare le modifiche apportate in ciascuna scheda.

Fasi

1. Selezionare **CONFIGURATION** > **Monitoring** > **SNMP Agent**.

   Viene visualizzata la pagina SNMP Agent.

2. Per disattivare l'agente SNMP su tutti i nodi della griglia, deselezionare la casella di controllo **attiva SNMP** e selezionare **Salva**.

   Se si riattiva l'agente SNMP, tutte le impostazioni di configurazione SNMP precedenti vengono mantenute.

3. Se si desidera, aggiornare le informazioni nella sezione Configurazione di base:
   a. Se necessario, aggiornare **System contact** e **System location**.
   b. In alternativa, selezionare o deselezionare la casella di controllo **attiva notifiche agente SNMP** per controllare se l'agente SNMP StorageGRID invia notifiche trap e inform.

      Quando questa casella di controllo è deselezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia notifiche SNMP.

   c. Facoltativamente, selezionare o deselezionare la casella di controllo **Abilita trap di autenticazione** per controllare se l'agente SNMP di StorageGRID invia trap di autenticazione quando riceve messaggi di protocollo autenticati in modo errato.
4. Se si utilizza SNMPv1 o SNMPv2c, è possibile aggiornare o aggiungere una comunità **di sola lettura** nella sezione Community Strings (stringhe comunità).
5. Per aggiornare le destinazioni trap, selezionare la scheda destinazioni trap nella sezione altre configurazioni.

   Utilizzare questa scheda per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

   Per informazioni dettagliate su cosa immettere, vedere "Creare destinazioni trap".

   - Facoltativamente, aggiornare o rimuovere la comunità trap predefinita.

Se si rimuove la comunità trap predefinita, è necessario innanzitutto verificare che tutte le destinazioni trap esistenti utilizzino una stringa di comunità personalizzata.

- Per aggiungere una destinazione trap, selezionare **Crea**.
- Per modificare una destinazione trap, selezionare il pulsante di opzione e selezionare **Modifica**.
- Per rimuovere una destinazione trap, selezionare il pulsante di opzione e selezionare **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

6. Per aggiornare gli indirizzi degli agenti, selezionare la scheda indirizzi agente nella sezione altre configurazioni.

   Utilizzare questa scheda per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

   Per informazioni dettagliate su cosa immettere, vedere "Creare gli indirizzi degli agenti".

   - Per aggiungere un indirizzo agente, selezionare **Crea**.
   - Per modificare l'indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Modifica**.
   - Per rimuovere un indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Rimuovi**.
   - Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

7. Per aggiornare gli utenti USM, selezionare la scheda utenti USM nella sezione altre configurazioni.

   Utilizzare questa scheda per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

   Per informazioni dettagliate su cosa immettere, vedere "Creare utenti USM".

   - Per aggiungere un utente USM, selezionare **Crea**.
   - Per modificare un utente USM, selezionare il pulsante di opzione e selezionare **Modifica**.

     Il nome utente di un utente USM esistente non può essere modificato. Se è necessario modificare un nome utente, rimuovere l'utente e crearne uno nuovo.

     > Se si aggiunge o si rimuove l'ID motore autorevole di un utente e tale utente è attualmente selezionato per una destinazione, è necessario modificare o rimuovere la destinazione. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

   - Per rimuovere un utente USM, selezionare il pulsante di opzione e selezionare **Rimuovi**.

     > Se l'utente rimosso è attualmente selezionato per una destinazione trap, è necessario modificare o rimuovere la destinazione. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

   - Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

8. Una volta aggiornata la configurazione dell'agente SNMP, selezionare **Salva**.

Accedere ai file MIB

I file MIB contengono definizioni e informazioni sulle proprietà delle risorse e dei servizi

gestiti per i nodi della griglia. È possibile accedere ai file MIB che definiscono gli oggetti e le notifiche per StorageGRID. Questi file possono essere utili per il monitoraggio della griglia.

Vedere "Utilizzare il monitoraggio SNMP" Per ulteriori informazioni sui file SNMP e MIB.

Accedere ai file MIB

Per accedere ai file MIB, procedere come segue.

Fasi

1. Selezionare **CONFIGURATION** > **Monitoring** > **SNMP Agent**.
2. Nella pagina dell'agente SNMP, selezionare il file che si desidera scaricare:
   - **NETAPP-STORAGEGRID-MIB.txt**: Definisce la tabella degli avvisi e le notifiche (trap) accessibili su tutti i nodi di amministrazione.
   - **ES-NETAPP-06-MIB.mib**: Definisce gli oggetti e le notifiche per le appliance basate su e-Series.
   - **MIB_1_10.zip**: Definisce gli oggetti e le notifiche per le appliance con un'interfaccia BMC.

   > È inoltre possibile accedere ai file MIB nella seguente posizione su qualsiasi nodo StorageGRID: `/usr/share/snmp/mibs`

3. Per estrarre gli OID StorageGRID dal file MIB:

   a. Ottenere l'OID della directory principale del MIB StorageGRID:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Risultato: `.1.3.6.1.4.1.789.28669` (`28669` È sempre l'OID per StorageGRID)

   a. Grep per l'OID di StorageGRID nell'intero albero (usando `paste` per unire le linee):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

> Il `snmptranslate` Command offre molte opzioni utili per esplorare il MIB. Questo comando è disponibile su qualsiasi nodo StorageGRID.

Contenuto del file MIB

Tutti gli oggetti si trovano sotto l'OID StorageGRID.

Nome dell'oggetto	ID oggetto (OID)	Descrizione
iso.org.dod.internet. + private.enterprise. netapp.storagegrid		Il modulo MIB per le entità NetApp StorageGRID.

Oggetti MIB

Nome dell'oggetto	ID oggetto (OID)	Descrizione
ActiveAlertCount	**1.3.6.1.4.1. +** 789.28669.1.3	Il numero di avvisi attivi in activeAlertTable.
ActiveAlertTable	**1.3.6.1.4.1. +** 789.28669.1.4	Tabella degli avvisi attivi in StorageGRID.
ActiveAlertId	**1.3.6.1.4.1. +** 789.28669.1.4.1.1	L'ID dell'avviso. Unico solo nel set corrente di avvisi attivi.
ActiveAlertName	**1.3.6.1.4.1. +** 789.28669.1.4.1.2	Il nome dell'avviso.
ActiveAlertInstance	**1.3.6.1.4.1. +** 789.28669.1.4.1.3	Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
ActiveAlertSeverity	**1.3.6.1.4.1. +** 789.28669.1.4.1.4	La severità dell'avviso.
ActiveAlertStartTime	**1.3.6.1.4.1. +** 789.28669.1.4.1.5	La data e l'ora di attivazione dell'avviso.

Tipi di notifica (trap)

Tutte le notifiche includono le seguenti variabili come varbind:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Tipo di notifica	ID oggetto (OID)	Descrizione
ActiveMinorAlert	**1.3.6.1.4.1. +** 789.28669.0.6	Un avviso con un livello di severità minore
ActiveMajorAlert	**1.3.6.1.4.1. +** 789.28669.0.7	Un avviso con severità maggiore
ActiveCriticalAlert	**1.3.6.1.4.1. +** 789.28669.0.8	Un avviso con severità critica

Raccogliere dati StorageGRID aggiuntivi

Utilizzare grafici e grafici

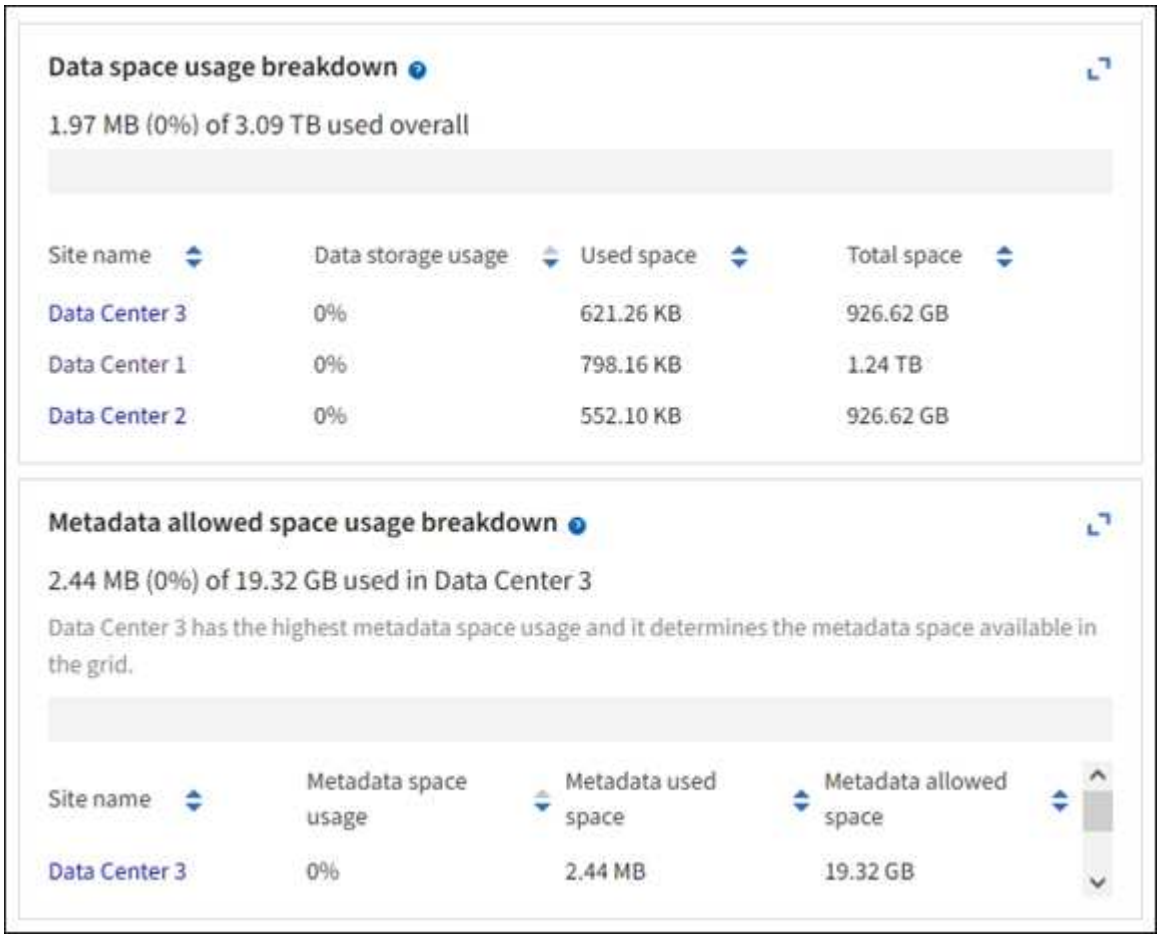
È possibile utilizzare grafici e report per monitorare lo stato del sistema StorageGRID e risolvere i problemi.

> Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere alle schermate di esempio di questa pagina.

Tipi di grafici

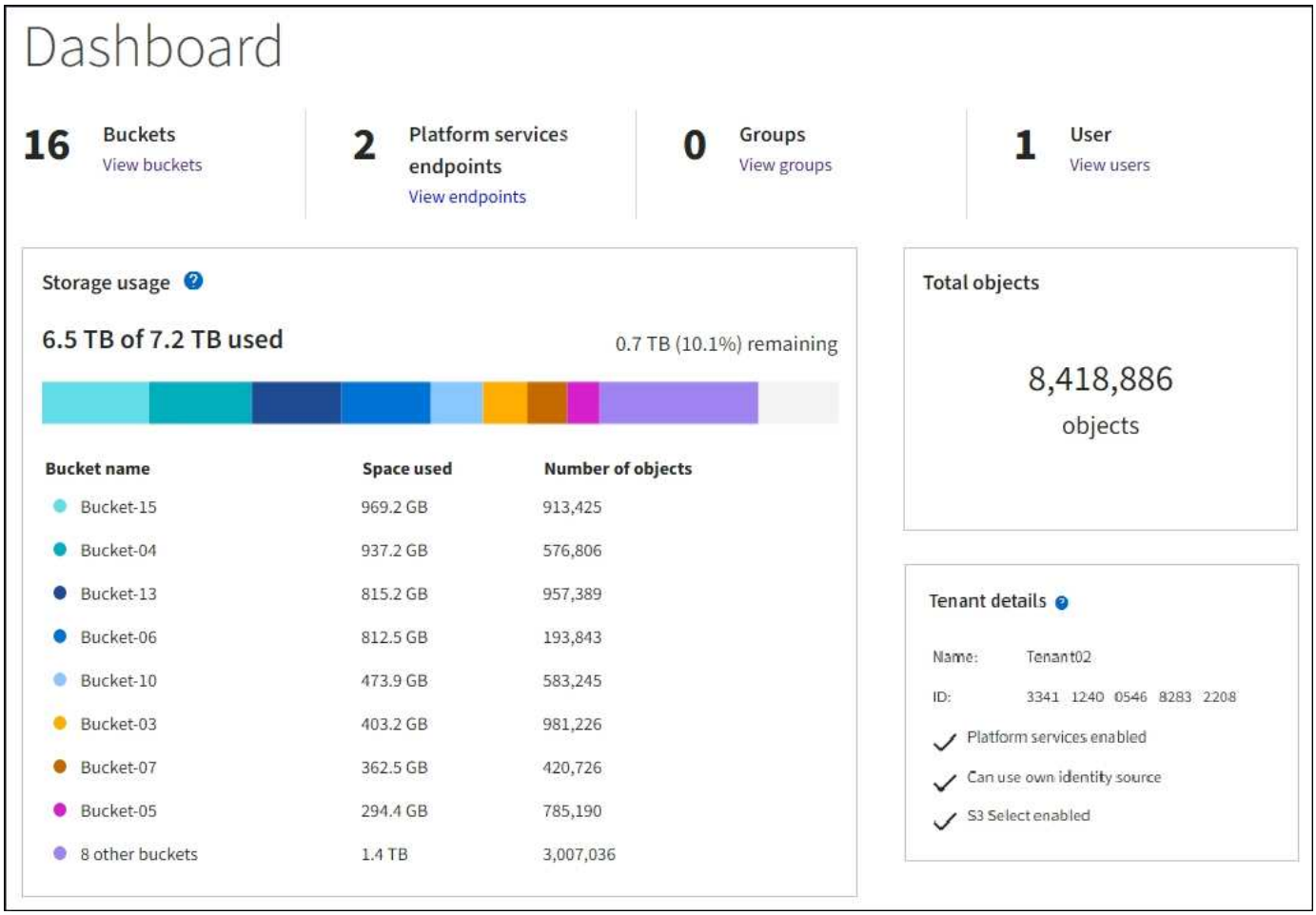
I grafici e i grafici riassumono i valori delle metriche e degli attributi specifici di StorageGRID.

La dashboard di Grid Manager include schede che riepilogano lo storage disponibile per la griglia e per ciascun sito.



Il pannello Storage Use (utilizzo storage) della dashboard di Tenant Manager visualizza quanto segue:

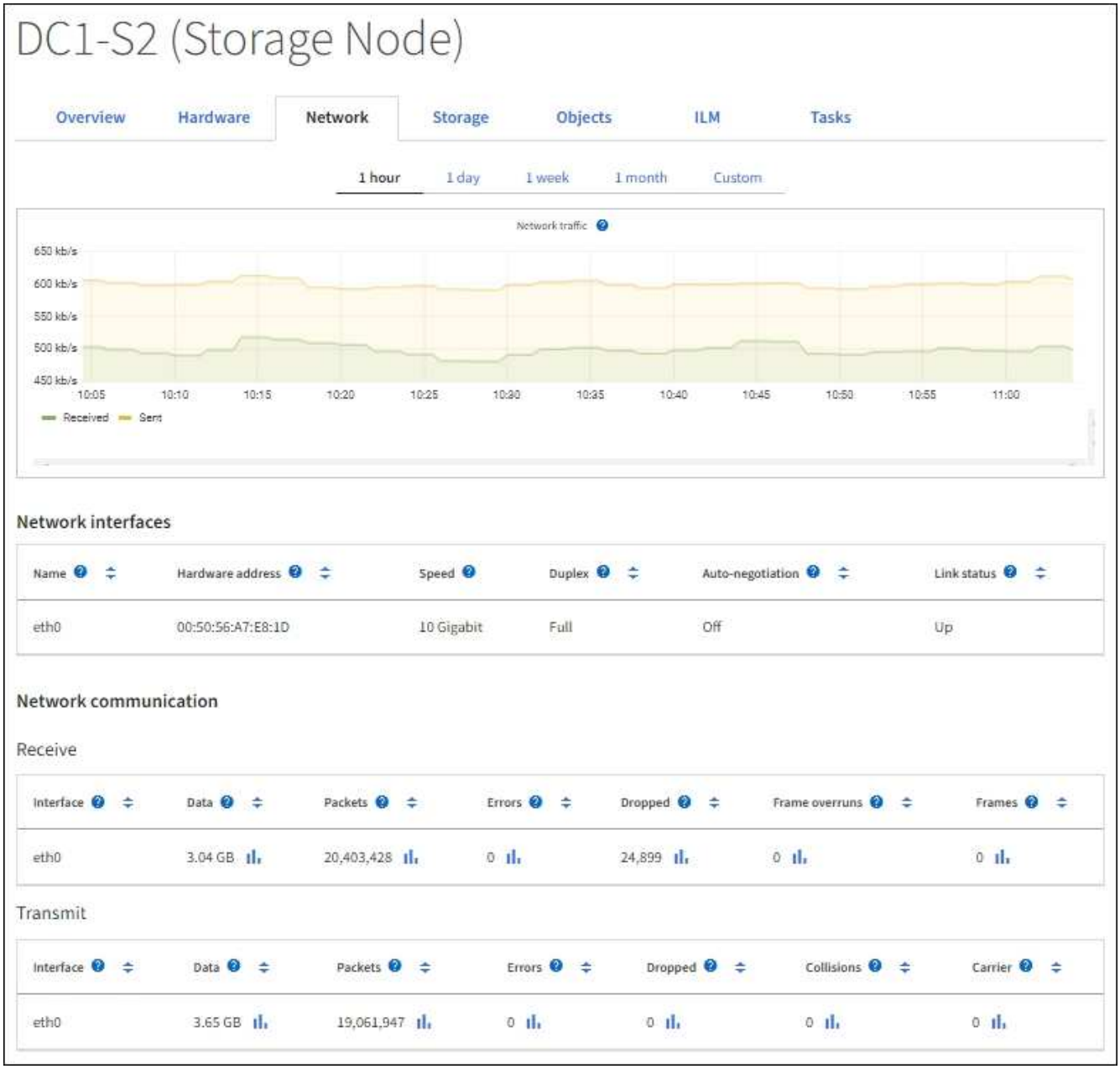
- Un elenco dei bucket più grandi (S3) o container (Swift) per il tenant
- Un grafico a barre che rappresenta le dimensioni relative dei bucket o dei container più grandi
- La quantità totale di spazio utilizzato e, se viene impostata una quota, la quantità e la percentuale di spazio rimanente



Inoltre, i grafici che mostrano come le metriche e gli attributi StorageGRID cambiano nel tempo sono disponibili dalla pagina nodi e dalla pagina **SUPPORTO** > **Strumenti** > **topologia griglia**.

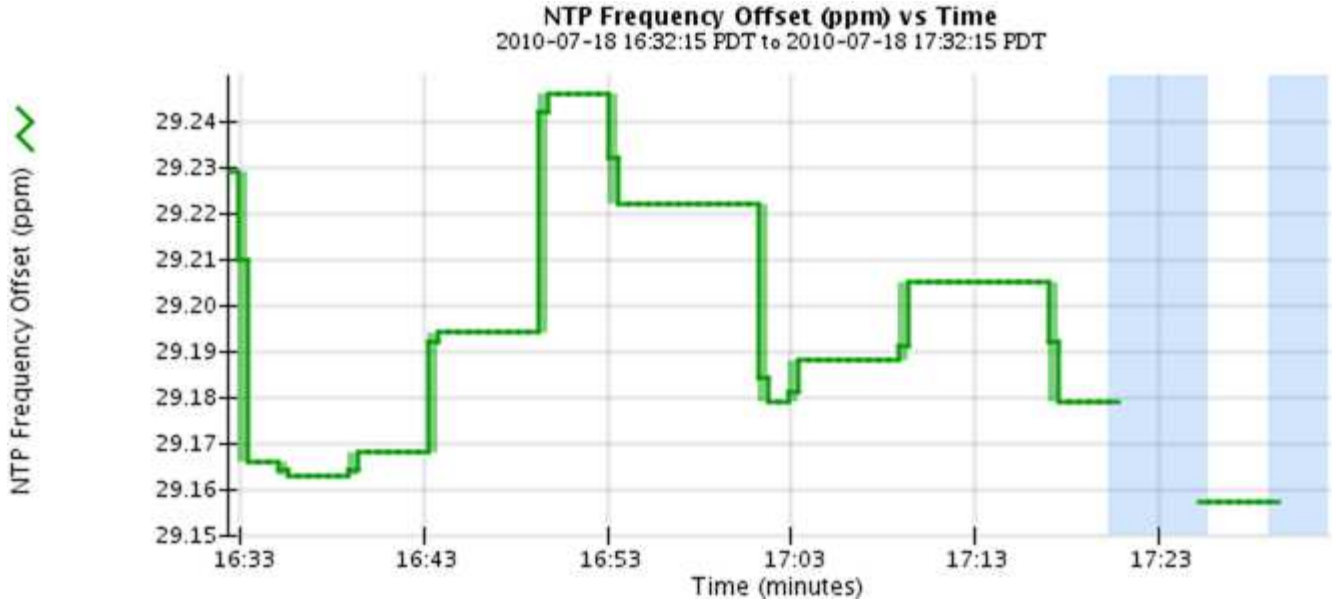
Esistono quattro tipi di grafici:

- **Grafici Grafana**: Mostrati nella pagina dei nodi, i grafici Grafana vengono utilizzati per tracciare i valori delle metriche Prometheus nel tempo. Ad esempio, la scheda **NODI** > **rete** di un nodo di storage include un grafico Grafana per il traffico di rete.

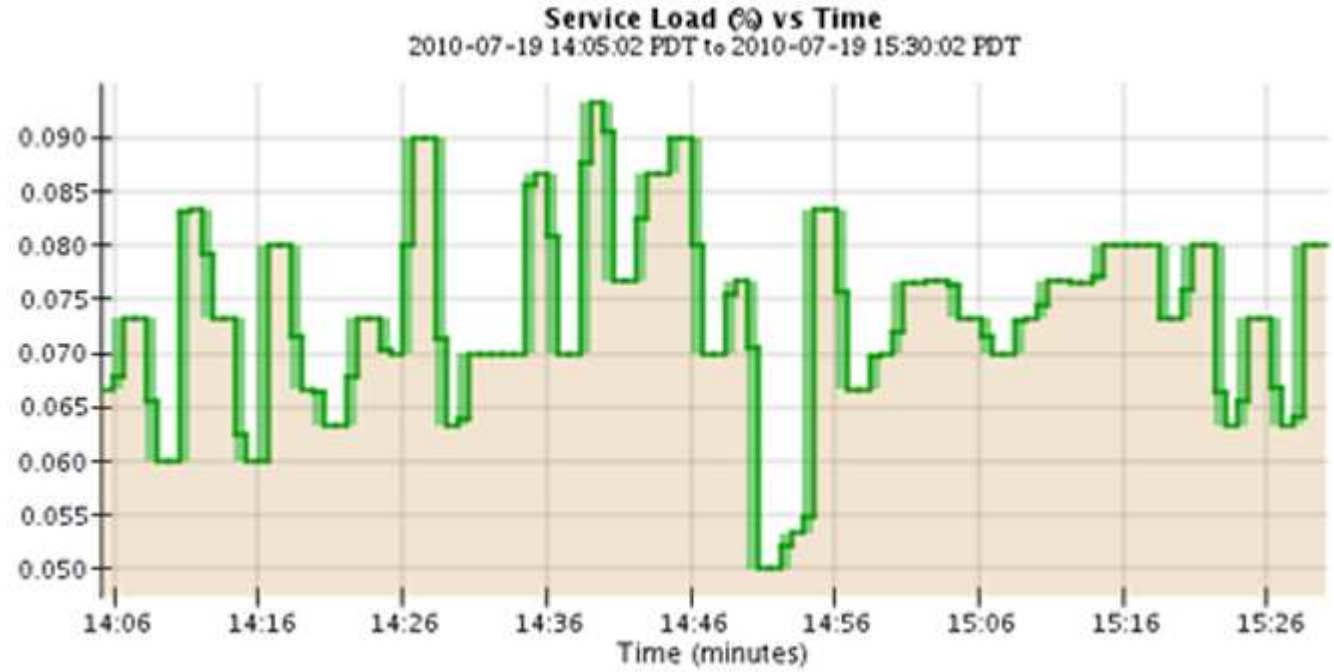


I grafici Grafana sono inclusi anche nelle dashboard predefinite disponibili nella pagina **SUPPORT** > **Tools** > **Metrics**.

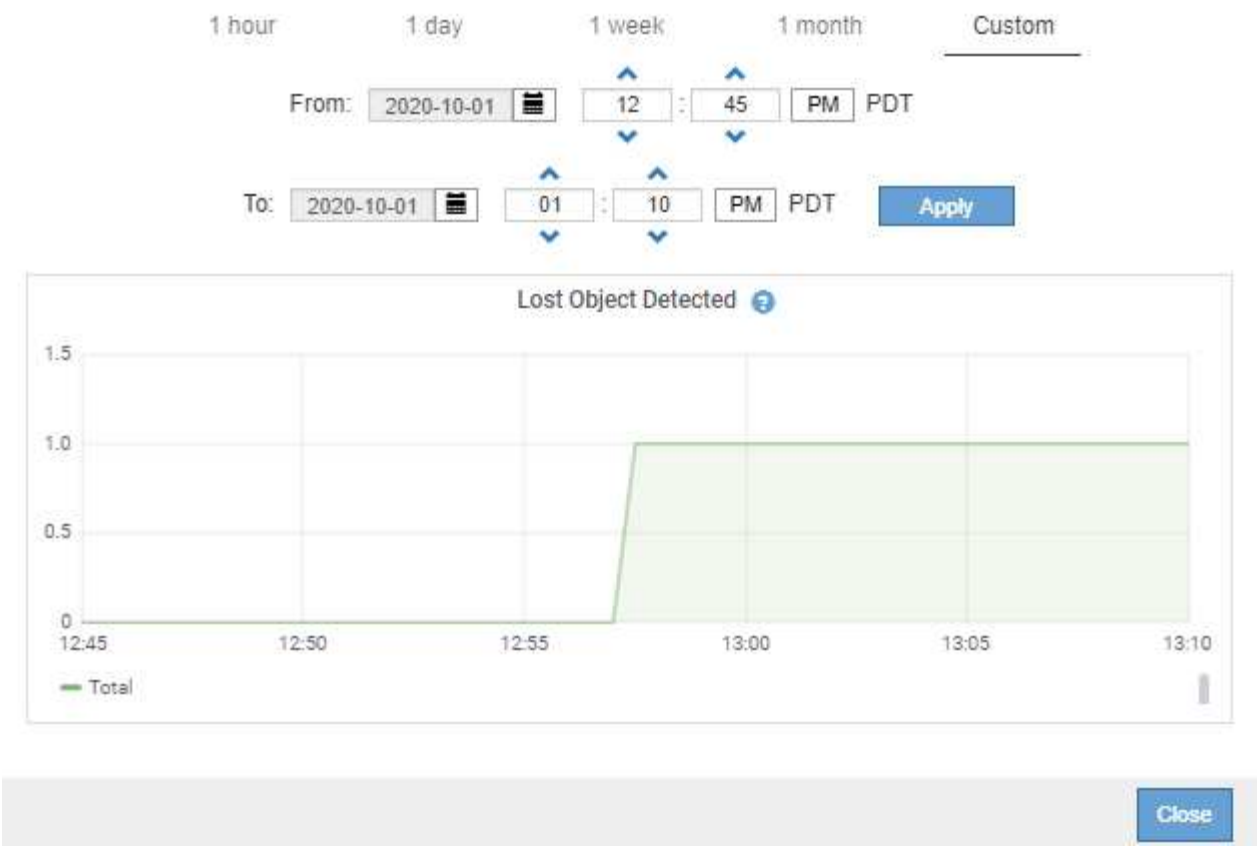
- **Grafici di linea**: Disponibili dalla pagina nodi e dalla pagina **SUPPORTO** > **Strumenti** > **topologia griglia** (selezionare l'icona del grafico) Dopo un valore di dati), i grafici a linee vengono utilizzati per rappresentare graficamente i valori degli attributi StorageGRID che hanno un valore unitario (ad esempio, offset di frequenza NTP, in ppm). Le modifiche al valore vengono tracciate a intervalli di dati regolari (bin) nel tempo.



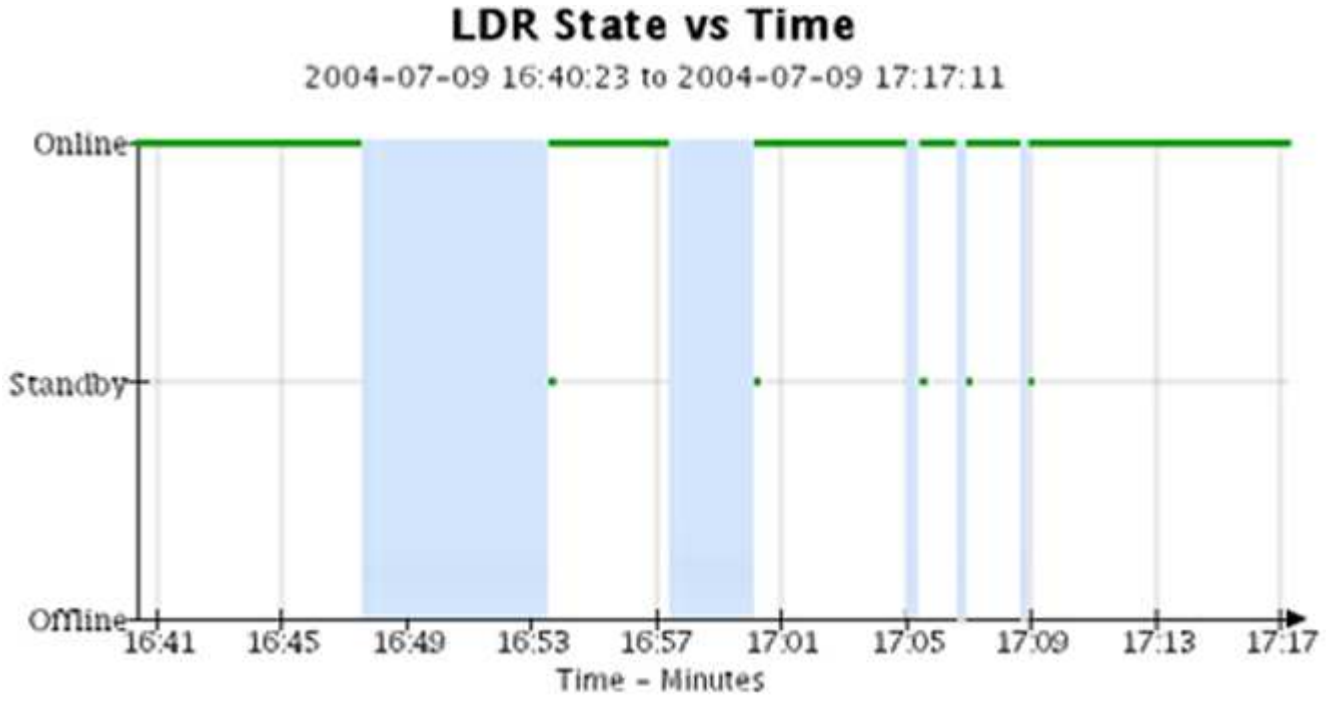
- **Area Graphs**: Disponibile dalla pagina Nodes e dalla pagina **SUPPORT** > **Tools** > **Grid topology** (Seleziona l'icona del grafico) dopo un valore di dati), i grafici di area vengono utilizzati per rappresentare graficamente le quantità di attributi volumetrici, come i conteggi di oggetti o i valori di carico del servizio. I grafici dell'area sono simili ai grafici a linee, ma includono un'ombreggiatura marrone chiaro sotto la linea. Le modifiche al valore vengono tracciate a intervalli di dati regolari (bin) nel tempo.



- Alcuni grafici sono contrassegnati da un diverso tipo di icona del grafico e hanno un formato diverso:



- **State graph**: Disponibile nella pagina **SUPPORT** > **Tools** > **Grid topology** (selezionare l'icona del grafico) dopo un valore di dati), i grafici di stato vengono utilizzati per rappresentare i valori degli attributi che rappresentano stati distinti, ad esempio uno stato del servizio che può essere in linea, in standby o offline. I grafici di stato sono simili ai grafici a linee, ma la transizione è discontinua, ovvero il valore passa da un valore di stato all'altro.



Informazioni correlate

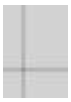
"Visualizzare la pagina nodi"

"Visualizzare l'albero topologia griglia"

"Rivedere le metriche di supporto"

Legenda del grafico

Le linee e i colori utilizzati per disegnare i grafici hanno un significato specifico.

Esempio	Significato
	I valori degli attributi riportati vengono tracciati utilizzando linee di colore verde scuro.
	L'ombreggiatura verde chiaro intorno a linee verdi scure indica che i valori effettivi in quell'intervallo di tempo variano e sono stati "binned" (binning) per una tracciatura più rapida. La linea scura rappresenta la media ponderata. L'intervallo in verde chiaro indica i valori massimi e minimi all'interno del contenitore. L'ombreggiatura marrone chiaro viene utilizzata per i grafici dell'area per indicare i dati volumetrici.
	Le aree vuote (nessun dato plottato) indicano che i valori degli attributi non erano disponibili. Lo sfondo può essere blu, grigio o una combinazione di grigio e blu, a seconda dello stato del servizio che segnala l'attributo.
	L'ombreggiatura blu chiaro indica che alcuni o tutti i valori degli attributi in quel momento erano indeterminati; l'attributo non stava riportando i valori perché il servizio era in uno stato sconosciuto.
	L'ombreggiatura dei grigi indica che alcuni o tutti i valori degli attributi in quel momento non erano noti perché il servizio che riporta gli attributi era amministrativamente inattivo.
	Una combinazione di ombreggiature grigie e blu indica che alcuni dei valori degli attributi all'epoca erano indeterminati (perché il servizio era in uno stato sconosciuto), mentre altri non erano noti perché il servizio che riportava gli attributi era amministrativamente inattivo.

Visualizza grafici e grafici

La pagina Nodes (nodi) contiene i grafici a cui si dovrebbe accedere regolarmente per monitorare attributi come la capacità dello storage e il throughput. In alcuni casi, in particolare quando si lavora con il supporto tecnico, è possibile utilizzare la pagina **SUPPORT** > **Tools** > **Grid topology** per accedere a grafici aggiuntivi.

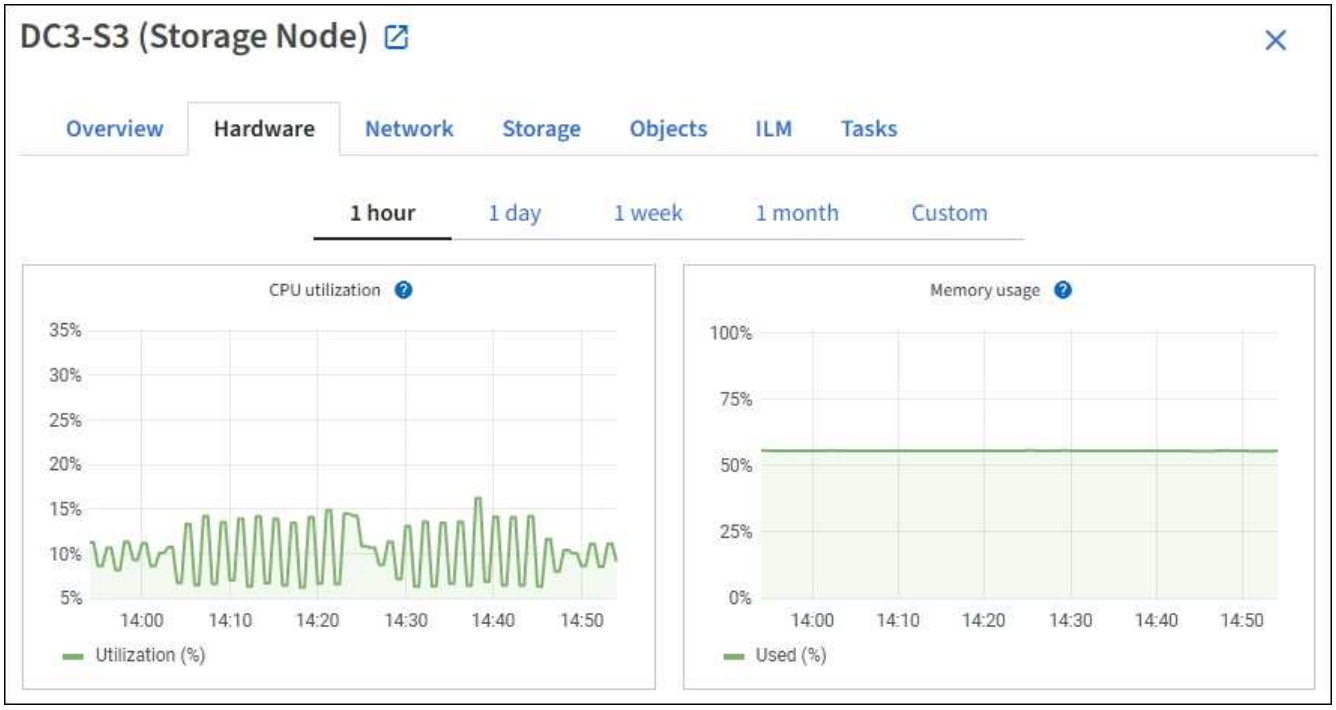
Prima di iniziare

È necessario accedere a Grid Manager utilizzando un "browser web supportato".

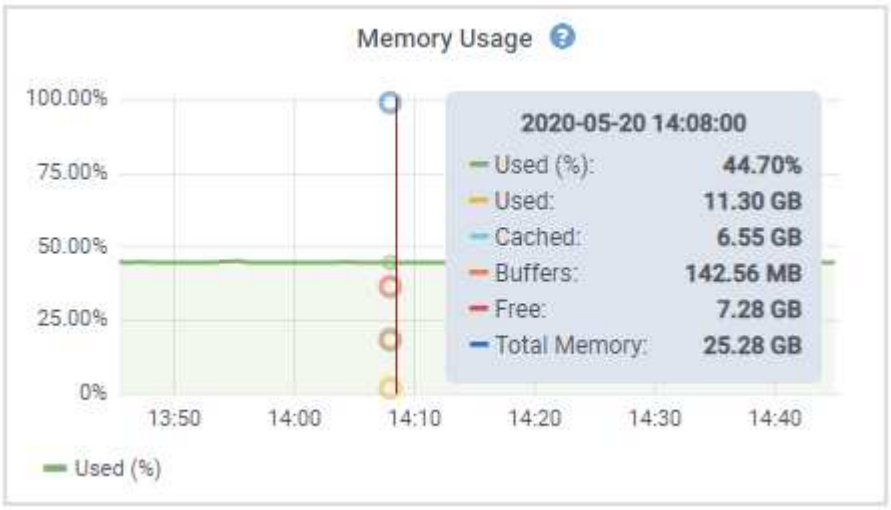
Fasi

1. Selezionare **NODI**. Quindi, selezionare un nodo, un sito o l'intera griglia.
2. Selezionare la scheda per la quale si desidera visualizzare le informazioni.

Alcune schede includono uno o più grafici Grafana, utilizzati per tracciare i valori delle metriche Prometheus nel tempo. Ad esempio, la scheda **NODI** > **hardware** di un nodo include due grafici Grafana.



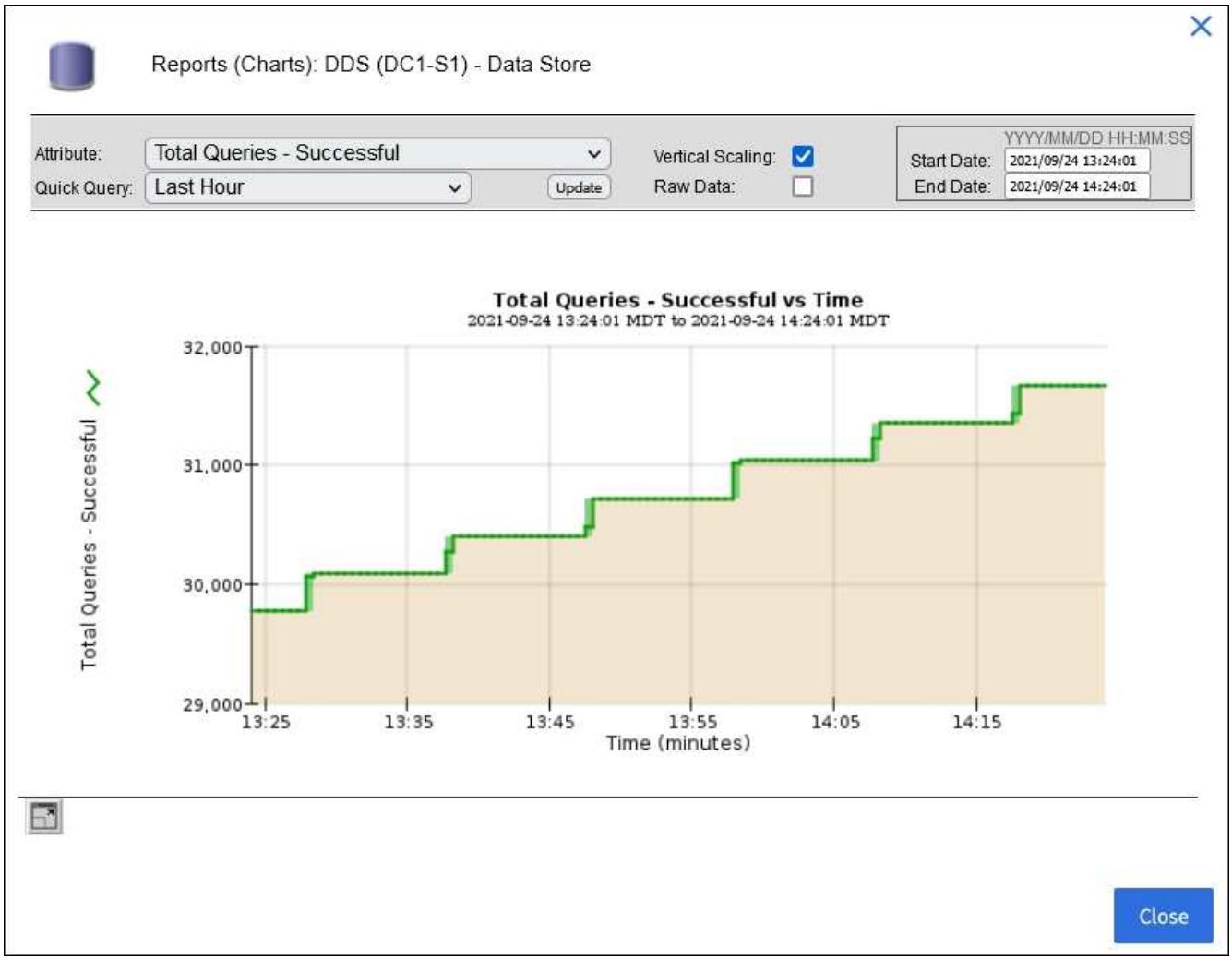
3. Se lo si desidera, posizionare il cursore sul grafico per visualizzare valori più dettagliati per un determinato punto nel tempo.

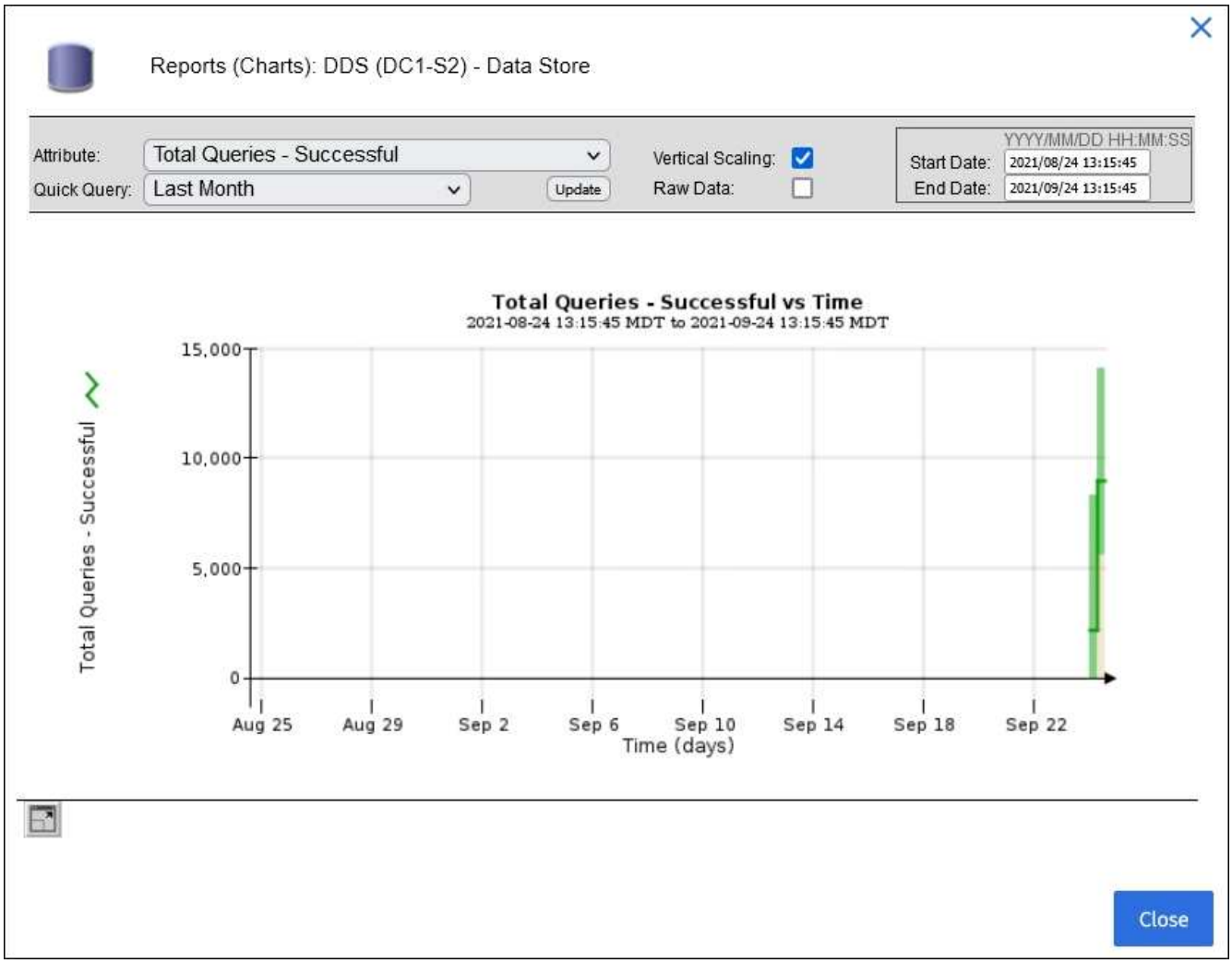


4. In base alle esigenze, spesso è possibile visualizzare un grafico per un attributo o una metrica specifici. Nella tabella della pagina nodi, selezionare l'icona del grafico a destra del nome dell'attributo.

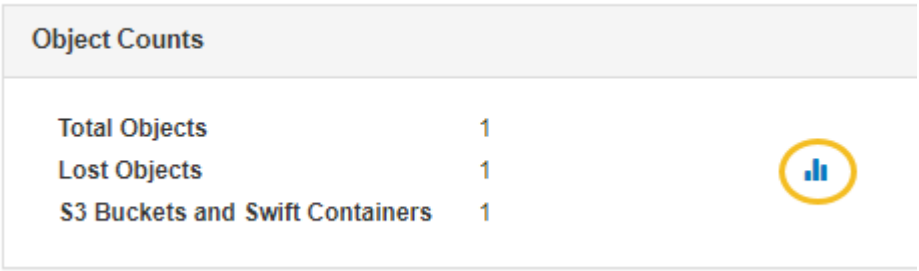
> I grafici non sono disponibili per tutte le metriche e gli attributi.

Esempio 1: Dalla scheda oggetti di un nodo di storage, è possibile selezionare l'icona del grafico Per visualizzare il numero totale di query di archiviazione dei metadati riuscite per il nodo di storage.

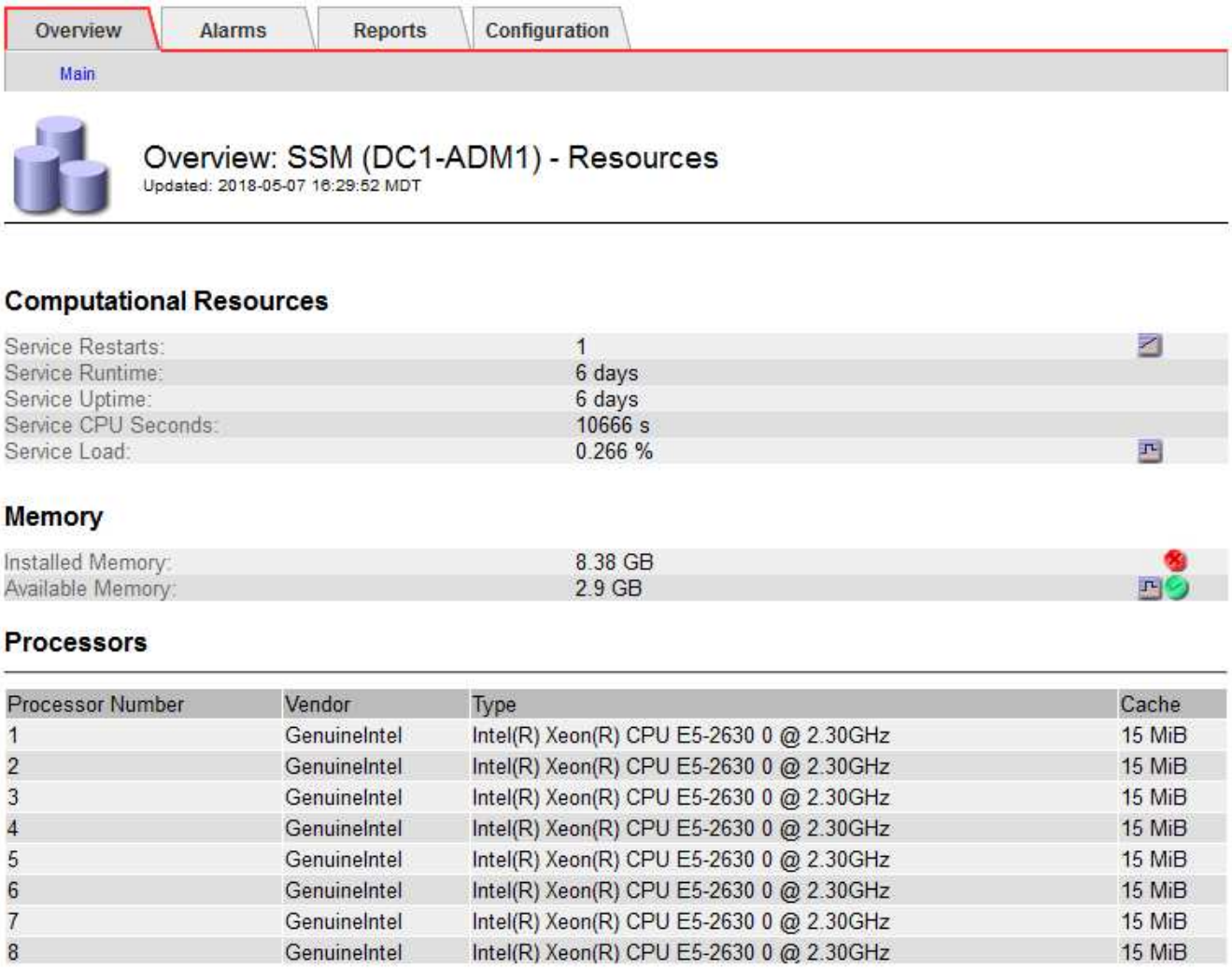

Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close



Esempio 2: Dalla scheda oggetti di un nodo di archiviazione, è possibile selezionare l'icona del grafico Per visualizzare il grafico Grafana del numero di oggetti persi rilevati nel tempo.



5. Per visualizzare i grafici degli attributi non visualizzati nella pagina nodo, selezionare **SUPPORT** > **Tools** > **Grid topology**.
6. Selezionare ***grid node*** > ***component or service*** > **Overview** > **Main**.



7. Selezionare l'icona del grafico accanto all'attributo.

   Il display passa automaticamente alla pagina **Report** > **grafici**. Il grafico visualizza i dati dell'attributo nel giorno passato.

Generare grafici

I grafici visualizzano una rappresentazione grafica dei valori dei dati degli attributi. È possibile creare report su un sito del data center, un nodo grid, un componente o un servizio.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***grid node*** > ***component or service*** > **Report** > **grafici**.
3. Selezionare l'attributo da segnalare dall'elenco a discesa **attributo**.
4. Per forzare l'inizio dell'asse Y a zero, deselezionare la casella di controllo **Vertical Scaling** (Scala verticale).

5. Per visualizzare i valori con la massima precisione, selezionare la casella di controllo **dati non elaborati** oppure per arrotondare i valori a un massimo di tre cifre decimali (ad esempio, per gli attributi riportati come percentuali), deselezionare la casella di controllo **dati non elaborati**.
6. Selezionare il periodo di tempo per il quale si desidera creare un report dall'elenco a discesa **Query rapida**.

   Selezionare l'opzione Custom Query (Query personalizzata) per selezionare un intervallo di tempo specifico.

   Il grafico viene visualizzato dopo alcuni istanti. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi.

7. Se si seleziona Custom Query (Query personalizzata), personalizzare il periodo di tempo per il grafico inserendo **Data di inizio** e **Data di fine**.

   Utilizzare il formato *YYYY/MM/DDHH:MM:SS* in ora locale. Gli zeri iniziali devono corrispondere al formato. Ad esempio, 2017/4/6 7:30:00 non supera la convalida. Il formato corretto è: 2017/04/06 07:30:00.

8. Selezionare **Aggiorna**.

   Dopo alcuni secondi viene generato un grafico. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi. A seconda del periodo di tempo impostato per la query, viene visualizzato un report di testo raw o aggregato.

Utilizzare report di testo

I report di testo visualizzano una rappresentazione testuale dei valori dei dati degli attributi elaborati dal servizio NMS. Esistono due tipi di report generati in base al periodo di tempo in cui si esegue il reporting: Report di testo raw per periodi inferiori a una settimana e report di testo aggregati per periodi superiori a una settimana.

Report di testo raw

Un report di testo raw visualizza i dettagli relativi all'attributo selezionato:

- Time Received (ora ricezione): Data e ora locali in cui un valore di esempio dei dati di un attributo è stato elaborato dal servizio NMS.
- Sample Time (ora campione): Data e ora locali in cui un valore di attributo è stato campionato o modificato all'origine.
- Value (valore): Valore dell'attributo al momento del campionamento.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Aggregare report di testo

Un report di testo aggregato visualizza i dati in un periodo di tempo più lungo (di solito una settimana) rispetto a un report di testo raw. Ciascuna voce è il risultato di un riepilogo di più valori di attributo (un aggregato di valori di attributo) da parte del servizio NMS nel tempo in una singola voce con valori medi, massimi e minimi derivati dall'aggregazione.

Ciascuna voce visualizza le seguenti informazioni:

- Aggregate time (ora aggregata): L'ultima data e ora locale in cui il servizio NMS ha aggregato (raccolto) un insieme di valori di attributo modificati.
- Average value (valore medio): La media del valore dell'attributo nel periodo di tempo aggregato.
- Minimum Value (valore minimo): Il valore minimo nel periodo di tempo aggregato.
- Maximum Value (valore massimo): Il valore massimo nel periodo di tempo aggregato.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Generare report di testo

I report di testo visualizzano una rappresentazione testuale dei valori dei dati degli attributi elaborati dal servizio NMS. È possibile creare report su un sito del data center, un nodo grid, un componente o un servizio.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Per i dati degli attributi che si prevede siano in continuo cambiamento, questi dati degli attributi vengono campionati dal servizio NMS (all'origine) a intervalli regolari. Per i dati degli attributi che cambiano di rado (ad esempio, dati basati su eventi come cambiamenti di stato o stato), un valore di attributo viene inviato al servizio NMS quando il valore cambia.

Il tipo di report visualizzato dipende dal periodo di tempo configurato. Per impostazione predefinita, i report di testo aggregati vengono generati per periodi di tempo superiori a una settimana.

Il testo grigio indica che il servizio è stato amministrativamente inattivo durante il campionamento. Il testo blu indica che il servizio si trova in uno stato sconosciuto.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***grid node*** > ***component o service*** > **Report** > **testo**.
3. Selezionare l'attributo da segnalare dall'elenco a discesa **attributo**.
4. Selezionare il numero di risultati per pagina dall'elenco a discesa **risultati per pagina**.
5. Per arrotondare i valori a un massimo di tre cifre decimali (ad esempio, per gli attributi riportati come percentuali), deselezionare la casella di controllo **dati non elaborati**.
6. Selezionare il periodo di tempo per il quale si desidera creare un report dall'elenco a discesa **Query rapida**.

   Selezionare l'opzione Custom Query (Query personalizzata) per selezionare un intervallo di tempo specifico.

Il report viene visualizzato dopo alcuni istanti. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi.

7. Se si seleziona Custom Query (Query personalizzata), è necessario personalizzare il periodo di tempo per il quale si desidera creare un report inserendo **Data di inizio** e **Data di fine**.

   Utilizzare il formato `YYYY/MM/DDHH:MM:SS` in ora locale. Gli zeri iniziali devono corrispondere al formato. Ad esempio, 2017/4/6 7:30:00 non supera la convalida. Il formato corretto è: 2017/04/06 07:30:00.

8. Fare clic su **Aggiorna**.

   Dopo alcuni istanti viene generato un report di testo. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi. A seconda del periodo di tempo impostato per la query, viene visualizzato un report di testo raw o aggregato.

Esportare report di testo

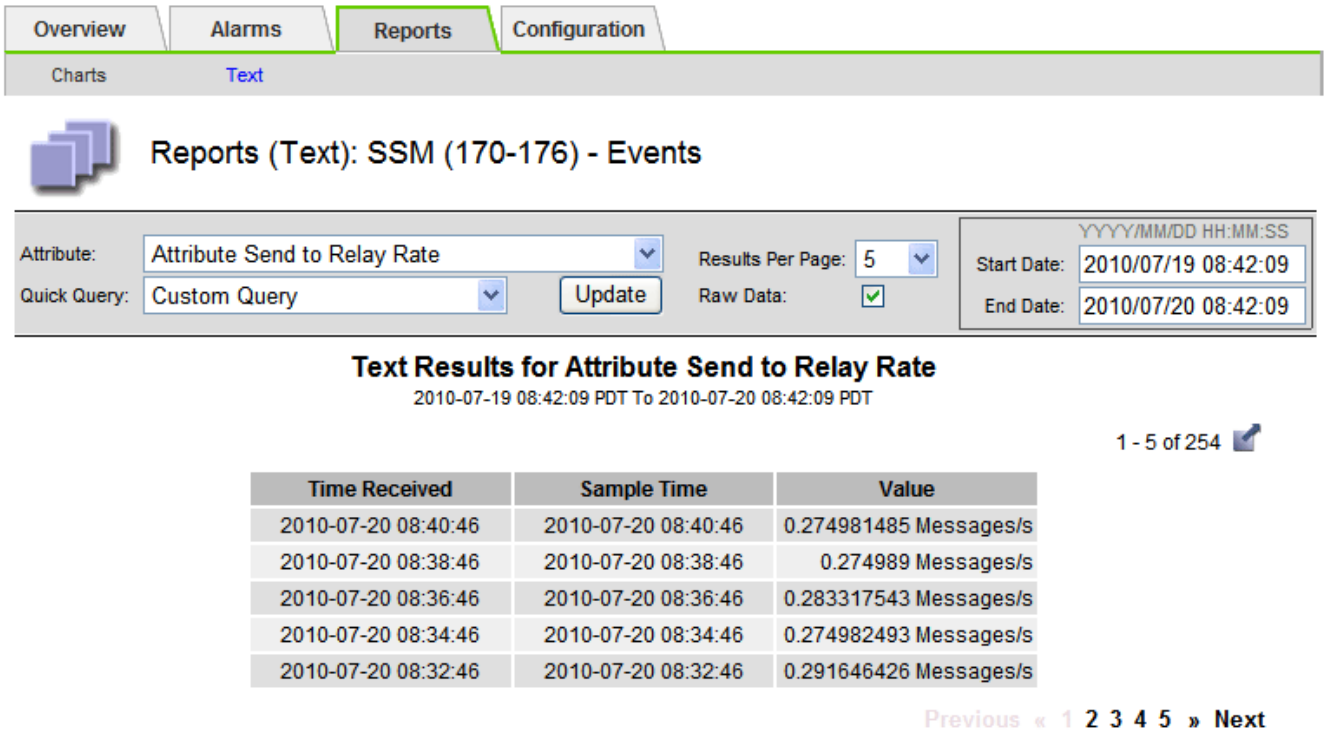
I report di testo esportati aprono una nuova scheda del browser che consente di selezionare e copiare i dati.

A proposito di questa attività

I dati copiati possono quindi essere salvati in un nuovo documento (ad esempio, un foglio di calcolo) e utilizzati per analizzare le prestazioni del sistema StorageGRID.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Creare un report di testo.
3. Fare clic su *Esporta*.



Viene visualizzata la finestra Export Text Report (Esporta report di testo) che visualizza il report.

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. Selezionare e copiare il contenuto della finestra Esporta report di testo.

   Questi dati possono ora essere incollati in un documento di terze parti, ad esempio un foglio di calcolo.

Monitorare L'EFFICIENZA e OTTENERE le performance

È possibile monitorare le performance di alcune operazioni, come ad esempio l'archiviazione e il recupero di oggetti, per identificare le modifiche che potrebbero richiedere ulteriori analisi.

A proposito di questa attività

Per monitorare LE performance, puoi eseguire i comandi S3 e Swift direttamente da una workstation o utilizzando l'applicazione open-source S3tester. L'utilizzo di questi metodi consente di valutare le performance indipendentemente da fattori esterni a StorageGRID, come problemi con un'applicazione client o problemi con una rete esterna.

Quando si eseguono i test delle operazioni PUT e GET, attenersi alle seguenti linee guida:

- Utilizzare dimensioni degli oggetti paragonabili agli oggetti che di solito si acquisiscono nella griglia.
- Eseguire operazioni su siti locali e remoti.

Messaggi in "log di audit" indicare il tempo totale necessario per eseguire determinate operazioni. Ad esempio, per determinare il tempo di elaborazione totale per una richiesta S3 GET, è possibile esaminare il valore dell'attributo TIME nel messaggio di audit SGET. È inoltre possibile trovare l'attributo TIME nei messaggi di audit per le seguenti operazioni:

- **S3**: DELETE, GET, HEAD, Metadata Updated, POST, IN PRIMO PIANO
- **SWIFT**: ELIMINA, OTTIENI, TESTA, METTI

Durante l'analisi dei risultati, esaminare il tempo medio richiesto per soddisfare una richiesta e il throughput complessivo che è possibile ottenere. Ripetere regolarmente gli stessi test e registrare i risultati, in modo da

poter identificare i trend che potrebbero richiedere un'indagine.

- È possibile "Scarica S3tester da github".

Monitorare le operazioni di verifica degli oggetti

Il sistema StorageGRID è in grado di verificare l'integrità dei dati degli oggetti sui nodi di storage, verificando la presenza di oggetti danneggiati e mancanti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".

A proposito di questa attività

Due "processi di verifica" lavorare insieme per garantire l'integrità dei dati:

- **La verifica in background** viene eseguita automaticamente, controllando continuamente la correttezza dei dati dell'oggetto.

  La verifica in background verifica automaticamente e continuamente tutti i nodi di storage per determinare se sono presenti copie corrotte dei dati degli oggetti replicati e codificati in cancellazione. In caso di problemi, il sistema StorageGRID tenta automaticamente di sostituire i dati dell'oggetto corrotto da copie memorizzate in un'altra parte del sistema. La verifica in background non viene eseguita sui nodi di archiviazione o sugli oggetti in un pool di storage cloud.

  > L'avviso **rilevato oggetto corrotto non identificato** viene attivato se il sistema rileva un oggetto corrotto che non può essere corretto automaticamente.

- **Il controllo dell'esistenza di oggetti** può essere attivato da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) dei dati dell'oggetto.

  Il controllo dell'esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti con codifica di cancellazione sono presenti in un nodo di storage. Il controllo dell'esistenza degli oggetti consente di verificare l'integrità dei dispositivi di storage, in particolare se un recente problema hardware potrebbe aver influenzato l'integrità dei dati.

È necessario esaminare regolarmente i risultati delle verifiche in background e dei controlli sull'esistenza degli oggetti. Esaminare immediatamente eventuali istanze di dati degli oggetti corrotti o mancanti per determinare la causa principale.

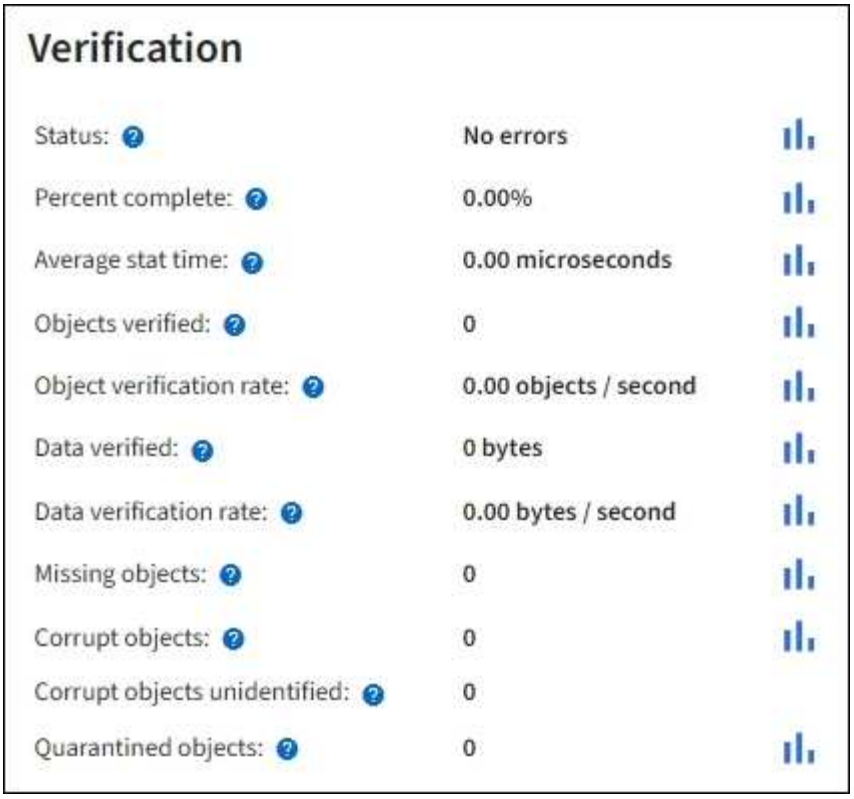
Fasi

1. Esaminare i risultati delle verifiche in background:

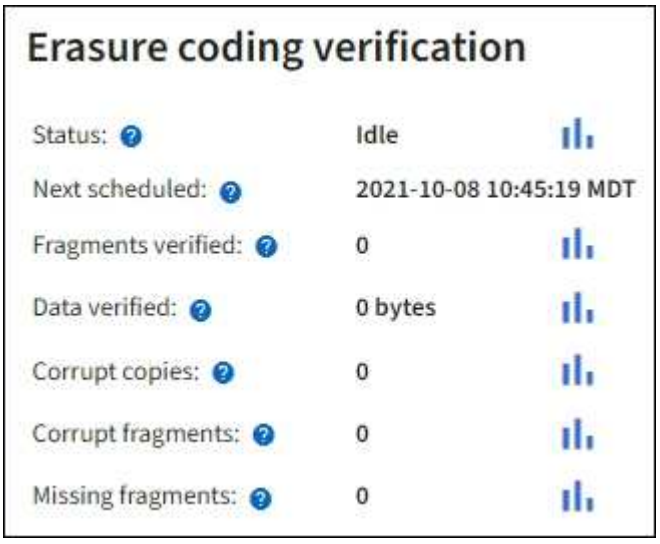
   a. Selezionare **NODI** > ***nodo di storage*** > **oggetti**.

   b. Verificare i risultati della verifica:

      - Per controllare la verifica dei dati degli oggetti replicati, esaminare gli attributi nella sezione verifica.

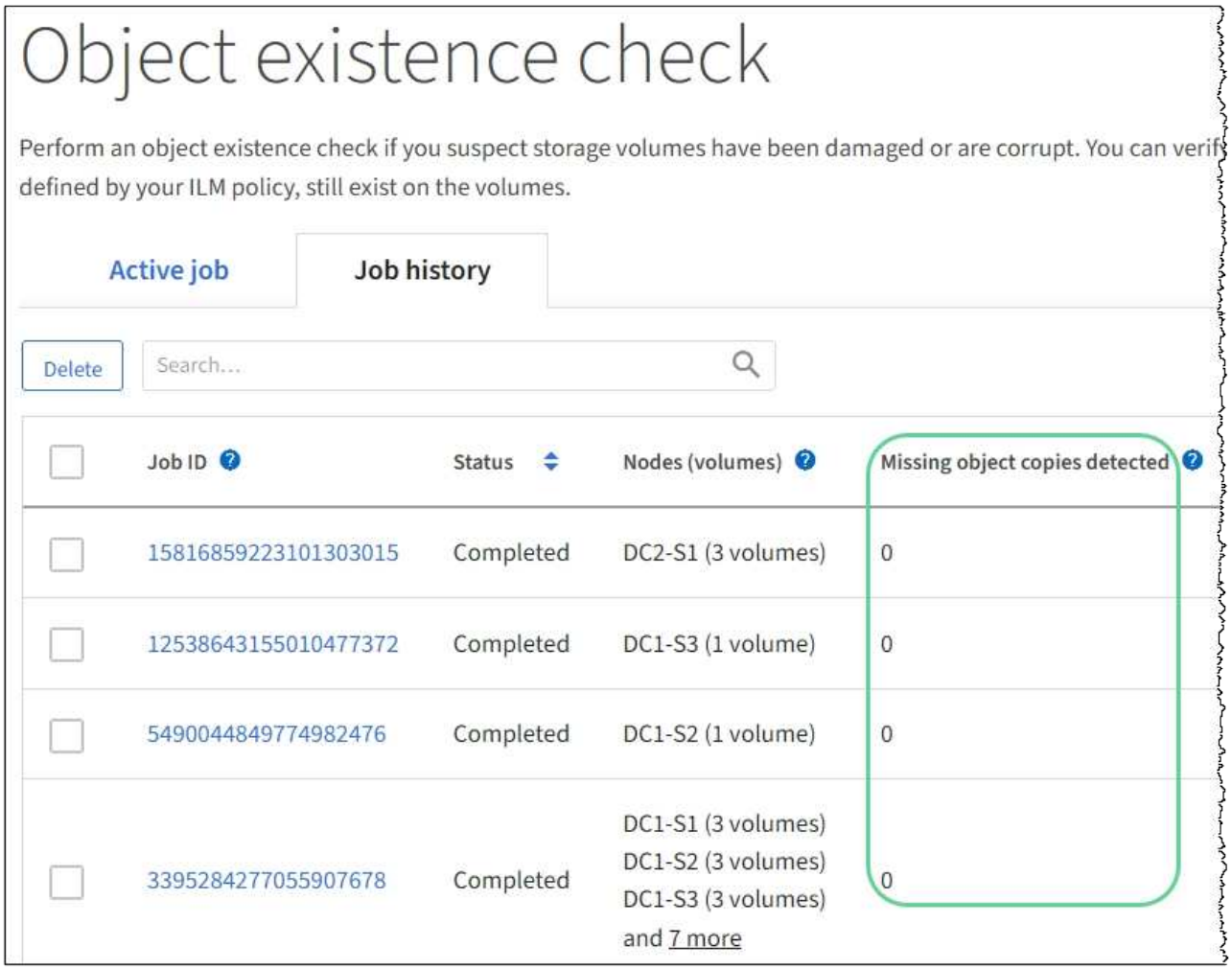


- Per controllare la verifica dei frammenti con codifica di cancellazione, selezionare ***Storage Node*** > **ILM** e controllare gli attributi nella sezione Erasure coding verifcation.



Selezionare il punto interrogativo accanto al nome di un attributo per visualizzare il testo della guida.

2. Esaminare i risultati dei job di controllo dell'esistenza di oggetti:
   a. Selezionare **MANUTENZIONE** > **verifica dell'esistenza dell'oggetto** > **Cronologia lavori**.
   b. Eseguire la scansione della colonna copie oggetto mancanti rilevate. Se un lavoro ha causato 100 o più copie di oggetti mancanti e l'avviso **oggetti persi** è stato attivato, contattare il supporto tecnico.



Monitorare gli eventi

È possibile monitorare gli eventi rilevati da un nodo grid, inclusi gli eventi personalizzati creati per tenere traccia degli eventi registrati nel server syslog. Il messaggio Last Event (ultimo evento) visualizzato in Grid Manager fornisce ulteriori informazioni sull'evento più recente.

I messaggi degli eventi sono elencati anche in `/var/local/log/bycast-err.log` file di log. Vedere "Riferimenti ai file di log".

L'allarme SMTT (Total events) può essere ripetutamente attivato da problemi come problemi di rete, interruzioni di corrente o aggiornamenti. Questa sezione contiene informazioni sull'analisi degli eventi, in modo da comprendere meglio il motivo per cui si sono verificati questi allarmi. Se un evento si è verificato a causa di un problema noto, è possibile ripristinare i contatori degli eventi in tutta sicurezza.

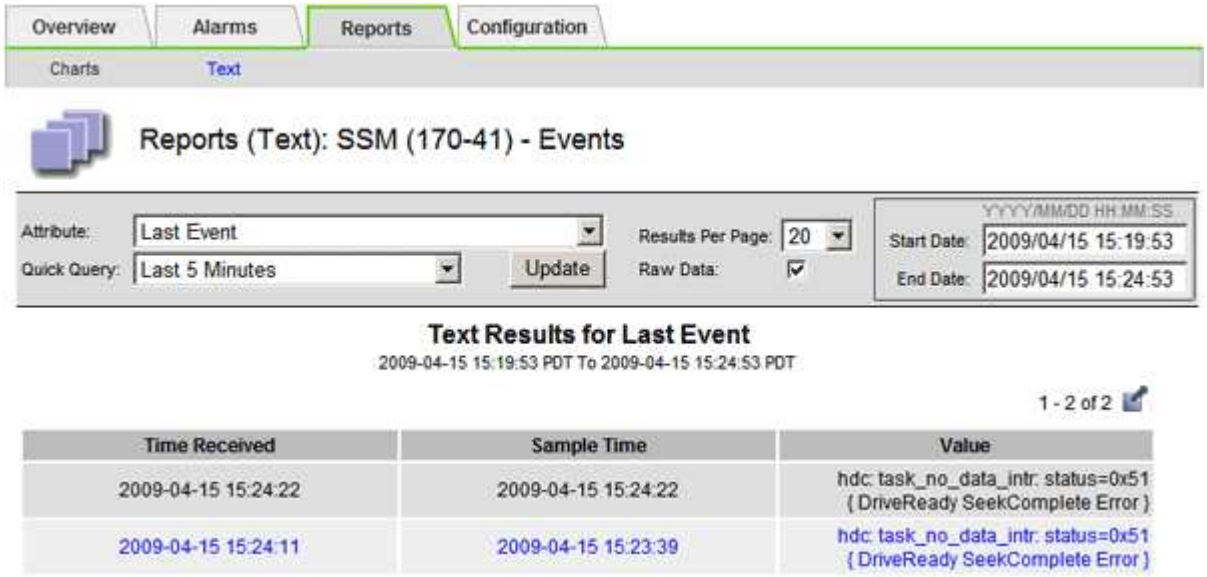
Fasi

1. Esaminare gli eventi di sistema per ciascun nodo della griglia:
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***site*** > ***grid node*** > **SSM** > **Eventi** > **Panoramica** > **principale**.
2. Genera un elenco di messaggi di eventi precedenti per isolare i problemi verificatisi in passato:

a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
b. Selezionare ***site*** > ***grid node*** > **SSM** > **Eventi** > **Report**.
c. Selezionare **testo**.

   L'attributo **Last Event** non viene visualizzato in "vista dei grafici". Per visualizzarlo:

d. Modificare **attributo** in **ultimo evento**.
e. Facoltativamente, selezionare un periodo di tempo per **Query rapida**.
f. Selezionare **Aggiorna**.



Creare eventi syslog personalizzati

Gli eventi personalizzati consentono di tenere traccia di tutti gli eventi utente di kernel, daemon, errori e livello critico registrati sul server syslog. Un evento personalizzato può essere utile per monitorare l'occorrenza dei messaggi del registro di sistema (e quindi gli eventi di sicurezza della rete e gli errori hardware).

A proposito di questa attività

Prendere in considerazione la creazione di eventi personalizzati per monitorare i problemi ricorrenti. Le seguenti considerazioni si applicano agli eventi personalizzati.

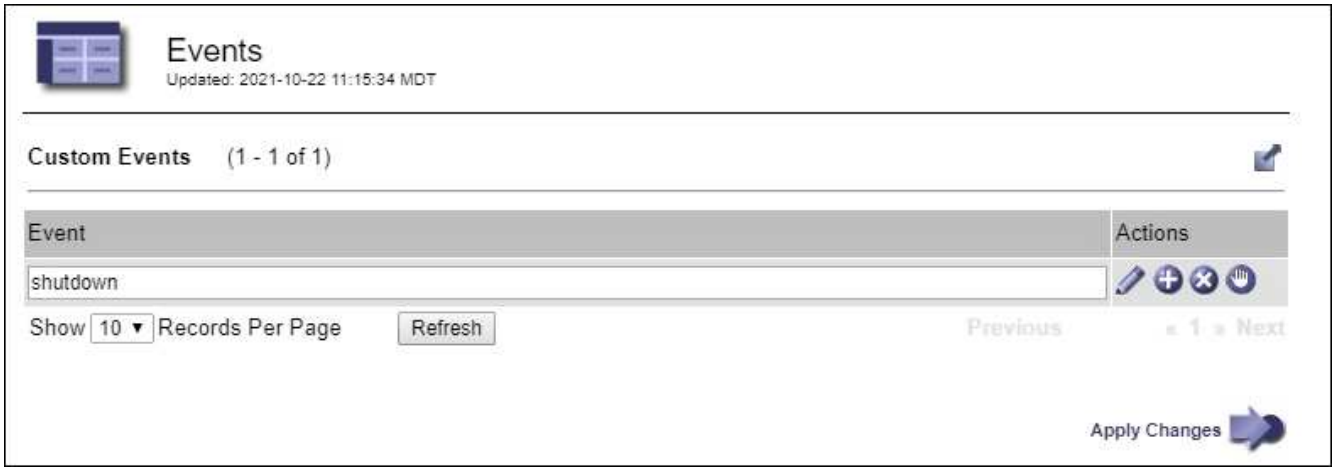
- Dopo la creazione di un evento personalizzato, viene monitorata ogni occorrenza.
- Per creare un evento personalizzato in base alle parole chiave in `/var/local/log/messages` i log in questi file devono essere:
  - Generato dal kernel
  - Generato da daemon o programma utente a livello di errore o critico

Nota: non tutte le voci in `/var/local/log/messages` i file verranno abbinati a meno che non soddisfino i requisiti indicati in precedenza.

Fasi

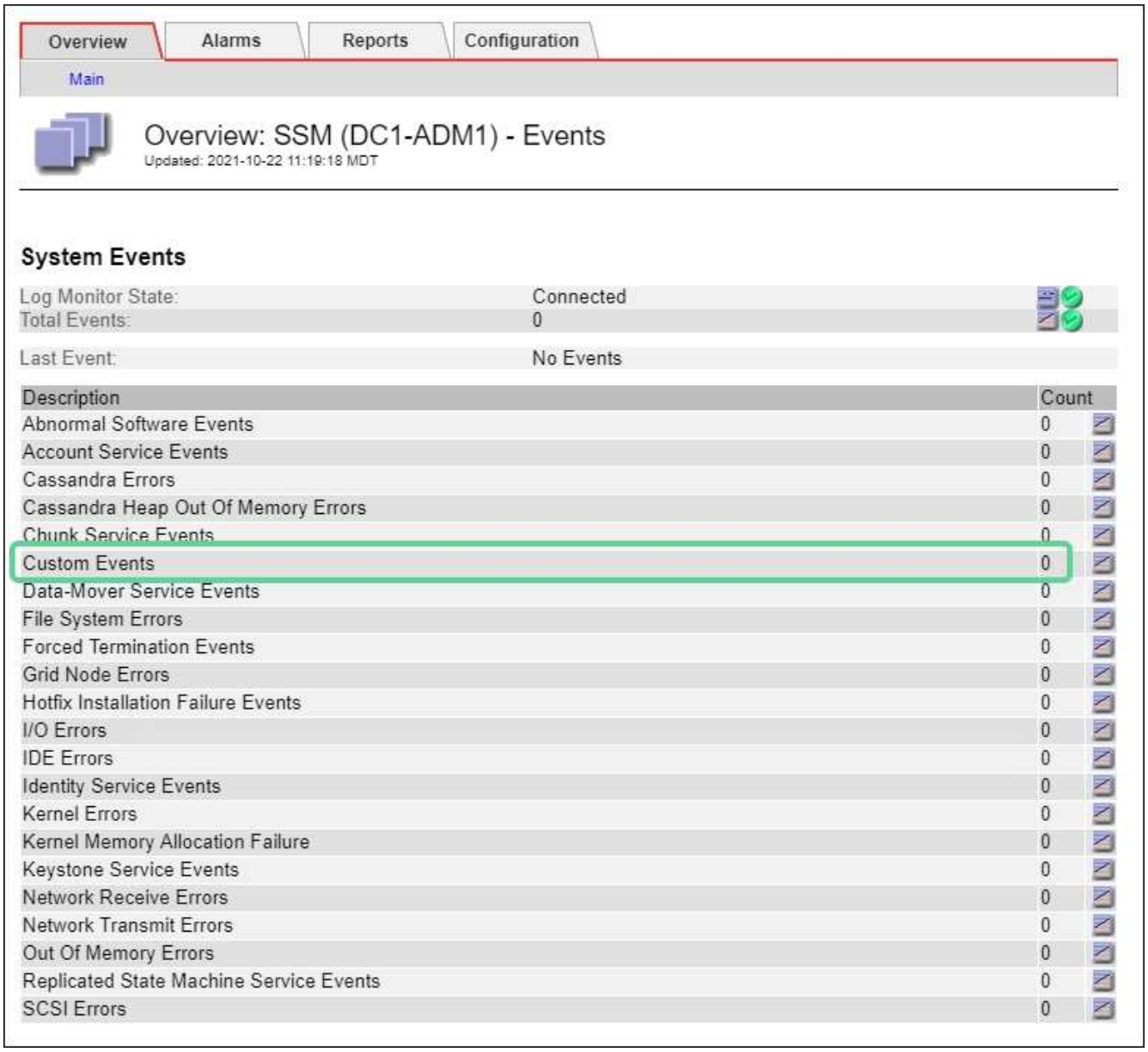
1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Eventi personalizzati**.
2. Fare clic su **Edit** (Modifica) (O **Inserisci** se questo non è il primo evento).

3. Inserire una stringa di eventi personalizzata, ad esempio shutdown



4. Selezionare **Applica modifiche**.
5. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
6. Selezionare ***grid node*** > **SSM** > **Events**.
7. Individuare la voce per gli eventi personalizzati nella tabella Eventi e monitorare il valore per **Conteggio**.

   Se il numero aumenta, viene attivato un evento personalizzato monitorato su quel nodo della griglia.



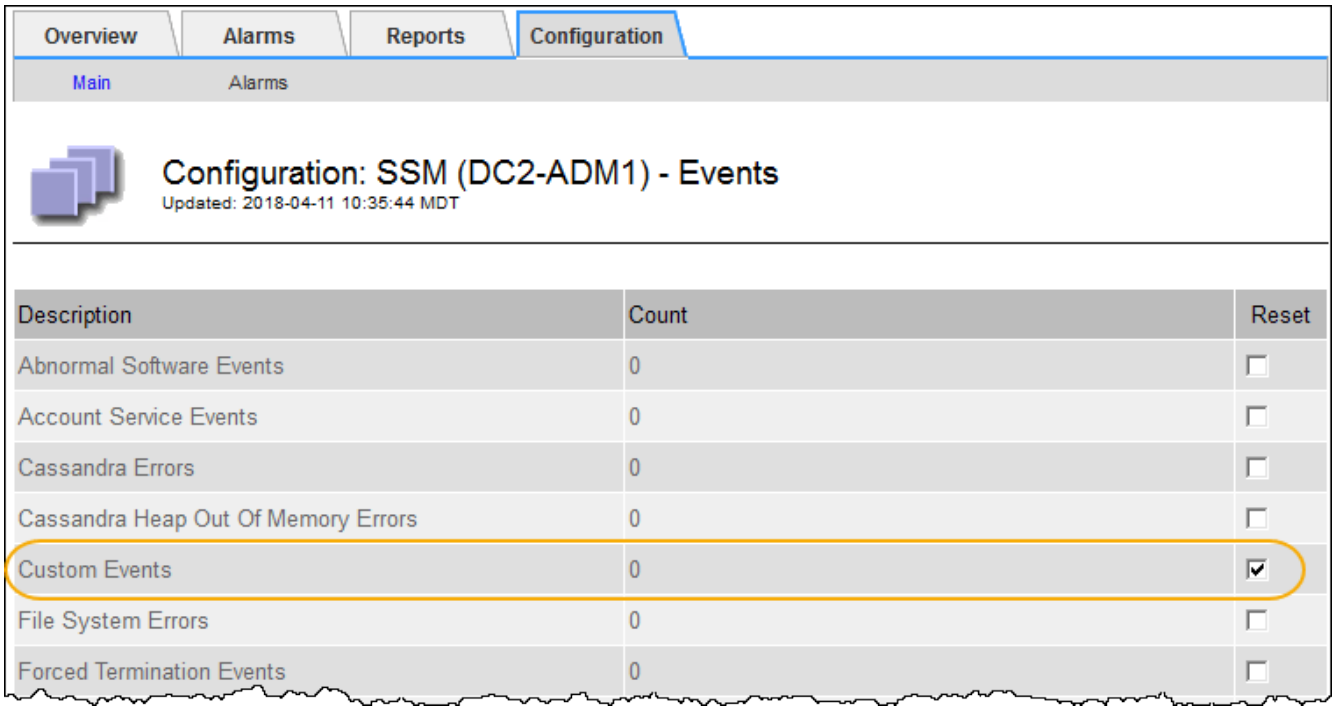
Azzerare il numero di eventi personalizzati

Se si desidera reimpostare il contatore solo per eventi personalizzati, è necessario utilizzare la pagina Grid Topology (topologia griglia) nel menu Support (supporto).

La reimpostazione di un contatore provoca l'attivazione dell'allarme all'evento successivo. Al contrario, quando si riconosce un allarme, questo viene riattivato solo se viene raggiunto il livello di soglia successivo.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***grid node*** > **SSM** > **Eventi** > **Configurazione** > **principale**.
3. Selezionare la casella di controllo **Reset** (Ripristina) per Custom Events (Eventi personalizzati).



4. Selezionare **Applica modifiche**.

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. Ogni nodo della griglia memorizza anche una copia delle informazioni di audit generate sul nodo.

Per un facile accesso ai registri di controllo, è possibile "Configurare l'accesso client di audit per NFS". È inoltre possibile accedere ai file di log di audit direttamente dalla riga di comando del nodo di amministrazione.

StorageGRID può inviare informazioni di audit per impostazione predefinita, oppure è possibile modificare la destinazione:

- Il valore predefinito di StorageGRID per le destinazioni di audit dei nodi locali.
- Le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di

archiviazione.

- In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno.
- "Informazioni sulla configurazione dei messaggi di controllo e delle destinazioni dei log".

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 "Esaminare i registri di audit".

Raccogliere i file di log e i dati di sistema

È possibile utilizzare Grid Manager per recuperare i file di log e i dati di sistema (inclusi i dati di configurazione) per il sistema StorageGRID.

Prima di iniziare

- È necessario accedere a Grid Manager sul nodo di amministrazione primario utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- È necessario disporre della passphrase di provisioning.

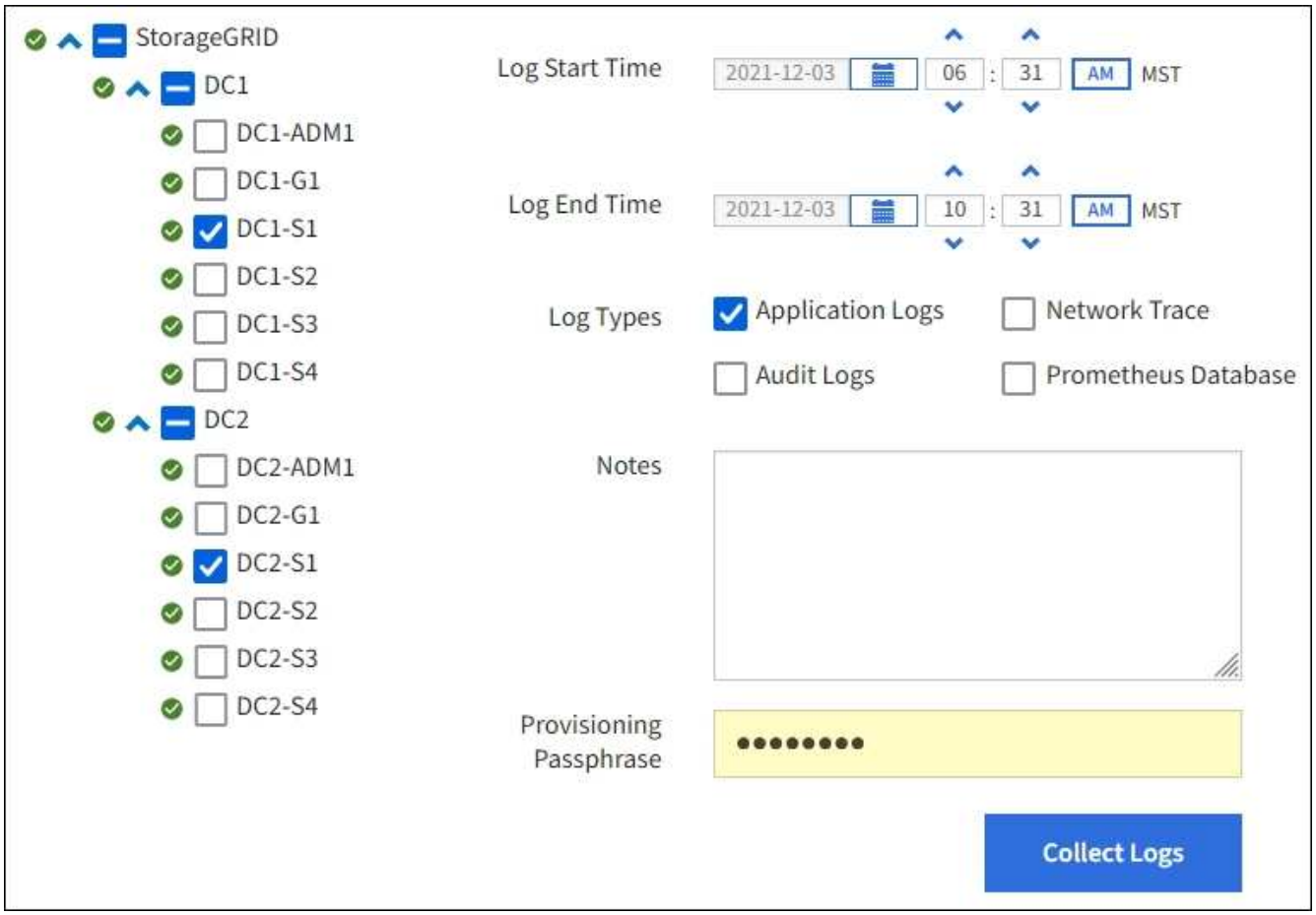
A proposito di questa attività

È possibile utilizzare Grid Manager per la raccolta "file di log", dati di sistema e dati di configurazione da qualsiasi nodo della griglia per il periodo di tempo selezionato. I dati vengono raccolti e archiviati in un file .tar.gz che è possibile scaricare sul computer locale.

In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno. Vedere "Configurare i messaggi di audit e le destinazioni dei log".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Logs**.



2. Selezionare i nodi della griglia per i quali si desidera raccogliere i file di log.

   Se necessario, è possibile raccogliere i file di log per l'intera griglia o per un intero sito del data center.

3. Selezionare **ora di inizio** e **ora di fine** per impostare l'intervallo di tempo dei dati da includere nei file di log.

   Se si seleziona un periodo di tempo molto lungo o si raccolgono i registri da tutti i nodi di una griglia di grandi dimensioni, l'archivio del registro potrebbe diventare troppo grande per essere memorizzato su un nodo o troppo grande per essere raccolto nel nodo di amministrazione primario per il download. In questo caso, è necessario riavviare la raccolta dei log con un set di dati più piccolo.

4. Selezionare i tipi di log che si desidera raccogliere.
   - **Registri delle applicazioni**: Registri specifici delle applicazioni che il supporto tecnico utilizza più frequentemente per la risoluzione dei problemi. I log raccolti sono un sottoinsieme dei log dell'applicazione disponibili.
   - **Audit Logs**: Registri contenenti i messaggi di audit generati durante il normale funzionamento del sistema.
   - **Network Trace**: Registri utilizzati per il debug della rete.
   - **Database Prometheus**: Metriche delle serie temporali dei servizi su tutti i nodi.
5. Se si desidera, inserire le note relative ai file di registro che si stanno raccogliendo nella casella di testo **Notes**.

   È possibile utilizzare queste note per fornire informazioni di supporto tecnico sul problema che ha richiesto di raccogliere i file di log. Le note vengono aggiunte a un file chiamato `info.txt`, insieme ad altre

informazioni sulla raccolta di file di log. Il `info.txt` il file viene salvato nel pacchetto di archiviazione del file di log.

6. Inserire la passphrase di provisioning per il sistema StorageGRID nella casella di testo **Passphrase di provisioning**.
7. Selezionare **Collect Logs** (raccolta registri).

   Quando si invia una nuova richiesta, la raccolta precedente di file di log viene eliminata.

   È possibile utilizzare la pagina Logs per monitorare l'avanzamento della raccolta dei file di log per ciascun nodo della griglia.

   Se viene visualizzato un messaggio di errore relativo alle dimensioni del registro, provare a raccogliere i registri per un periodo di tempo più breve o per un numero inferiore di nodi.

8. Selezionare **Download** al termine della raccolta dei file di log.

   Il file *.tar.gz* contiene tutti i file di log di tutti i nodi della griglia in cui la raccolta dei log ha avuto esito positivo. All'interno del file *.tar.gz* combinato, è presente un archivio di file di log per ciascun nodo della griglia.

Al termine

Se necessario, è possibile scaricare nuovamente il pacchetto di archiviazione del file di log in un secondo momento.

In alternativa, è possibile selezionare **Delete** (Elimina) per rimuovere il pacchetto di archiviazione del file di log e liberare spazio su disco. Il pacchetto di archiviazione del file di log corrente viene automaticamente rimosso alla successiva raccolta dei file di log.

Attivare manualmente un pacchetto AutoSupport

Per assistere il supporto tecnico nella risoluzione dei problemi del sistema StorageGRID, è possibile attivare manualmente l'invio di un pacchetto AutoSupport.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- È necessario disporre dell'autorizzazione di accesso root o di altra configurazione della griglia.

Fasi

1. Selezionare **SUPPORTO** > **Strumenti** > **AutoSupport**.
2. Nella scheda **azioni**, selezionare **Invia AutoSupport** attivato dall'utente.

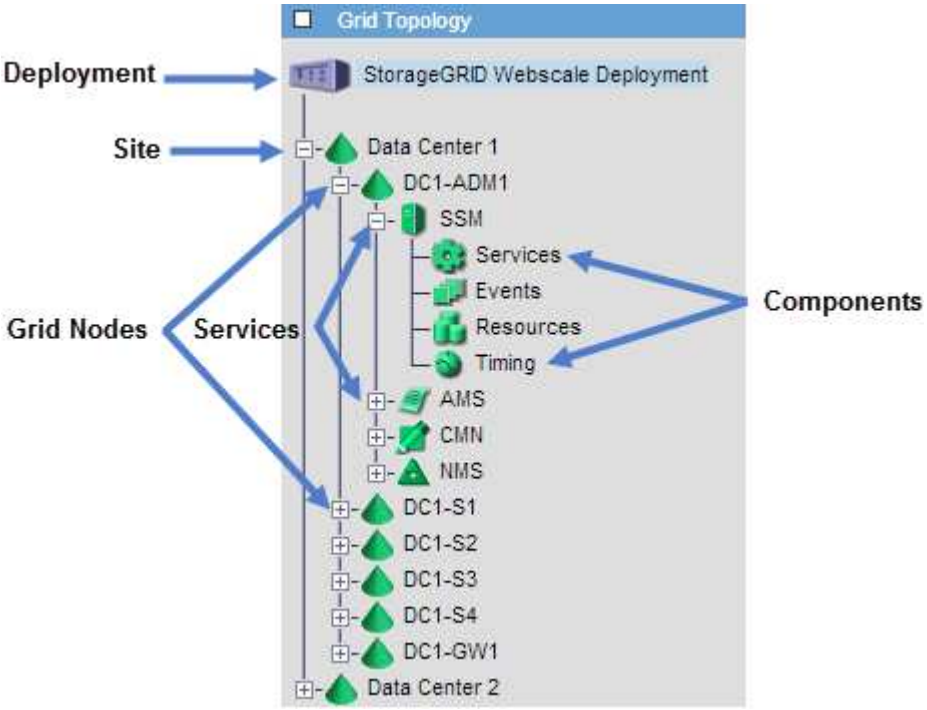
   StorageGRID tenta di inviare un pacchetto AutoSupport al sito di supporto NetApp. Se il tentativo ha esito positivo, i valori **risultato più recente** e **tempo ultimo successo** nella scheda **risultati** vengono aggiornati. Se si verifica un problema, il valore **risultato più recente** viene aggiornato a "non riuscito" e StorageGRID non tenta di inviare nuovamente il pacchetto AutoSupport.

   > Dopo aver inviato un pacchetto AutoSupport attivato dall'utente, aggiornare la pagina AutoSupport nel browser dopo 1 minuto per accedere ai risultati più recenti.

Visualizzare l'albero topologia griglia

L'albero topologia griglia consente di accedere a informazioni dettagliate sugli elementi del sistema StorageGRID, inclusi siti, nodi griglia, servizi e componenti. Nella maggior parte dei casi, è necessario accedere all'albero topologia griglia solo quando indicato nella documentazione o quando si lavora con il supporto tecnico.

Per accedere all'albero topologia griglia, selezionare **SUPPORTO** > **Strumenti** > **topologia griglia**.



Per espandere o comprimere l'albero topologia griglia, fare clic su ⊞ oppure ⊟ a livello di sito, nodo o servizio. Per espandere o comprimere tutti gli elementi dell'intero sito o di ciascun nodo, tenere premuto il tasto **<Ctrl>** e fare clic su.

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 diversi punti del grid manager:

- 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.

Rivedere le metriche di supporto

Durante la risoluzione di un problema, puoi lavorare con il supporto tecnico per rivedere metriche e grafici dettagliati per il tuo sistema StorageGRID.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

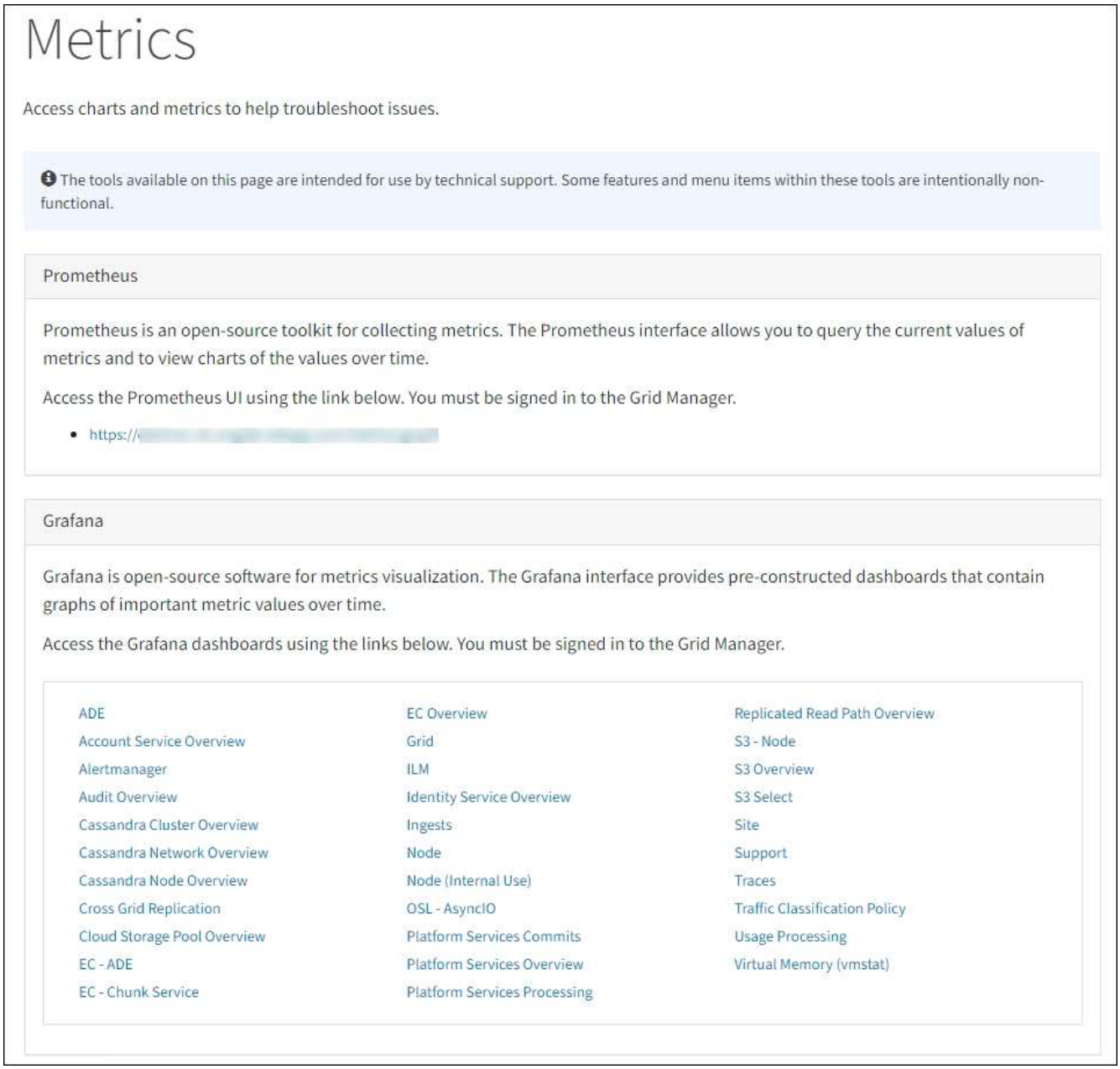
La pagina metriche consente di accedere alle interfacce utente Prometheus e Grafana. Prometheus è un software open-source per la raccolta di metriche. Grafana è un software open-source per la visualizzazione delle metriche.

> 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. Vedere l'elenco di "Metriche Prometheus comunemente utilizzate".

Fasi

1. Come indicato dal supporto tecnico, selezionare **SUPPORTO** > **Strumenti** > **metriche**.

   Di seguito è riportato un esempio della pagina Metrics (metriche):



2. Per interrogare i valori correnti delle metriche StorageGRID e visualizzare i grafici dei valori nel tempo, fare clic sul collegamento nella sezione Prometheus.

   Viene visualizzata l'interfaccia Prometheus. È possibile utilizzare questa interfaccia per eseguire query sulle metriche StorageGRID disponibili e per rappresentare graficamente le metriche StorageGRID nel tempo.

   > 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.

3. Per accedere alle dashboard predefinite contenenti grafici delle metriche StorageGRID nel tempo, fare clic sui collegamenti nella sezione Grafana.

   Viene visualizzata l'interfaccia Grafana per il collegamento selezionato.

Eseguire la diagnostica

Durante la risoluzione di un problema, è possibile collaborare con il supporto tecnico per eseguire la diagnostica sul sistema StorageGRID e rivedere i risultati.

- "Rivedere le metriche di supporto"
- "Metriche Prometheus comunemente utilizzate"

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

La pagina Diagnostics (Diagnostica) esegue una serie di controlli diagnostici sullo stato corrente della griglia. Ogni controllo diagnostico può avere uno dei tre stati seguenti:

-

- **Normale**: Tutti i valori rientrano nell'intervallo normale.
- **Attenzione**: Uno o più valori non rientrano nell'intervallo normale.
- **Attenzione**: Uno o più valori sono significativamente al di fuori dell'intervallo normale.

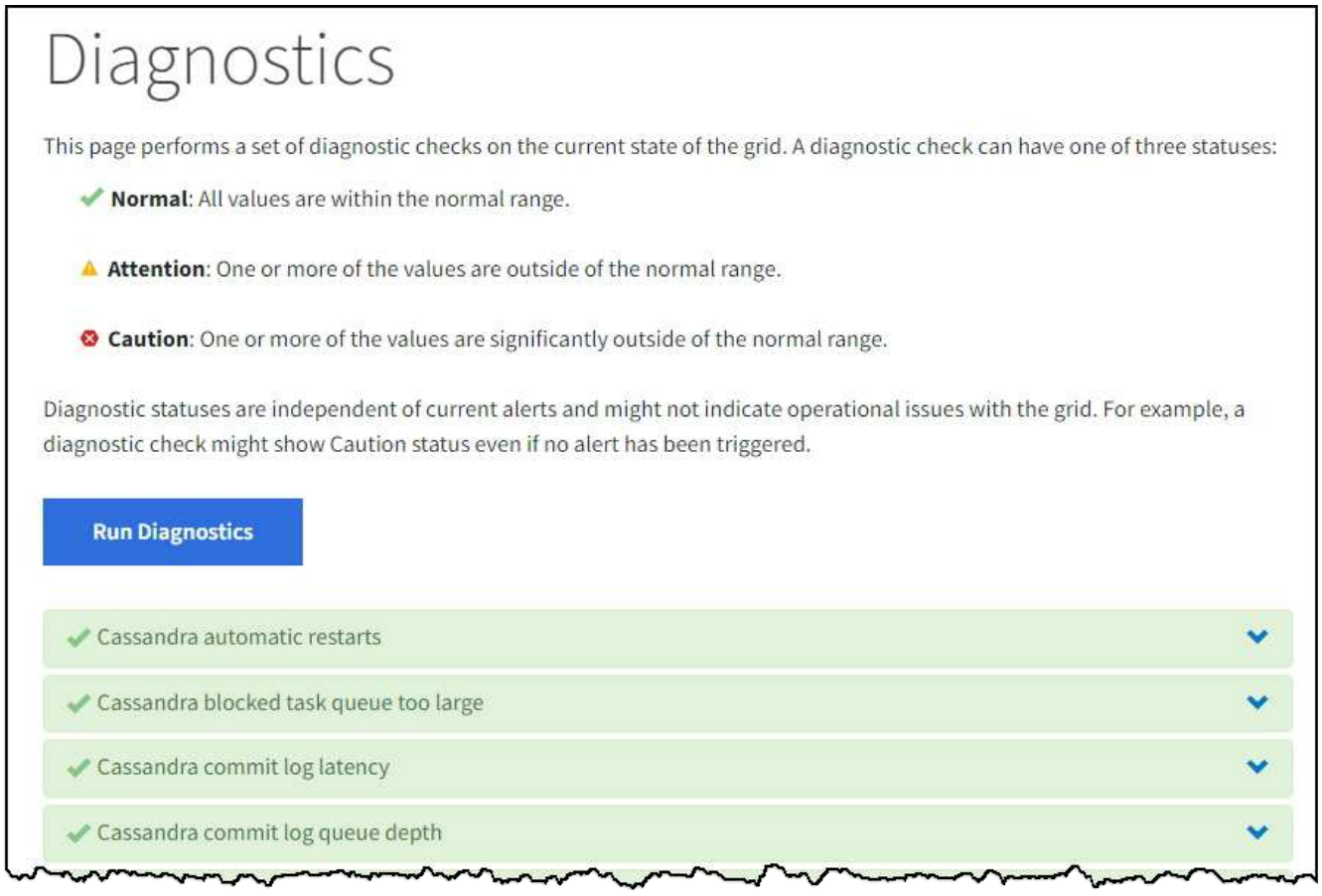
Gli stati di diagnostica sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con la griglia. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato di attenzione anche se non è stato attivato alcun allarme.

Fasi

1. Selezionare **SUPPORTO** > **Strumenti** > **Diagnostica**.

   Viene visualizzata la pagina Diagnostics (Diagnostica) che elenca i risultati di ciascun controllo diagnostico. I risultati vengono ordinati in base alla gravità (attenzione, attenzione e quindi normale). All'interno di ciascuna severità, i risultati sono ordinati in ordine alfabetico.

   In questo esempio, tutte le diagnostiche hanno uno stato normale.



2. Per ulteriori informazioni su una diagnostica specifica, fare clic in un punto qualsiasi della riga.

   Vengono visualizzati i dettagli relativi alla diagnostica e ai risultati correnti. Sono elencati i seguenti dettagli:

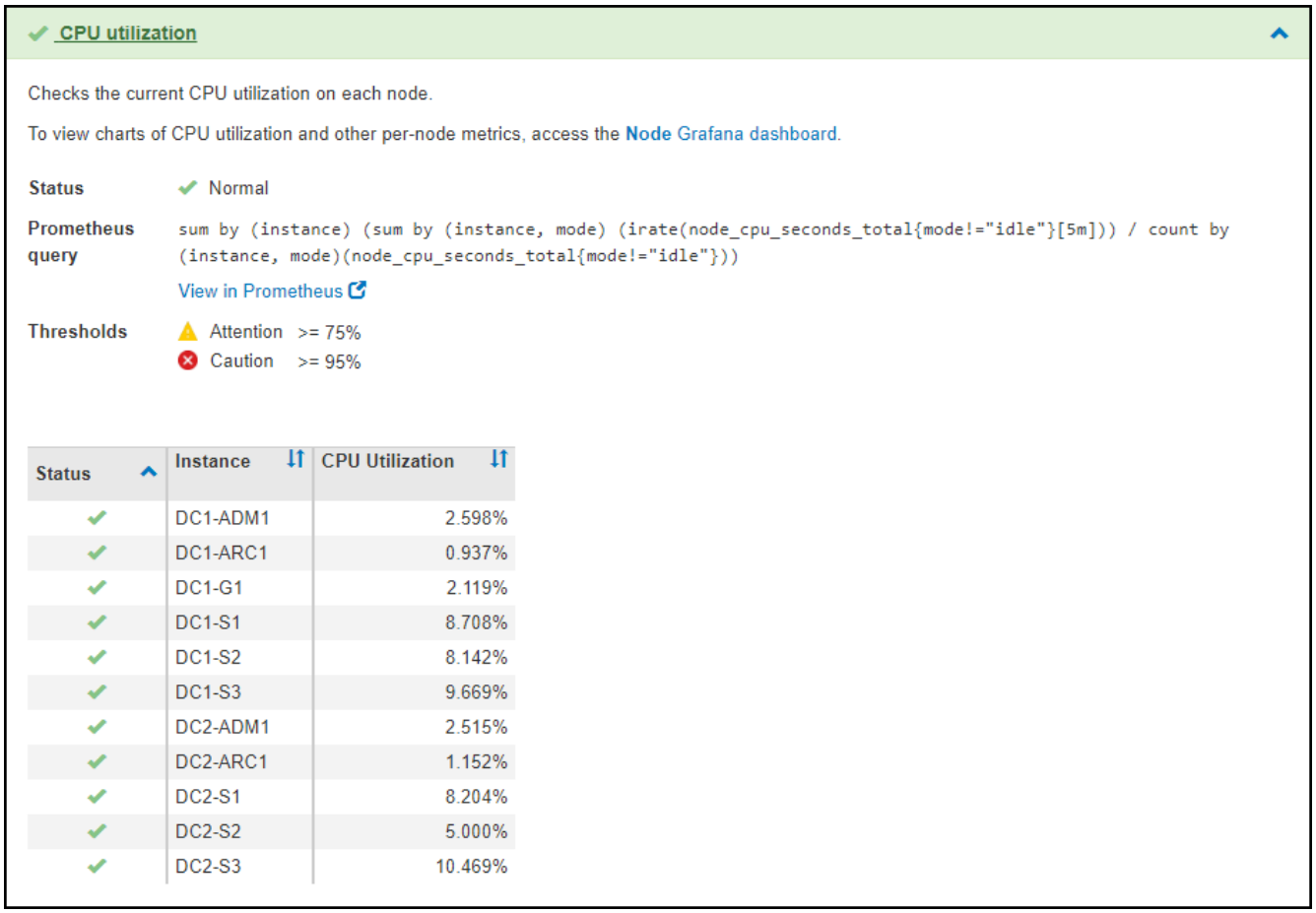
   - **Status** (Stato): Lo stato corrente di questa diagnostica: Normal (normale), Attention (attenzione) o Caution (attenzione).
   - **Query Prometheus**: Se utilizzata per la diagnostica, l'espressione Prometheus utilizzata per generare

i valori di stato. (Un'espressione Prometheus non viene utilizzata per tutte le diagnostiche).

- **Soglie**: Se disponibili per la diagnostica, le soglie definite dal sistema per ogni stato di diagnostica anomalo. (I valori di soglia non vengono utilizzati per tutte le diagnostiche).

  Non puoi modificare queste soglie.

- **Valori di stato**: Una tabella che mostra lo stato e il valore della diagnostica nel sistema StorageGRID. 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.



3. **Opzionale**: Per visualizzare i grafici Grafana relativi a questa diagnostica, fare clic sul collegamento **dashboard Grafana**.

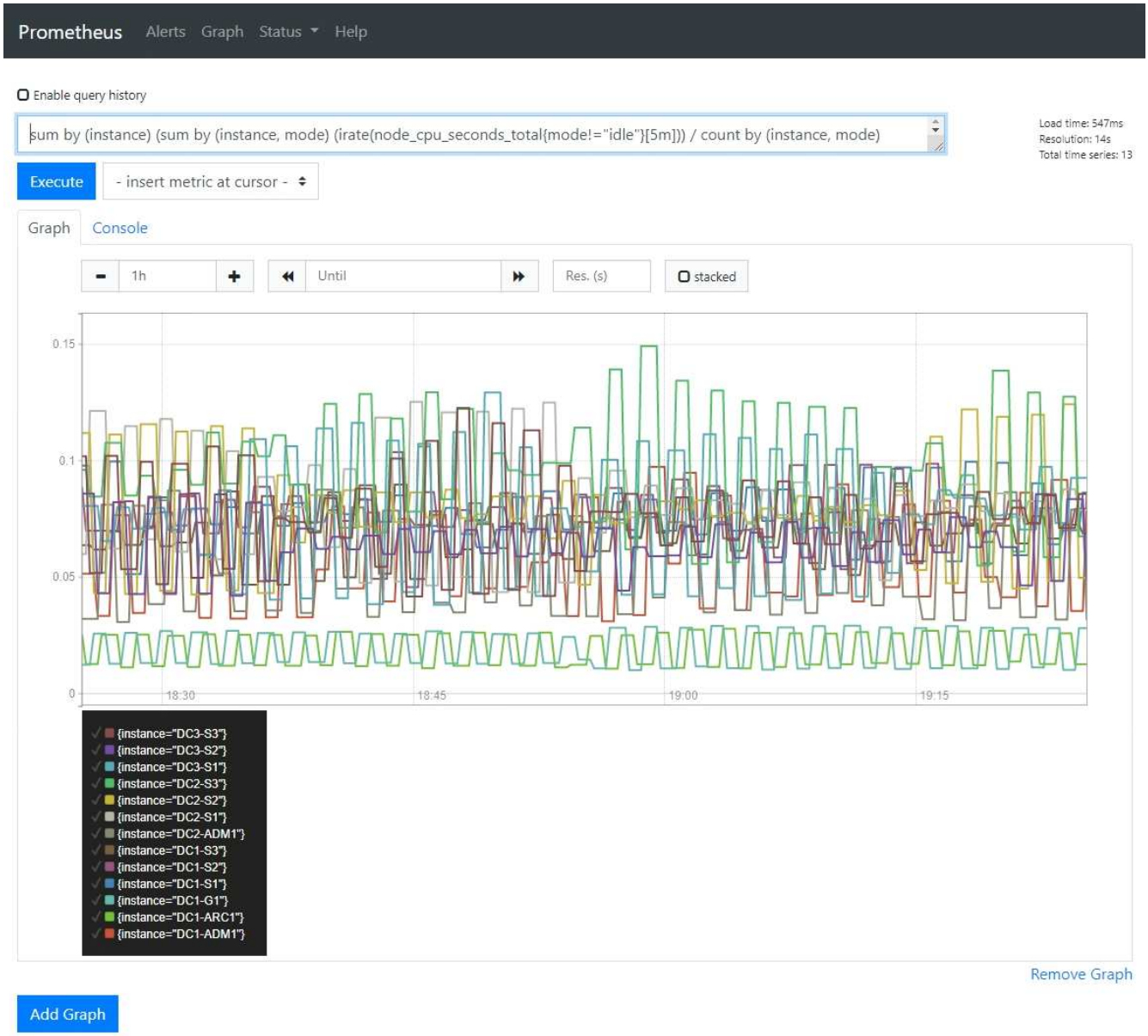
   Questo collegamento non viene visualizzato per tutte le diagnostiche.

   Viene visualizzata la dashboard Grafana correlata. In questo esempio, viene visualizzata la dashboard Node (nodo) che mostra l'utilizzo della CPU nel tempo per questo nodo e altri grafici Grafana per il nodo.

   Puoi anche accedere ai dashboard di Grafana già costruiti dalla sezione Grafana della pagina **SUPPORT** > **Tools** > **Metrics**.

4. **Opzionale**: Per visualizzare un grafico dell'espressione Prometheus nel tempo, fare clic su **Visualizza in Prometheus**.

   Viene visualizzato un grafico Prometheus dell'espressione utilizzata nella diagnostica.



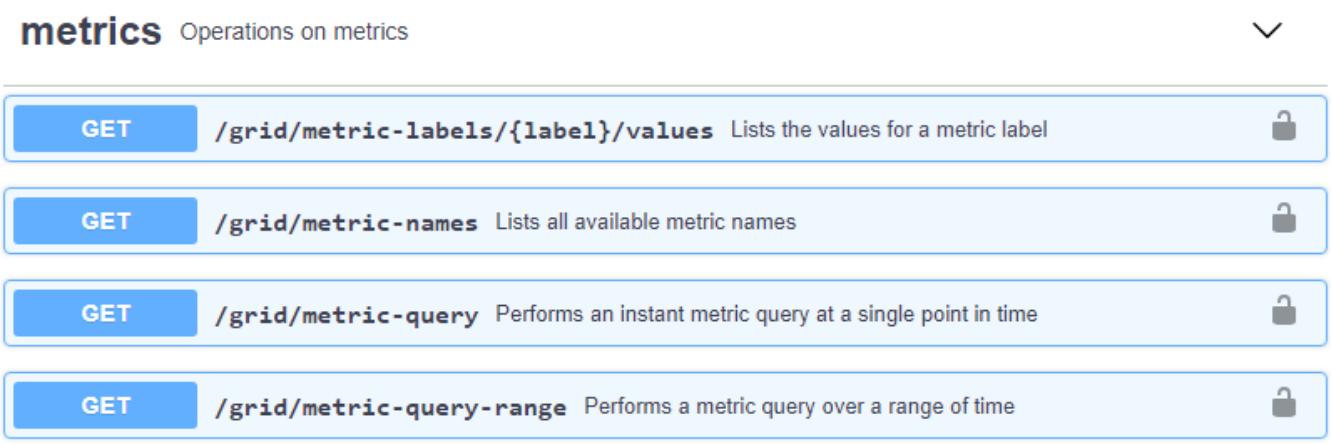
Creare applicazioni di monitoraggio personalizzate

Puoi creare dashboard e applicazioni di monitoraggio personalizzate utilizzando le metriche StorageGRID disponibili nell'API di gestione del grid.

Se si desidera monitorare le metriche non visualizzate in una pagina esistente di Grid Manager o se si desidera creare dashboard personalizzati per StorageGRID, è possibile utilizzare l'API di gestione griglia per eseguire query sulle metriche StorageGRID.

Puoi anche accedere direttamente alle metriche Prometheus con uno strumento di monitoraggio esterno, come Grafana. L'utilizzo di uno strumento esterno richiede il caricamento o la generazione di un certificato client amministrativo per consentire a StorageGRID di autenticare lo strumento per la sicurezza. Vedere "Istruzioni per l'amministrazione di StorageGRID".

Per visualizzare le operazioni API delle metriche, incluso l'elenco completo delle metriche disponibili, accedere a Grid Manager. Nella parte superiore della pagina, selezionare l'icona della guida e selezionare **documentazione API** > **metriche**.



I dettagli su come implementare un'applicazione di monitoraggio personalizzata esulano dall'ambito di questa documentazione.

Risolvere i problemi relativi al sistema StorageGRID

Risoluzione dei problemi di un sistema StorageGRID: Panoramica

Se si riscontrano problemi durante l'utilizzo di un sistema StorageGRID, consultare i suggerimenti e le linee guida di questa sezione per ottenere assistenza nella determinazione e nella risoluzione del problema.

Spesso è possibile risolvere i problemi da soli; tuttavia, potrebbe essere necessario eseguire l'escalation di alcuni problemi al supporto tecnico.

definire il problema

Il primo passo per risolvere un problema è definire il problema in modo chiaro.

Questa tabella fornisce esempi dei tipi di informazioni che è possibile raccogliere per definire un problema:

Domanda	Esempio di risposta
Cosa fa o non fa il sistema StorageGRID? Quali sono i suoi sintomi?	Le applicazioni client segnalano che non è possibile acquisire oggetti in StorageGRID.
Quando è iniziato il problema?	L'acquisizione di oggetti è stata negata per la prima volta alle 14:50 dell'8 gennaio 2020.
Come hai notato il problema per la prima volta?	Notificato dall'applicazione client. Ha ricevuto anche notifiche email di avviso.
Il problema si verifica in modo coerente o solo a volte?	Il problema è in corso.

Domanda	Esempio di risposta
Se il problema si verifica regolarmente, quali passaggi lo causano	Il problema si verifica ogni volta che un client tenta di acquisire un oggetto.
Se il problema si verifica in modo intermittente, quando si verifica? Registrare i tempi di ciascun incidente di cui si è a conoscenza.	Il problema non è intermittente.
Hai già visto questo problema? Con quale frequenza avete avuto questo problema in passato?	Questa è la prima volta che vedo questo problema.

Valutare i rischi e l'impatto sul sistema

Una volta definito il problema, valutarne il rischio e l'impatto sul sistema StorageGRID. Ad esempio, la presenza di avvisi critici non significa necessariamente che il sistema non stia fornendo servizi di base.

Questa tabella riassume l'impatto del problema di esempio sulle operazioni del sistema:

Domanda	Esempio di risposta
Il sistema StorageGRID è in grado di acquisire contenuti?	No
Le applicazioni client possono recuperare il contenuto?	Alcuni oggetti possono essere recuperati e altri no.
I dati sono a rischio?	No
La capacità di condurre il business è gravemente compromessa?	Sì, perché le applicazioni client non possono memorizzare oggetti nel sistema StorageGRID e i dati non possono essere recuperati in modo coerente.

Raccogliere i dati

Dopo aver definito il problema e averne valutato il rischio e l'impatto, raccogliere i dati per l'analisi. Il tipo di dati più utili da raccogliere dipende dalla natura del problema.

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Creare una tempistica delle modifiche recenti	Le modifiche al sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.	• Creare una tempistica delle modifiche recenti

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Consente di rivedere avvisi e allarmi	Gli avvisi e gli allarmi possono aiutare a determinare rapidamente la causa principale di un problema fornendo importanti indizi sui problemi sottostanti che potrebbero causarlo. Consultare l'elenco degli avvisi e degli allarmi correnti per verificare se StorageGRID ha identificato la causa principale di un problema. Per ulteriori informazioni, rivedere gli avvisi e gli allarmi attivati in passato.	• "Visualizzare gli avvisi correnti e risolti" • "Gestire gli allarmi (sistema legacy)"
Monitorare gli eventi	Gli eventi includono qualsiasi errore di sistema o evento di guasto per un nodo, inclusi errori come gli errori di rete. Monitorare gli eventi per ottenere ulteriori informazioni sui problemi o per la risoluzione dei problemi.	• "Monitorare gli eventi"
Identificare i trend utilizzando grafici e report di testo	Le tendenze possono fornire indizi preziosi su quando sono comparsi i problemi per la prima volta e possono aiutarti a capire quanto rapidamente le cose stanno cambiando.	• "Utilizzare grafici e grafici" • "Utilizzare report di testo"
Stabilire le linee di base	Raccogliere informazioni sui livelli normali dei vari valori operativi. Questi valori di riferimento, e le deviazioni da queste linee di base, possono fornire indizi preziosi.	• Stabilire le linee di base
Eseguire test di acquisizione e recupero	Per risolvere i problemi di performance con acquisizione e recupero, utilizzare una workstation per memorizzare e recuperare gli oggetti. Confrontare i risultati con quelli osservati durante l'utilizzo dell'applicazione client.	• "Monitorare L'EFFICIENZA e OTTENERE le performance"
Esaminare i messaggi di audit	Esaminare i messaggi di audit per seguire in dettaglio le operazioni di StorageGRID. I dettagli nei messaggi di audit possono essere utili per la risoluzione di molti tipi di problemi, inclusi quelli relativi alle performance.	• "Esaminare i messaggi di audit"
Controllare le posizioni degli oggetti e l'integrità dello storage	In caso di problemi di storage, verificare che gli oggetti siano posizionati nel punto previsto. Verificare l'integrità dei dati dell'oggetto su un nodo di storage.	• "Monitorare le operazioni di verifica degli oggetti" • "Confermare le posizioni dei dati degli oggetti" • "Verificare l'integrità dell'oggetto"

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Raccogliere i dati per il supporto tecnico	Il supporto tecnico potrebbe richiedere di raccogliere dati o rivedere informazioni specifiche per risolvere i problemi.	• "Raccogliere i file di log e i dati di sistema" • "Attivare manualmente un pacchetto AutoSupport" • "Rivedere le metriche di supporto"

Crea una timeline di modifiche recenti

Quando si verifica un problema, è necessario prendere in considerazione le modifiche apportate di recente e il momento in cui si sono verificate tali modifiche.

- Le modifiche al sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.
- Una tempistica delle modifiche può aiutarti a identificare quali modifiche potrebbero essere responsabili di un problema e in che modo ciascuna modifica potrebbe avere influenzato il suo sviluppo.

Creare una tabella di modifiche recenti al sistema che includa informazioni su quando si è verificata ogni modifica e su eventuali dettagli rilevanti relativi alla modifica, ad esempio informazioni su ciò che è accaduto durante l'esecuzione della modifica:

Tempo di cambiamento	Tipo di cambiamento	Dettagli
Ad esempio: • Quando è stato avviato il ripristino del nodo? • Quando è stato completato l'aggiornamento del software? • Hai interrotto il processo?	Che cosa è successo? Cosa hai fatto?	Documentare i dettagli relativi alla modifica. Ad esempio: • Dettagli delle modifiche di rete. • Quale hotfix è stato installato. • Come sono cambiati i carichi di lavoro dei client. Assicurarsi di notare se più di una modifica si è verificata contemporaneamente. Ad esempio, questa modifica è stata apportata mentre era in corso un aggiornamento?

Esempi di modifiche recenti significative

Ecco alcuni esempi di modifiche potenzialmente significative:

- Il sistema StorageGRID è stato recentemente installato, ampliato o ripristinato?
- Il sistema è stato aggiornato di recente? È stata applicata una correzione rapida?
- L'hardware è stato riparato o modificato di recente?
- La policy ILM è stata aggiornata?

- Il carico di lavoro del client è cambiato?
- L'applicazione client o il suo comportamento sono cambiati?
- Hai modificato i bilanciatori di carico o aggiunto o rimosso un gruppo ad alta disponibilità di nodi di amministrazione o nodi gateway?
- Sono state avviate attività che potrebbero richiedere molto tempo? Alcuni esempi sono:
  - Ripristino di un nodo di storage guasto
  - Disattivazione del nodo di storage
- Sono state apportate modifiche all'autenticazione dell'utente, ad esempio l'aggiunta di un tenant o la modifica della configurazione LDAP?
- La migrazione dei dati è in corso?
- I servizi della piattaforma sono stati abilitati o modificati di recente?
- La compliance è stata abilitata di recente?
- I pool di storage cloud sono stati aggiunti o rimossi?
- Sono state apportate modifiche alla compressione o alla crittografia dello storage?
- Sono state apportate modifiche all'infrastruttura di rete? Ad esempio, VLAN, router o DNS.
- Sono state apportate modifiche alle origini NTP?
- Sono state apportate modifiche alle interfacce Grid, Admin o Client Network?
- Sono state apportate modifiche alla configurazione del nodo di archiviazione?
- Sono state apportate altre modifiche al sistema StorageGRID o al suo ambiente?

Stabilire le linee di base

È possibile stabilire linee di base per il sistema registrando i livelli normali di diversi valori operativi. In futuro, è possibile confrontare i valori correnti con queste linee di base per rilevare e risolvere i valori anomali.

Proprietà	Valore	Come ottenere
Consumo medio di storage	GB consumati al giorno Percentuale consumata al giorno	Accedere a Grid Manager. Nella pagina Nodes (nodi), selezionare l'intera griglia o un sito e passare alla scheda Storage (archiviazione). Nel grafico Storage used - Object Data (Storage utilizzato - dati oggetto), individuare un periodo in cui la riga è abbastanza stabile. Posizionare il cursore sul grafico per stimare la quantità di storage consumata ogni giorno È possibile raccogliere queste informazioni per l'intero sistema o per un data center specifico.

Proprietà	Valore	Come ottenere
Consumo medio di metadati	GB consumati al giorno Percentuale consumata al giorno	Accedere a Grid Manager. Nella pagina Nodes (nodi), selezionare l'intera griglia o un sito e passare alla scheda Storage (archiviazione). Nel grafico Storage used - Object Metadata (Storage utilizzato - metadati oggetto), individuare un punto in cui la riga è abbastanza stabile. Posiziona il cursore sul grafico per stimare la quantità di storage dei metadati consumata ogni giorno È possibile raccogliere queste informazioni per l'intero sistema o per un data center specifico.
Tasso di operazioni S3/Swift	Operazioni/secondo	Nella dashboard di Grid Manager, selezionare **Performance** > **S3 Operations** o **Performance** > **Swift Operations**. Per visualizzare i tassi di acquisizione e recupero e i conteggi per un sito o nodo specifico, selezionare **NODES** > ***Site o Storage Node*** > **Objects**. Posizionare il cursore sul grafico Ingest e Retrieve per S3 o Swift.
Operazioni S3/Swift non riuscite	Operazioni	Selezionare **SUPPORT** > **Tools** > **Grid topology**. Nella scheda Overview (Panoramica) della sezione API Operations (operazioni API), visualizzare il valore di S3 Operations - Failed (operazioni S3 - non riuscite) o Swift Operations - Failed (operazioni Swift - non riuscite).
Tasso di valutazione ILM	Oggetti/secondo	Dalla pagina nodi, selezionare ***grid*** > **ILM**. Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore sul grafico per stimare un valore di riferimento per **Evaluation rate** per il sistema.
Velocità di scansione ILM	Oggetti/secondo	Selezionare **NODI** > ***grid*** > **ILM**. Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore sul grafico per stimare un valore di riferimento per **velocità di scansione** per il sistema.

Proprietà	Valore	Come ottenere
Oggetti accodati dalle operazioni del client	Oggetti/secondo	Selezionare **NODI** > ***grid*** > **ILM**. Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore sul grafico per stimare un valore di riferimento per **oggetti accodati (da operazioni client)** per il sistema.
Latenza media delle query	Millisecondi	Selezionare **NODI** > ***nodo di storage*** > **oggetti**. Nella tabella Query, visualizzare il valore della latenza media.

Analizzare i dati

Utilizzare le informazioni raccolte per determinare la causa del problema e le potenziali soluzioni.

-analisi dipende dal problema, ma in generale:

- Individuare i punti di guasto e i colli di bottiglia utilizzando gli allarmi.
- Ricostruire la cronologia dei problemi utilizzando la cronologia degli allarmi e i grafici.
- Utilizzare i grafici per individuare le anomalie e confrontare la situazione del problema con il normale funzionamento.

Lista di controllo per le informazioni di escalation

Se non riesci a risolvere il problema da solo, contatta il supporto tecnico. Prima di contattare il supporto tecnico, raccogliere le informazioni elencate nella seguente tabella per facilitare la risoluzione del problema.

✔	Elemento	Note
	Dichiarazione del problema	Quali sono i sintomi del problema? Quando è iniziato il problema? Si verifica in modo coerente o intermittente? In caso di intermittenza, quali sono le volte in cui si è verificato il problema? Definire il problema
	Valutazione dell'impatto	Qual è la gravità del problema? Qual è l'impatto sull'applicazione client? • Il client si è connesso correttamente in precedenza? • Il client è in grado di acquisire, recuperare ed eliminare i dati?
	ID sistema StorageGRID	Selezionare **MANUTENZIONE** > **sistema** > **licenza**. L'ID di sistema StorageGRID viene visualizzato come parte della licenza corrente.

✔	Elemento	Note
	Versione del software	Nella parte superiore di Gestione griglia, selezionare l'icona della guida e selezionare **About** (informazioni su) per visualizzare la versione di StorageGRID.
	Personalizzazione	Riepilogare la configurazione del sistema StorageGRID. Ad esempio, elencare quanto segue: • Il grid utilizza la compressione dello storage, la crittografia dello storage o la conformità? • ILM produce oggetti replicati o sottoposti a erasure coding? ILM garantisce la ridondanza del sito? Le regole ILM utilizzano i comportamenti di ingest bilanciato, rigoroso o doppio commit?
	File di log e dati di sistema	Raccogliere i file di log e i dati di sistema per il sistema. Selezionare **SUPPORT** > **Tools** > **Logs**. È possibile raccogliere i log per l'intera griglia o per i nodi selezionati. Se si stanno raccogliendo registri solo per i nodi selezionati, assicurarsi di includere almeno un nodo di storage che dispone del servizio ADC. I primi tre nodi di storage di un sito includono il servizio ADC. "Raccogliere i file di log e i dati di sistema"
	Informazioni di riferimento	Raccogliere informazioni di riferimento relative alle operazioni di acquisizione, alle operazioni di recupero e al consumo dello storage. Stabilire le linee di base
	Tempistiche delle modifiche recenti	Creare una timeline che riepiloga le modifiche recenti apportate al sistema o al suo ambiente. Creare una tempistica delle modifiche recenti
	Cronologia degli sforzi per diagnosticare il problema	Se sono state adottate misure per diagnosticare o risolvere il problema da soli, assicurarsi di registrare i passaggi e il risultato.

Risolvere i problemi relativi a oggetti e storage

Confermare le posizioni dei dati degli oggetti

A seconda del problema, potrebbe essere necessario "confermare la posizione in cui vengono memorizzati i dati dell'oggetto". Ad esempio, è possibile verificare che il criterio

ILM funzioni come previsto e che i dati degli oggetti vengano memorizzati dove previsto.

Prima di iniziare

- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:
  - **UUID**: Identificativo universalamente univoco dell'oggetto. Inserire l'UUID in tutte le lettere maiuscole.
  - **CBID**: Identificatore univoco dell'oggetto all'interno di StorageGRID . È possibile ottenere il CBID di un oggetto dal log di audit. Inserire il CBID in tutte le lettere maiuscole.
  - **S3 bucket and object key** (bucket S3 e chiave oggetto): Quando un oggetto viene acquisito tramite "Interfaccia S3", l'applicazione client utilizza una combinazione di bucket e chiave oggetto per memorizzare e identificare l'oggetto.
  - **Swift container and object name**: Quando un oggetto viene acquisito tramite "Interfaccia Swift", l'applicazione client utilizza una combinazione di container e nome oggetto per memorizzare e identificare l'oggetto.

Fasi

1. Selezionare **ILM** > **Object metadata lookup**.
2. Digitare l'identificativo dell'oggetto nel campo **Identifier**.

   È possibile immettere UUID, CBID, S3 bucket/object-key o Swift container/object-name.

3. Se si desidera cercare una versione specifica dell'oggetto, inserire l'ID versione (facoltativo).

4. Selezionare **Cerca**.

   Il "risultati della ricerca dei metadati degli oggetti" appare. In questa pagina sono elencati i seguenti tipi di informazioni:

   - Metadati di sistema, tra cui l'ID oggetto (UUID), l'ID versione (facoltativo), il nome dell'oggetto, il nome del contenitore, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora della prima creazione dell'oggetto e la data e l'ora dell'ultima modifica dell'oggetto.
   - Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
   - Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
   - Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
   - Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
   - Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.

- Per oggetti segmentati e multiparte, un elenco di segmenti di oggetti che include identificatori di segmenti e dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono visualizzati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.

  Nell'esempio seguente vengono illustrati i risultati della ricerca dei metadati degli oggetti per un oggetto di test S3 memorizzato come due copie replicate.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Errori dell'archivio di oggetti (volume di storage)

Lo storage sottostante su un nodo di storage è diviso in archivi di oggetti. Gli archivi di oggetti sono anche noti come volumi di storage.

È possibile visualizzare le informazioni sull'archivio di oggetti per ciascun nodo di storage. Gli archivi di oggetti sono visualizzati nella parte inferiore della pagina **NODE** > ***Storage Node*** > **Storage**.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

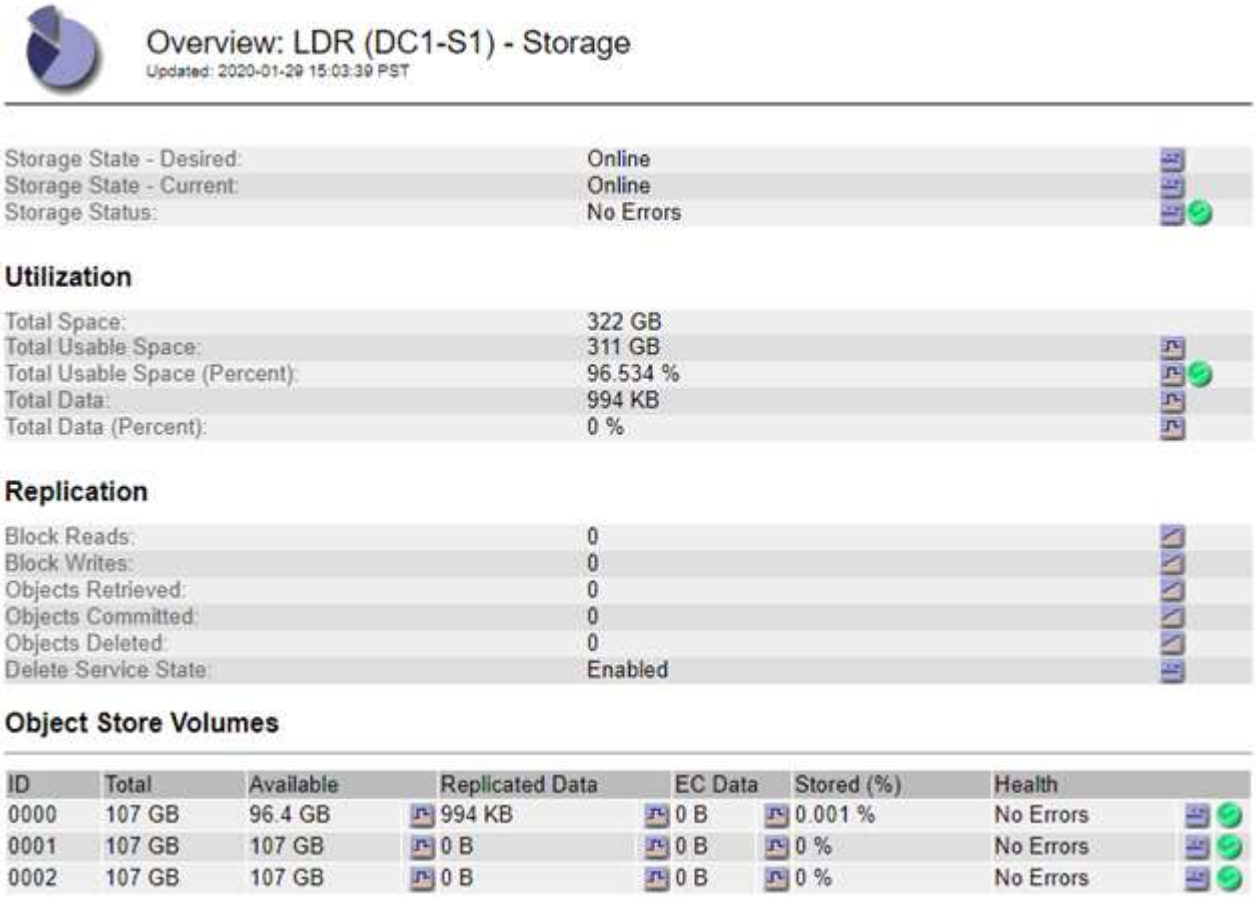
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Per saperne di più "Dettagli su ciascun nodo di storage", attenersi alla seguente procedura:

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Storage** > **Overview** > **Main**.



A seconda della natura del guasto, gli errori di un volume di storage potrebbero essere riflessi in un allarme sullo stato di storage o sullo stato di un archivio di oggetti. In caso di guasto di un volume di storage, è necessario riparare il volume di storage guasto per ripristinare la funzionalità completa del nodo di storage il prima possibile. Se necessario, accedere alla scheda **Configurazione** e. "Posizionare il nodo di storage in uno stato di sola-lettura" In modo che il sistema StorageGRID possa utilizzarlo per il recupero dei dati durante la preparazione per un ripristino completo del server.

Verificare l'integrità dell'oggetto

Il sistema StorageGRID verifica l'integrità dei dati degli oggetti sui nodi di storage, verificando la presenza di oggetti corrotti e mancanti.

Esistono due processi di verifica: Verifica in background e verifica dell'esistenza degli oggetti (in precedenza chiamata verifica in primo piano). Lavorano insieme per garantire l'integrità dei dati. La verifica in background viene eseguita automaticamente e verifica continuamente la correttezza dei dati dell'oggetto. Il controllo dell'esistenza degli oggetti può essere attivato da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) degli oggetti.

Che cos'è la verifica in background?

Il processo di verifica in background verifica automaticamente e continuamente la presenza di copie corrotte

dei dati degli oggetti nei nodi di storage e tenta automaticamente di risolvere eventuali problemi rilevati.

La verifica in background verifica l'integrità degli oggetti replicati e degli oggetti con codifica in cancellazione, come segue:

- **Oggetti replicati**: Se il processo di verifica in background trova un oggetto replicato corrotto, la copia corrotta viene rimossa dalla sua posizione e messa in quarantena in un altro punto del nodo di storage. Quindi, viene generata e posizionata una nuova copia non danneggiata per soddisfare le policy ILM attive. La nuova copia potrebbe non essere inserita nel nodo di storage utilizzato per la copia originale.

  > I dati degli oggetti corrotti vengono messi in quarantena invece che cancellati dal sistema, in modo che sia ancora possibile accedervi. Per ulteriori informazioni sull'accesso ai dati degli oggetti in quarantena, contattare il supporto tecnico.

- **Oggetti con codifica di cancellazione**: Se il processo di verifica in background rileva che un frammento di un oggetto con codifica di cancellazione è corrotto, StorageGRID tenta automaticamente di ricostruire il frammento mancante sullo stesso nodo di storage, utilizzando i dati rimanenti e i frammenti di parità. Se il frammento danneggiato non può essere ricostruito, viene eseguito un tentativo di recuperare un'altra copia dell'oggetto. Se il recupero ha esito positivo, viene eseguita una valutazione ILM per creare una copia sostitutiva dell'oggetto con codice di cancellazione.

  Il processo di verifica in background controlla solo gli oggetti sui nodi di storage. Non controlla gli oggetti nei nodi di archiviazione o in un pool di storage cloud. Gli oggetti devono avere più di quattro giorni di età per poter essere qualificati per la verifica in background.

La verifica in background viene eseguita a una velocità continua che non interferisce con le normali attività del sistema. Impossibile interrompere la verifica in background. Tuttavia, se si sospetta un problema, è possibile aumentare il tasso di verifica in background per verificare più rapidamente il contenuto di un nodo di storage.

Avvisi e allarmi (legacy) relativi alla verifica in background

Se il sistema rileva un oggetto corrotto che non è in grado di correggere automaticamente (perché il danneggiamento impedisce l'identificazione dell'oggetto), viene attivato l'avviso **rilevato oggetto corrotto non identificato**.

Se la verifica in background non riesce a sostituire un oggetto corrotto perché non riesce a individuare un'altra copia, viene attivato l'avviso **oggetti persi**.

Modificare il tasso di verifica in background

È possibile modificare la velocità con cui la verifica in background controlla i dati degli oggetti replicati su un nodo di storage in caso di dubbi sull'integrità dei dati.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

È possibile modificare il tasso di verifica per la verifica in background su un nodo di storage:

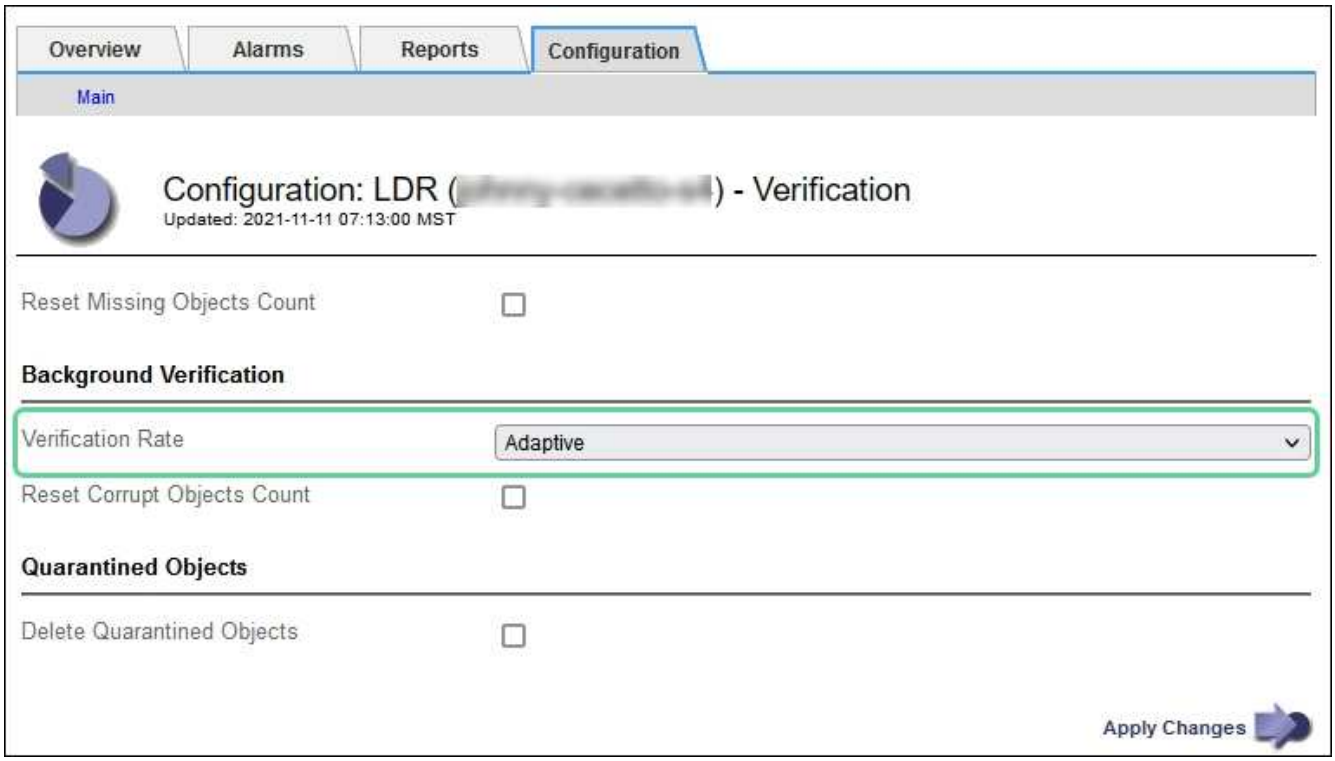
- Adattivo: Impostazione predefinita. L'attività è progettata per la verifica a un massimo di 4 MB/s o 10 oggetti/s (a seconda di quale valore viene superato per primo).

- Elevato: La verifica dello storage procede rapidamente, a una velocità che può rallentare le normali attività del sistema.

Utilizzare la frequenza di verifica alta solo quando si sospetta che un errore hardware o software possa avere dati oggetto corrotti. Una volta completata la verifica in background con priorità alta, la velocità di verifica viene ripristinata automaticamente su Adaptive.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Storage Node*** > **LDR** > **Verification**.
3. Selezionare **Configurazione** > **principale**.
4. Accedere a **LDR** > **verifica** > **Configurazione** > **principale**.
5. In background Verification (verifica in background), selezionare **Verification Rate** (tasso di verifica) > **High** (Alto) o **Verification Rate** (tasso di verifica) > **Adaptive** (



Impostando la frequenza di verifica su alta, si attiva l'allarme VPRI (tasso di verifica) legacy a livello di avviso.

6. Fare clic su **Applica modifiche**.
7. Monitorare i risultati della verifica in background per gli oggetti replicati.
   a. Andare a **NODES** > ***Storage Node*** > **Objects**.
   b. Nella sezione verifica, monitorare i valori per **oggetti corrotti** e **oggetti corrotti non identificati**.

      Se la verifica in background trova dati di oggetti replicati corrotti, la metrica **Corrupt Objects** viene incrementata e StorageGRID tenta di estrarre l'identificatore di oggetti dai dati, come segue:

      - Se è possibile estrarre l'identificativo dell'oggetto, StorageGRID crea automaticamente una nuova copia dei dati dell'oggetto. La nuova copia può essere effettuata in qualsiasi punto del sistema

StorageGRID che soddisfi le policy ILM attive.

- Se l'identificatore dell'oggetto non può essere estratto (perché è stato danneggiato), la metrica **Corrupt Objects Unidentified** viene incrementata e viene attivato l'avviso **Unidentified corrotto object detected**.

c. Se vengono rilevati dati di oggetti replicati corrotti, contattare il supporto tecnico per determinare la causa principale del danneggiamento.

8. Monitorare i risultati della verifica in background per gli oggetti con codifica erasure.

   Se la verifica in background trova frammenti corrotti di dati di oggetti con codifica di cancellazione, l'attributo corrotto Fragments Detected (frammenti corrotti rilevati) viene incrementato. StorageGRID esegue il ripristino ricostruendo il frammento corrotto in posizione sullo stesso nodo di storage.

   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***Storage Node*** > **LDR** > **Erasure Coding**.
   c. Nella tabella Verification Results (risultati verifica), monitorare l'attributo corrotto Fragments Detected (ECCD).

9. Una volta ripristinati automaticamente gli oggetti corrotti dal sistema StorageGRID, ripristinare il numero di oggetti corrotti.
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
   c. Selezionare **Ripristina conteggio oggetti corrotti**.
   d. Fare clic su **Applica modifiche**.

10. Se sei sicuro che gli oggetti in quarantena non sono necessari, puoi eliminarli.

    > Se viene attivato l'allarme **oggetti persi** o l'allarme legacy PERSI (oggetti persi), il supporto tecnico potrebbe voler accedere agli oggetti in quarantena per eseguire il debug del problema sottostante o tentare il ripristino dei dati.

    a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
    b. Selezionare ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
    c. Selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena).
    d. Selezionare **Applica modifiche**.

Che cos'è il controllo dell'esistenza di un oggetto?

Il controllo dell'esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti con codifica di cancellazione sono presenti in un nodo di storage. Il controllo dell'esistenza degli oggetti non verifica i dati degli oggetti stessi (la verifica in background lo fa), ma fornisce un modo per verificare l'integrità dei dispositivi di storage, soprattutto se un recente problema hardware potrebbe avere influenzato l'integrità dei dati.

A differenza della verifica in background, che si verifica automaticamente, è necessario avviare manualmente un lavoro di verifica dell'esistenza di un oggetto.

Il controllo dell'esistenza degli oggetti legge i metadati di ogni oggetto memorizzato in StorageGRID e verifica l'esistenza di copie di oggetti replicate e frammenti di oggetti codificati per la cancellazione. I dati mancanti vengono gestiti come segue:

- **Copie replicate**: Se manca una copia dei dati degli oggetti replicati, StorageGRID tenta automaticamente di sostituire la copia da una copia memorizzata altrove nel sistema. Il nodo di storage esegue una copia esistente attraverso una valutazione ILM, che determina che il criterio ILM corrente non è più soddisfatto per questo oggetto perché manca un'altra copia. Viene generata e posizionata una nuova copia per soddisfare i criteri ILM attivi del sistema. Questa nuova copia potrebbe non essere posizionata nella stessa posizione in cui è stata memorizzata la copia mancante.
- **Frammenti con codifica di cancellazione**: Se manca un frammento di un oggetto con codifica di cancellazione, StorageGRID tenta automaticamente di ricostruire il frammento mancante sullo stesso nodo di storage utilizzando i frammenti rimanenti. Se il frammento mancante non può essere ricostruito (perché sono stati persi troppi frammenti), ILM tenta di trovare un'altra copia dell'oggetto, che può utilizzare per generare un nuovo frammento con codifica di cancellazione.

Eseguire il controllo dell'esistenza dell'oggetto

Viene creato ed eseguito un job di controllo dell'esistenza di un oggetto alla volta. Quando si crea un processo, selezionare i nodi di archiviazione e i volumi che si desidera verificare. È inoltre possibile selezionare la coerenza per il lavoro.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Hai garantito che i nodi di storage che desideri controllare siano online. Selezionare **NODES** per visualizzare la tabella dei nodi. Assicurarsi che non venga visualizzata alcuna icona di avviso accanto al nome del nodo per i nodi che si desidera controllare.
- Si è verificato che le seguenti procedure siano **non** in esecuzione sui nodi che si desidera controllare:
  - Espansione della griglia per aggiungere un nodo di storage
  - Decommissionare il nodo di storage
  - Ripristino di un volume di storage guasto
  - Ripristino di un nodo di storage con un disco di sistema guasto
  - Ribilanciamento EC
  - Clone del nodo dell'appliance

Il controllo dell'esistenza degli oggetti non fornisce informazioni utili durante l'esecuzione di queste procedure.

A proposito di questa attività

Il completamento di un processo di verifica dell'esistenza di un oggetto può richiedere giorni o settimane, in base al numero di oggetti nella griglia, ai volumi e ai nodi di storage selezionati e alla coerenza selezionata. È possibile eseguire un solo processo alla volta, ma è possibile selezionare più nodi e volumi di storage contemporaneamente.

Fasi

1. Selezionare **MANUTENZIONE** > **attività** > **controllo dell'esistenza dell'oggetto**.
2. Selezionare **Crea job**. Viene visualizzata la procedura guidata Crea un processo di verifica dell'esistenza di un oggetto.
3. Selezionare i nodi contenenti i volumi che si desidera verificare. Per selezionare tutti i nodi online, selezionare la casella di controllo **Node name** (Nome nodo) nell'intestazione della colonna.

   È possibile eseguire la ricerca in base al nome del nodo o al sito.

Non è possibile selezionare nodi che non sono connessi alla griglia.

4. Selezionare **continua**.
5. Selezionare uno o più volumi per ciascun nodo dell'elenco. È possibile cercare i volumi utilizzando il numero del volume di storage o il nome del nodo.

   Per selezionare tutti i volumi per ciascun nodo selezionato, selezionare la casella di controllo **Storage volume** nell'intestazione della colonna.

6. Selezionare **continua**.
7. Selezionare la coerenza per il lavoro.

   La coerenza determina il numero di copie dei metadati degli oggetti utilizzate per il controllo dell'esistenza dell'oggetto.

   - **Strong-site**: Due copie di metadati in un singolo sito.
   - **Strong-Global**: Due copie di metadati in ogni sito.
   - **Tutti** (impostazione predefinita): Tutte e tre le copie dei metadati di ciascun sito.

     Per ulteriori informazioni sulla coerenza, vedere le descrizioni nella procedura guidata.

8. Selezionare **continua**.
9. Controllare e verificare le selezioni. È possibile selezionare **Previous** (precedente) per passare a una fase precedente della procedura guidata e aggiornare le selezioni.

   Viene generato un job di controllo dell'esistenza di un oggetto che viene eseguito fino a quando non si verifica una delle seguenti condizioni:

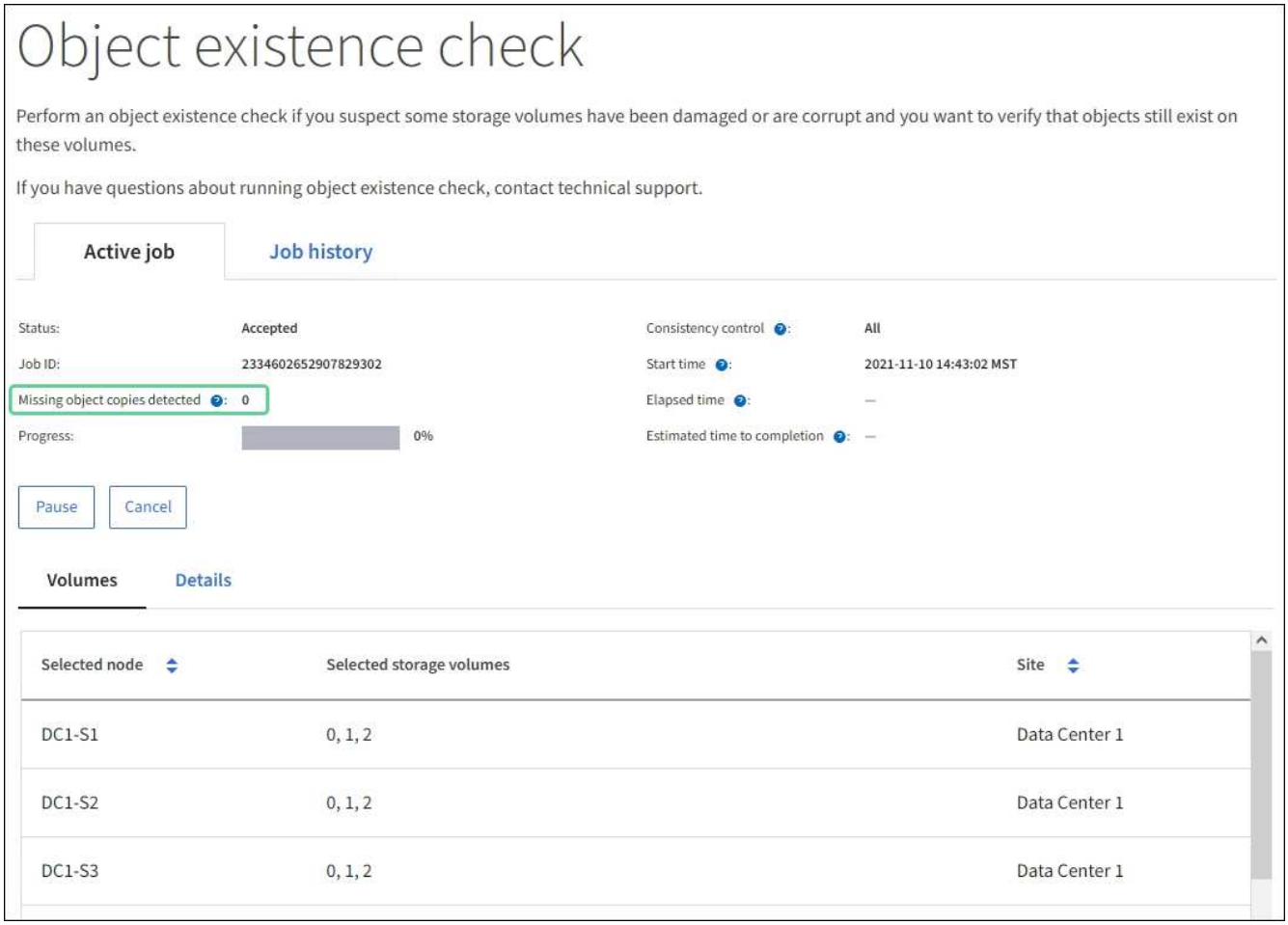
   - Il lavoro viene completato.
   - Il processo viene sospeso o annullato. È possibile riprendere un lavoro che è stato messo in pausa, ma non è possibile riprendere un lavoro che è stato annullato.
   - Il lavoro si blocca. Viene attivato l'avviso **controllo dell'esistenza dell'oggetto bloccato**. Seguire le azioni correttive specificate per l'avviso.
   - Il lavoro non riesce. Viene attivato l'avviso **controllo dell'esistenza dell'oggetto non riuscito**. Seguire le azioni correttive specificate per l'avviso.
   - Viene visualizzato il messaggio "Servizio non disponibile" o "errore interno del server". Dopo un minuto, aggiornare la pagina per continuare a monitorare il lavoro.

     Se necessario, è possibile allontanarsi dalla pagina di controllo dell'esistenza dell'oggetto e tornare indietro per continuare a monitorare il lavoro.

10. Durante l'esecuzione del processo, visualizzare la scheda **lavoro attivo** e annotare il valore di copie oggetto mancanti rilevate.

    Questo valore rappresenta il numero totale di copie mancanti di oggetti replicati e di oggetti con codifica di cancellazione con uno o più frammenti mancanti.

    Se il numero di copie di oggetti mancanti rilevate è superiore a 100, potrebbe esserci un problema con lo storage del nodo di storage.



11. Una volta completato il lavoro, eseguire eventuali azioni aggiuntive richieste:
    - Se le copie oggetto mancanti rilevate sono pari a zero, non sono stati rilevati problemi. Non è richiesta alcuna azione.
    - Se vengono rilevate copie di oggetti mancanti maggiori di zero e l'avviso **oggetti persi** non è stato attivato, tutte le copie mancanti sono state riparate dal sistema. Verificare che eventuali problemi hardware siano stati corretti per evitare danni futuri alle copie degli oggetti.
    - Se le copie degli oggetti mancanti rilevate sono superiori a zero e viene attivato l'avviso **oggetti persi**, l'integrità dei dati potrebbe risentirne. Contattare il supporto tecnico.
    - È possibile analizzare le copie degli oggetti persi utilizzando grep per estrarre i messaggi di audit LLST: `grep LLST audit_file_name`.

      Questa procedura è simile a quella per "analisi degli oggetti smarriti", anche se per le copie di oggetto cercate `LLST` invece di `OLST`.

12. Se è stata selezionata la coerenza globale forte o strong-Site per il lavoro, attendere circa tre settimane per la coerenza dei metadati, quindi rieseguire nuovamente il lavoro sugli stessi volumi.

    Quando StorageGRID ha avuto il tempo di ottenere la coerenza dei metadati per i nodi e i volumi inclusi nel processo, la riesecuzione del processo potrebbe eliminare le copie degli oggetti mancanti segnalate erroneamente o causare il controllo di altre copie degli oggetti in caso di mancata esecuzione.

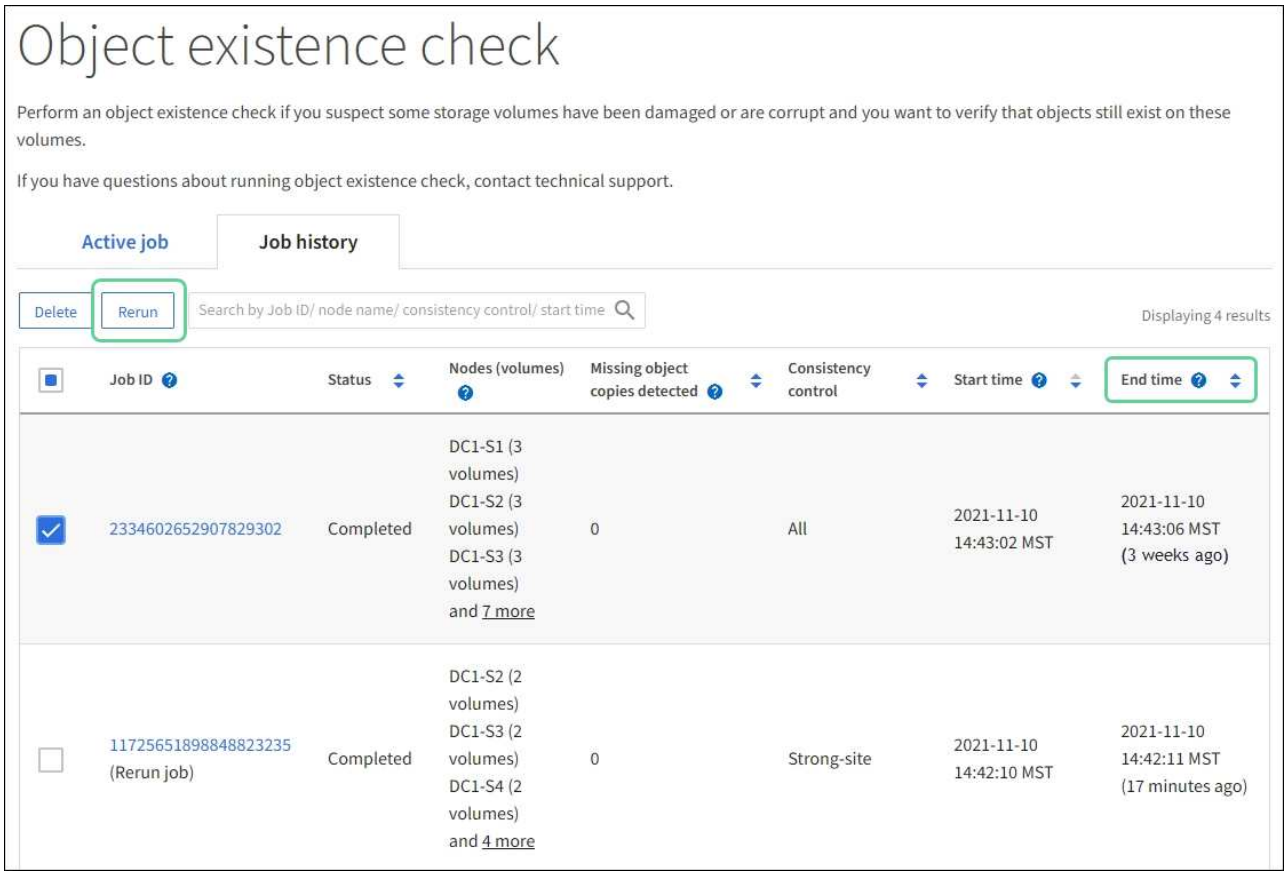
    a. Selezionare **MANUTENZIONE** > **verifica dell'esistenza dell'oggetto** > **Cronologia lavori**.

    b. Determinare quali lavori sono pronti per essere rieseguiti:

i. Esaminare la colonna **ora di fine** per determinare quali lavori sono stati eseguiti più di tre settimane fa.

ii. Per questi lavori, eseguire la scansione della colonna di controllo della coerenza per individuare la presenza di un sito forte o globale forte.

c. Selezionare la casella di controllo per ciascun processo che si desidera rieseguire, quindi selezionare **Rerun**.



d. Nella procedura guidata Riesegui lavori, esaminare i nodi e i volumi selezionati e la coerenza.

e. Quando si è pronti per rieseguire i lavori, selezionare **Rerun**.

Viene visualizzata la scheda lavoro attivo. Tutti i lavori selezionati vengono rieseguiti come un unico lavoro con una consistenza di sito sicuro. Un campo **lavori correlati** nella sezione Dettagli elenca gli ID lavoro per i lavori originali.

Al termine

Se hai ancora dubbi sull'integrità dei dati, vai a **SUPPORT** > **Tools** > **Grid topology** > ***Site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration** > **Main** e aumenta il tasso di verifica in background. La verifica in background verifica la correttezza di tutti i dati degli oggetti memorizzati e ripara eventuali problemi rilevati. L'individuazione e la riparazione di potenziali problemi il più rapidamente possibile riduce il rischio di perdita di dati.

Risoluzione dei problemi S3 - Avviso DIMENSIONE oggetto troppo grande

L'avviso S3 PUT object size too large viene attivato se un tenant tenta un'operazione PutObject non multiparte che supera il limite di dimensione S3 di 5 GiB.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Determinare quali tenant utilizzano oggetti di dimensioni superiori a 5 GiB, in modo da poterli notificare.

Fasi

1. Accedere a **CONFIGURAZIONE** > **monitoraggio** > **server di audit e syslog**.
2. Se le scritture del client sono normali, accedere al registro di controllo:

   a. Invio `ssh admin@primary_Admin_Node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

   e. Passare alla directory in cui si trovano i registri di controllo.

   La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni della destinazione di controllo.

Opzione	Destinazione
Nodi locali (impostazione predefinita)	`/var/local/log/localaudit.log`
Nodi amministrativi/nodi locali	• Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante in questa modalità.
Server syslog esterno	`/var/local/log/localaudit.log`

   In base alle impostazioni della destinazione di controllo, immettere: `cd /var/local/log` O. `/var/local/audit/export/`

   Per ulteriori informazioni, fare riferimento a "Selezionare le destinazioni delle informazioni di audit".

   f. Identificare i tenant che utilizzano oggetti di dimensioni superiori a 5 GiB.

      i. Invio `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

      ii. Per ogni messaggio di audit nei risultati, consultare `S3AI` Per determinare l'ID account tenant. Utilizzare gli altri campi del messaggio per determinare l'indirizzo IP utilizzato dal client, dal bucket e dall'oggetto:

Codice	Descrizione
SAIP	IP di origine
S3AI	ID tenant
S3BK	Bucket
S3KY	Oggetto
CSIZ	Dimensione (byte)

Esempio di risultati del registro di controllo

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"933908492661540043 43"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::933908492661540043 43:root"][SBAI(CSTR):"933908492661540043 43"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Se le scritture del client non sono normali, utilizzare l'ID tenant dell'avviso per identificare il tenant:

   a. Accedere a **SUPPORT** > **Tools** > **Logs**. Raccogliere i log delle applicazioni per il nodo di storage nell'avviso. Specificare 15 minuti prima e dopo l'avviso.

   b. Estrarre il file e accedere a. `bycast.log`:

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. Cercare nel registro `method=PUT` e identificare il client in `clientIP` campo.

      Esempio di bycast.log

      ```
      Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
      2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ:
      EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
      name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
      ```

4. Informare i locatari che la dimensione massima di PutObject è di 5 GiB e di utilizzare caricamenti multiparte per oggetti superiori a 5 GiB.

5. Ignorare l'avviso per una settimana se l'applicazione è stata modificata.

Risolvere i problemi relativi ai dati degli oggetti persi e mancanti

Risoluzione dei problemi relativi ai dati degli oggetti persi e mancanti: Panoramica

Gli oggetti possono essere recuperati per diversi motivi, tra cui le richieste di lettura da un'applicazione client, le verifiche in background dei dati degli oggetti replicati, le rivalutazioni ILM e il ripristino dei dati degli oggetti durante il ripristino di un nodo di storage.

Il sistema StorageGRID utilizza le informazioni sulla posizione nei metadati di un oggetto per determinare da quale posizione recuperare l'oggetto. Se una copia dell'oggetto non viene trovata nella posizione prevista, il sistema tenta di recuperare un'altra copia dell'oggetto da un'altra parte del sistema, supponendo che il criterio ILM contenga una regola per eseguire due o più copie dell'oggetto.

Se il recupero riesce, il sistema StorageGRID sostituisce la copia mancante dell'oggetto. In caso contrario, viene attivato l'avviso **oggetti persi**, come segue:

- Per le copie replicate, se non è possibile recuperare un'altra copia, l'oggetto viene considerato perso e viene attivato l'avviso.
- Per le copie con erasure coding, se non è possibile recuperare una copia dalla posizione prevista, l'attributo copie danneggiate rilevate (ECOR) viene incrementato di uno prima di tentare di recuperare una copia da un'altra posizione. Se non viene trovata alcuna altra copia, viene attivato l'avviso.

Esaminare immediatamente tutti gli avvisi **oggetti persi** per determinare la causa principale della perdita e determinare se l'oggetto potrebbe ancora esistere in un nodo di storage o in un nodo di archivio offline o al momento non disponibile. Vedere "Esaminare gli oggetti persi".

Nel caso in cui i dati degli oggetti senza copie vadano persi, non esiste una soluzione di recovery. Tuttavia, è necessario reimpostare il contatore Lost Objects (oggetti persi) per evitare che oggetti persi noti mascherino eventuali nuovi oggetti persi. Vedere "Ripristinare i conteggi degli oggetti persi e mancanti".

Esaminare gli oggetti persi

Quando viene attivato l'avviso **oggetti persi**, è necessario eseguire un'analisi immediata. Raccogliere informazioni sugli oggetti interessati e contattare il supporto tecnico.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

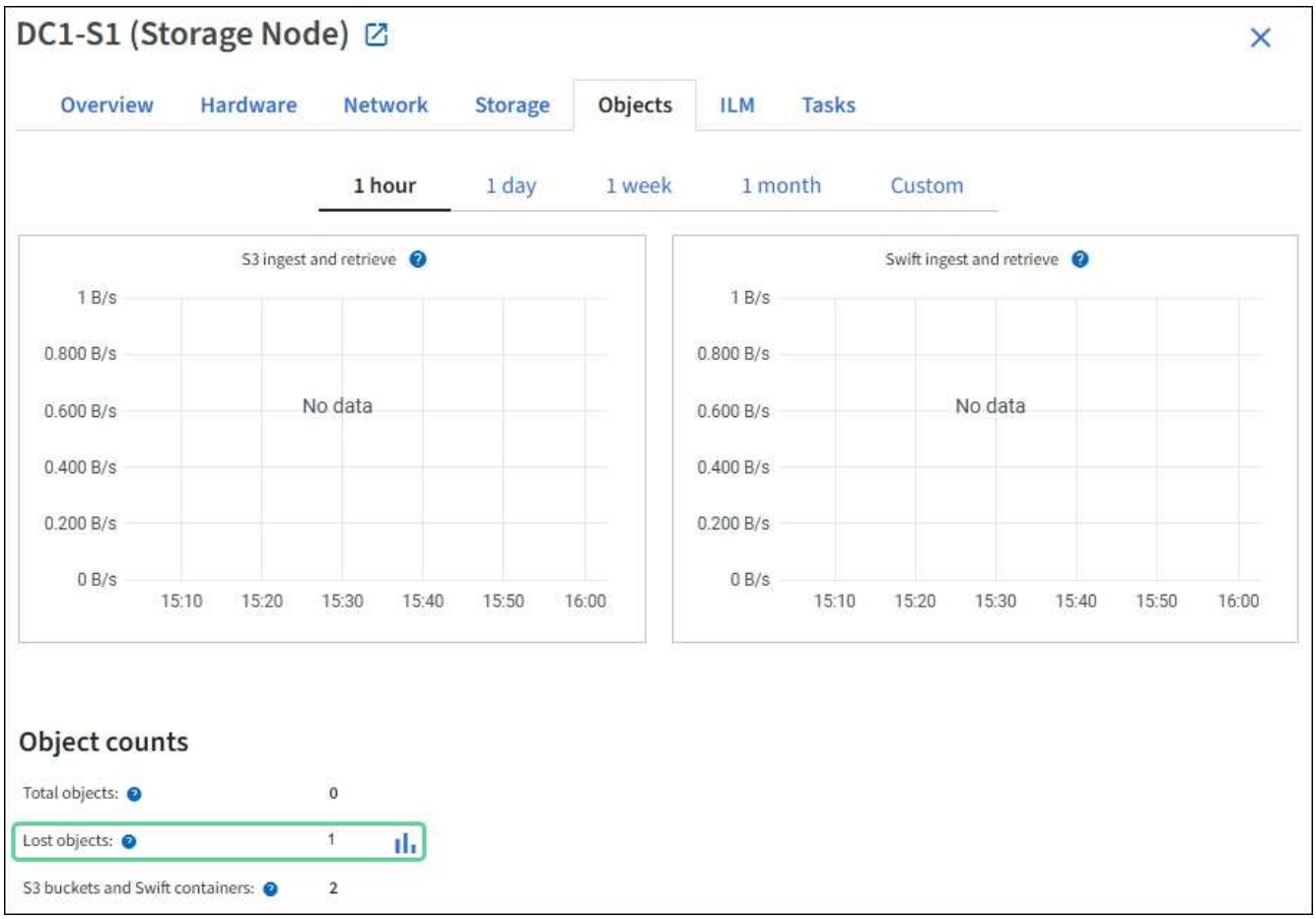
L'avviso **oggetti persi** indica che StorageGRID ritiene che non vi siano copie di un oggetto nella griglia. I dati potrebbero essere stati persi in modo permanente.

Esaminare immediatamente gli avvisi di oggetti smarriti. Potrebbe essere necessario intervenire per evitare ulteriori perdite di dati. In alcuni casi, potrebbe essere possibile ripristinare un oggetto perso se si esegue un'azione rapida.

Fasi

1. Selezionare **NODI**.
2. Selezionare ***Storage Node*** > **Objects**.
3. Esaminare il numero di oggetti persi visualizzato nella tabella dei conteggi degli oggetti.

   Questo numero indica il numero totale di oggetti che il nodo della griglia rileva come mancanti dall'intero sistema StorageGRID. Il valore è la somma dei contatori Lost Objects del componente Data Store all'interno dei servizi LDR e DDS.



4. Da un nodo Admin, "accedere al registro di controllo" Per determinare l'identificatore univoco (UUID) dell'oggetto che ha attivato l'avviso **oggetti persi**:
   a. Accedere al nodo Grid:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file.
      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
   b. Passare alla directory in cui si trovano i registri di controllo.

      La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni della destinazione di controllo.

Opzione	Destinazione
Nodi locali (impostazione predefinita)	`/var/local/log/localaudit.log`
Nodi amministrativi/nodi locali	• Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante in questa modalità.
Server syslog esterno	`/var/local/log/localaudit.log`

In base alle impostazioni della destinazione di controllo, immettere: `cd /var/local/log` O. `/var/local/audit/export/`

Per ulteriori informazioni, fare riferimento a "Selezionare le destinazioni delle informazioni di audit".

c. Utilizzare grep per estrarre i messaggi di audit OLST (Object Lost). Inserire: `grep OLST audit_file_name`

d. Annotare il valore UUID incluso nel messaggio.

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-
AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Utilizzare `ObjectByUUID` Comando per trovare l'oggetto in base al relativo identificatore (UUID), quindi determinare se i dati sono a rischio.

a. Utilizzare SSH per accedere a qualsiasi nodo storage. Quindi accedere alla console LDR digitando "telnet 0 1402".

b. Inserire: `/proc/OBRP/ObjectByUUID UUID_value`

In questo primo esempio, l'oggetto con `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` ha due posizioni elencate.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
```

```
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
```

```
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

Nel secondo esempio, l'oggetto con `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` non ha posizioni elencate.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. Esaminare l'output di /proc/OBRP/ObjectByUUID e intraprendere l'azione appropriata:

Metadati	Conclusione
Nessun oggetto trovato ("ERRORE":"")	Se l'oggetto non viene trovato, viene visualizzato il messaggio "ERROR":". Se l'oggetto non viene trovato, è possibile azzerare il numero di **oggetti persi** per eliminare l'avviso. La mancanza di un oggetto indica che l'oggetto è stato intenzionalmente cancellato.
Posizioni > 0	Se nell'output sono presenti posizioni, l'avviso **oggetti persi** potrebbe essere un falso positivo. Verificare che gli oggetti esistano. Utilizzare l'ID nodo e il percorso del file elencati nell'output per confermare che il file a oggetti si trova nella posizione indicata. (La procedura per "ricerca di oggetti potenzialmente persi" Spiega come utilizzare l'ID nodo per trovare il nodo di storage corretto). Se gli oggetti sono presenti, è possibile ripristinare il numero di **oggetti persi** per cancellare l'avviso.
Posizioni = 0	Se nell'output non sono presenti posizioni, l'oggetto potrebbe essere mancante. Puoi provare "cercare e ripristinare l'oggetto" oppure puoi contattare il supporto tecnico. Il supporto tecnico potrebbe richiedere di determinare se è in corso una procedura di ripristino dello storage. Consultare le informazioni su "Ripristino dei dati degli oggetti mediante Grid Manager" e. "ripristino dei dati degli oggetti in un volume di storage".

Cercare e ripristinare oggetti potenzialmente persi

Potrebbe essere possibile trovare e ripristinare oggetti che hanno attivato un allarme Lost Objects (LOST Objects, oggetti persi) e un avviso **Object Lost** e che sono stati identificati come potenzialmente persi.

Prima di iniziare

- Si dispone dell'UUID di qualsiasi oggetto perso, come identificato nella "Esaminare gli oggetti persi".
- Hai il `Passwords.txt` file.

A proposito di questa attività

È possibile seguire questa procedura per cercare copie replicate dell'oggetto perso in un altro punto della griglia. Nella maggior parte dei casi, l'oggetto perso non viene trovato. Tuttavia, in alcuni casi, potrebbe essere possibile trovare e ripristinare un oggetto replicato perso se si esegue un'azione rapida.

Contattare il supporto tecnico per assistenza con questa procedura.

Fasi

1. Da un nodo amministratore, cercare nei registri di controllo le posizioni possibili degli oggetti:

a. Accedere al nodo Grid:

   i. Immettere il seguente comando: `ssh admin@grid_node_IP`

   ii. Immettere la password elencata in `Passwords.txt` file.

   iii. Immettere il seguente comando per passare a root: `su -`

   iv. Immettere la password elencata in `Passwords.txt` file.
   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

b. passare alla directory in cui si trovano i registri di controllo.

   La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni della destinazione di controllo.

Opzione	Destinazione
Nodi locali (impostazione predefinita)	`/var/local/log/localaudit.log`
Nodi amministrativi/nodi locali	• Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante in questa modalità.
Server syslog esterno	`/var/local/log/localaudit.log`

   In base alle impostazioni della destinazione di controllo, immettere: `cd /var/local/log` O. `/var/local/audit/export/`

   Per ulteriori informazioni, fare riferimento a "Selezionare le destinazioni delle informazioni di audit".

c. Utilizzare grep per estrarre "messaggi di audit associati all'oggetto potenzialmente perso" e inviarli a un file di output. Inserire: `grep uuid-valueaudit_file_name > output_file_name`

   Ad esempio:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_lost_object.txt
```

d. Utilizzare grep per estrarre i messaggi di controllo LLST (Location Lost) da questo file di output. Inserire: `grep LLST output_file_name`

   Ad esempio:

```
Admin: # grep LLST /var/local/tmp/messages_about_lost_objects.txt
```

   Un messaggio di controllo LLST è simile a questo messaggio di esempio.

```
[AUDT:[NOID(UI32):12448208][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD(CSTR):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
868710831907434 09]]
```

e. Individuare il campo PCLD e IL campo NOID nel messaggio LLST.

Se presente, il valore di PCLD è il percorso completo sul disco verso la copia dell'oggetto replicato mancante. IL valore DI NOID è l'id del nodo dell'LDR in cui è possibile trovare una copia dell'oggetto.

Se si trova una posizione dell'oggetto, potrebbe essere possibile ripristinarlo.

a. Trova il nodo di storage associato a questo ID nodo LDR. In Grid Manager, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Data Center*** > ***Storage Node*** > **LDR**.

L'ID nodo per il servizio LDR si trova nella tabella Node Information (informazioni nodo). Esaminare le informazioni relative a ciascun nodo di storage fino a individuare quello che ospita questo LDR.

2. Determinare se l'oggetto esiste sul nodo di storage indicato nel messaggio di audit:

a. Accedere al nodo Grid:

i. Immettere il seguente comando: `ssh admin@grid_node_IP`

ii. Immettere la password elencata in `Passwords.txt` file.

iii. Immettere il seguente comando per passare a root: `su -`

iv. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

b. Determinare se il percorso del file per l'oggetto esiste.

Per il percorso file dell'oggetto, utilizzare il valore PCLD del messaggio di audit LLST.

Ad esempio, immettere:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Racchiudere sempre il percorso del file oggetto tra virgolette singole nei comandi per escapire eventuali caratteri speciali.

- Se il percorso dell'oggetto non viene trovato, l'oggetto viene perso e non può essere ripristinato utilizzando questa procedura. Contattare il supporto tecnico.
- Se viene trovato il percorso dell'oggetto, passare alla fase successiva. È possibile tentare di ripristinare l'oggetto trovato in StorageGRID.

3. Se il percorso dell'oggetto è stato trovato, tentare di ripristinare l'oggetto in StorageGRID:
   a. Dallo stesso nodo di storage, modificare la proprietà del file a oggetti in modo che possa essere gestito da StorageGRID. Inserire: `chown ldr-user:bycast 'file_path_of_object'`
   b. Utilizzare SSH per accedere a qualsiasi nodo storage. Quindi accedere alla console LDR digitando "telnet 0 1402".
   c. Inserire: `cd /proc/STOR`
   d. Inserire: `Object_Found 'file_path_of_object'`

      Ad esempio, immettere:

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      Emissione di `Object\_Found` il comando notifica alla griglia la posizione dell'oggetto. Attiva inoltre i criteri ILM attivi, che eseguono copie aggiuntive come specificato in ciascun criterio.

      > Se il nodo di storage in cui è stato trovato l'oggetto non è in linea, è possibile copiare l'oggetto in qualsiasi nodo di storage in linea. Posizionare l'oggetto in qualsiasi directory /var/local/rangedb del nodo di storage online. Quindi, eseguire il `Object\_Found` utilizzando il percorso del file all'oggetto.

      - Se l'oggetto non può essere ripristinato, il `Object\_Found` comando non riuscito. Contattare il supporto tecnico.
      - Se l'oggetto è stato ripristinato correttamente in StorageGRID, viene visualizzato un messaggio di esito positivo. Ad esempio:

        ```
        ade 12448208: /proc/STOR > Object_Found
        '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

        ade 12448208: /proc/STOR > Object found succeeded.
        First packet of file was valid. Extracted key: 38186FE53E3C49A5
        Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
        '/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
        ```

        Passare alla fase successiva.

4. Se l'oggetto è stato ripristinato correttamente in StorageGRID, verificare che siano state create nuove posizioni.
   a. Inserire: `cd /proc/OBRP`
   b. Inserire: `ObjectByUUID UUID_value`

      L'esempio seguente mostra che sono presenti due posizioni per l'oggetto con UUID 926026C4-00A4-449B-AC72-BCCA72DD1311.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
```

```
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
```

```
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

a. Disconnettersi dalla console LDR. Inserire: `exit`

5. Da un nodo di amministrazione, cercare nei registri di controllo il messaggio di audit ORLM relativo a questo oggetto per confermare che ILM (Information Lifecycle Management) ha inserito le copie come richiesto.

   a. Accedere al nodo Grid:

      i. Immettere il seguente comando: `ssh admin@grid_node_IP`

      ii. Immettere la password elencata in `Passwords.txt` file.

      iii. Immettere il seguente comando per passare a root: `su -`

      iv. Immettere la password elencata in `Passwords.txt` file.
      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

   b. Passare alla directory in cui si trovano i registri di controllo. Fare riferimento alla sottosezione 1. b.

   c. Utilizzare grep per estrarre i messaggi di audit associati all'oggetto in un file di output. Inserire: `grep uuid-valueaudit_file_name > output_file_name`

      Ad esempio:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      /var/local/tmp/messages_about_restored_object.txt
      ```

   d. Utilizzare grep per estrarre i messaggi di audit ORLM (Object Rules Met) da questo file di output. Inserire: `grep ORLM output_file_name`

      Ad esempio:

      ```
      Admin: # grep ORLM /var/local/tmp/messages_about_restored_object.txt
      ```

      Un messaggio di controllo ORLM è simile a questo messaggio di esempio.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Individuare il campo LOCS (POSIZIONI) nel messaggio di audit.

   Se presente, il valore di CLDI in LOCS è l'ID del nodo e l'ID del volume in cui è stata creata una copia dell'oggetto. Questo messaggio indica che l'ILM è stato applicato e che sono state create due copie di oggetti in due posizioni nella griglia.

6. "Ripristinare i conteggi degli oggetti persi e mancanti" In Grid Manager.

Ripristinare i conteggi degli oggetti persi e mancanti

Dopo aver esaminato il sistema StorageGRID e aver verificato che tutti gli oggetti persi registrati vengano persi in modo permanente o che si tratti di un falso allarme, è possibile azzerare il valore dell'attributo oggetti persi.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

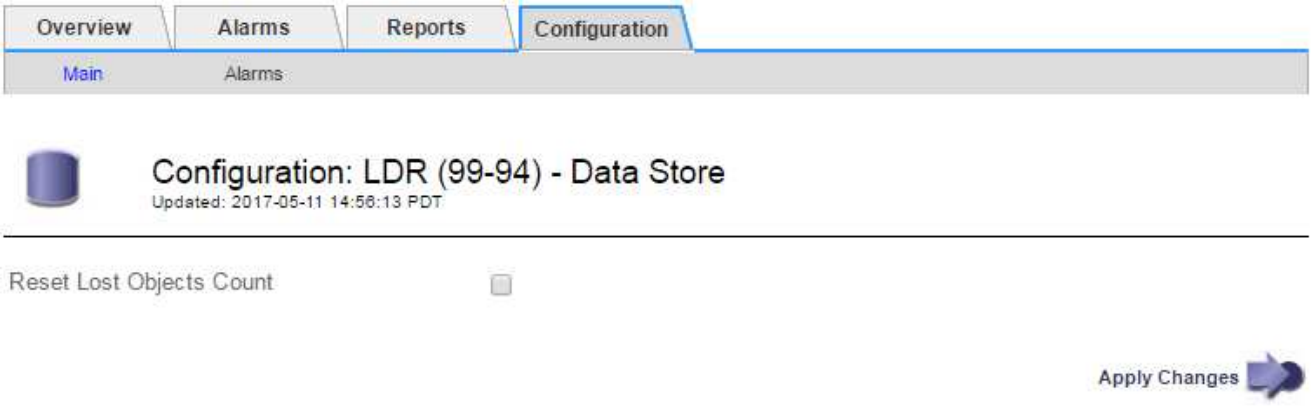
È possibile reimpostare il contatore Lost Objects da una delle seguenti pagine:

- **SUPPORT** > **Tools** > **Grid topology** > ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Overview** > **Main**
- **SUPPORTO** > **Strumenti** > **topologia griglia** > ***Sito*** > ***nodo di archiviazione*** > **DDS** > **Archivio dati** > **Panoramica** > **principale**

Queste istruzioni mostrano come azzerare il contatore dalla pagina **LDR** > **Data Store**.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Configuration** per il nodo di storage che presenta l'avviso **Objects Lost** o l'allarme LOST.
3. Selezionare **Reset Lost Objects Count** (Ripristina conteggio oggetti persi).



4. Fare clic su **Applica modifiche**.

   L'attributo Lost Objects (oggetti persi) viene reimpostato su 0 e l'avviso **Objects lost** (oggetti persi) e l'allarme LOST (PERSO) vengono eliminati, che possono richiedere alcuni minuti.

5. Facoltativamente, reimpostare altri valori degli attributi correlati che potrebbero essere stati incrementati durante il processo di identificazione dell'oggetto perso.

   a. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Erasure Coding** > **Configuration**.

   b. Selezionare **Reset Reads Failure Count** e **Reset corrotto copies Detected Count**.

   c. Fare clic su **Applica modifiche**.

   d. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration**.

   e. Selezionare **Reset Missing Objects Count** e **Reset Corrupt Objects Count**.

   f. Se si è certi che gli oggetti in quarantena non siano necessari, selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena).

      Gli oggetti in quarantena vengono creati quando la verifica in background identifica una copia di oggetti replicati corrotta. Nella maggior parte dei casi, StorageGRID sostituisce automaticamente l'oggetto corrotto ed è sicuro eliminare gli oggetti in quarantena. Tuttavia, se viene attivato l'allarme **oggetti persi** o L'allarme PERSO, il supporto tecnico potrebbe voler accedere agli oggetti in quarantena.

   g. Fare clic su **Applica modifiche**.

   Dopo aver fatto clic su **Apply Changes** (Applica modifiche), il ripristino degli attributi può richiedere alcuni istanti.

Risolvere i problemi relativi all'avviso di storage dei dati a oggetti in esaurimento

L'avviso **Low Object Data Storage** monitora lo spazio disponibile per memorizzare i dati degli oggetti su ciascun nodo di storage.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

L'avviso **archiviazione dati oggetto bassa** viene attivato quando la quantità totale di dati oggetto replicati e con erasure coding su un nodo di archiviazione soddisfa una delle condizioni configurate nella regola di avviso.

Per impostazione predefinita, viene attivato un avviso importante quando questa condizione viene valutata come true:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

In questa condizione:

- `storagegrid_storage_utilization_data_bytes` È una stima delle dimensioni totali dei dati di oggetti replicati e con erasure coding per un nodo storage.
- `storagegrid_storage_utilization_usable_space_bytes` È la quantità totale di spazio di storage a oggetti rimanente per un nodo di storage.

Se viene attivato un avviso **Low Object Data Storage** maggiore o minore, è necessario eseguire una procedura di espansione il prima possibile.

Fasi

1. Selezionare **ALERTS** > **current**.

   Viene visualizzata la pagina Avvisi.

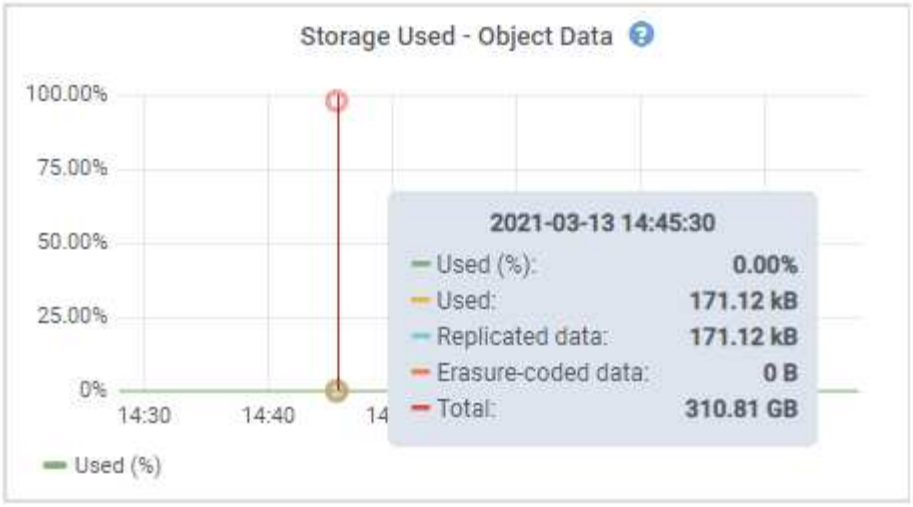
2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low Object Data Storage**, se necessario, e selezionare l'avviso che si desidera visualizzare.

   Selezionare l'avviso, non l'intestazione di un gruppo di avvisi.

3. Esaminare i dettagli nella finestra di dialogo e prendere nota di quanto segue:
   - Tempo di attivazione
   - Il nome del sito e del nodo
   - I valori correnti delle metriche per questo avviso
4. Selezionare **NODES** > ***Storage Node or Site*** > **Storage**.
5. Posizionare il cursore sul grafico Storage Used - Object Data (Storage utilizzato - dati oggetto).

   Vengono visualizzati i seguenti valori:

   - **Used (%)**: Percentuale dello spazio utilizzabile totale utilizzato per i dati dell'oggetto.
   - **Used**: Quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
   - **Dati replicati**: Stima della quantità di dati degli oggetti replicati su questo nodo, sito o griglia.
   - **Erasure-coded data**: Stima della quantità di dati dell'oggetto con codifica di cancellazione su questo nodo, sito o griglia.
   - **Total**: Quantità totale di spazio utilizzabile su questo nodo, sito o griglia.
     Il valore utilizzato è `storagegrid_storage_utilization_data_bytes` metrico.



6. Selezionare i controlli dell'ora sopra il grafico per visualizzare l'utilizzo dello storage in diversi periodi di tempo.

   L'utilizzo dello storage nel tempo può aiutarti a capire la quantità di storage utilizzata prima e dopo l'attivazione dell'avviso e può aiutarti a stimare il tempo necessario per lo spazio rimanente del nodo.

7. Il più presto possibile, "aggiungere capacità di storage" alla tua griglia.

   È possibile aggiungere volumi di storage (LUN) ai nodi di storage esistenti oppure aggiungere nuovi nodi di storage.

   Per ulteriori informazioni, vedere "Gestire nodi storage completi".

Informazioni correlate

"Risoluzione dei problemi relativi all'allarme dello stato dello storage (SST) (legacy)"

Risolvere i problemi relativi agli avvisi di override del watermark di sola lettura bassa

Se si utilizzano valori personalizzati per le filigrane dei volumi di storage, potrebbe essere necessario risolvere l'avviso **bassa sostituzione filigrana di sola lettura**. Se possibile, aggiornare il sistema per iniziare a utilizzare i valori ottimizzati.

Nelle release precedenti, le tre "filigrane dei volumi di storage" Erano impostazioni globali e n. 8212; gli stessi valori applicati a ogni volume di storage su ogni nodo di storage. A partire da StorageGRID 11.6, il software può ottimizzare queste filigrane per ogni volume di storage, in base alle dimensioni del nodo di storage e alla capacità relativa del volume.

Quando si esegue l'aggiornamento a StorageGRID 11.6 o versioni successive, le filigrane ottimizzate di sola lettura e di lettura/scrittura vengono applicate automaticamente a tutti i volumi di storage, a meno che non si verifichino le seguenti condizioni:

- Il sistema è vicino alla capacità e non è in grado di accettare nuovi dati se sono state applicate filigrane ottimizzate. In questo caso, StorageGRID non modificherà le impostazioni della filigrana.
- In precedenza, le filigrane dei volumi di storage sono state impostate su un valore personalizzato. StorageGRID non sovrascrive le impostazioni personalizzate del watermark con valori ottimizzati. Tuttavia, StorageGRID potrebbe attivare l'avviso **override filigrana di sola lettura bassa** se il valore personalizzato

per la filigrana di sola lettura morbida del volume di storage è troppo piccolo.

Comprendere l'avviso

Se si utilizzano valori personalizzati per le filigrane dei volumi di storage, l'avviso **Low Read-only watermark override** potrebbe essere attivato per uno o più nodi di storage.

Ogni istanza dell'avviso indica che il valore personalizzato di **Storage Volume Soft Read-Only Watermark** è inferiore al valore minimo ottimizzato per quel nodo di storage. Se si continua a utilizzare l'impostazione personalizzata, lo spazio del nodo di storage potrebbe essere molto basso prima di poter passare in sicurezza allo stato di sola lettura. Alcuni volumi di storage potrebbero diventare inaccessibili (automaticamente smontati) quando il nodo raggiunge la capacità.

Ad esempio, si supponga di aver precedentemente impostato la filigrana di sola lettura **Storage Volume Soft** su 5 GB. Supponiamo ora che StorageGRID abbia calcolato i seguenti valori ottimizzati per i quattro volumi di storage nel nodo di storage A:

Volume 0	12 GB
Volume 1	12 GB
Volume 2	11 GB
Volume 3	15 GB

L'avviso **Low Read-only watermark override** viene attivato per il nodo di storage A perché il watermark personalizzato (5 GB) è inferiore al valore minimo ottimizzato per tutti i volumi in quel nodo (11 GB). Se si continua a utilizzare l'impostazione personalizzata, lo spazio del nodo potrebbe essere estremamente ridotto prima di poter passare in sicurezza allo stato di sola lettura.

Risolvere l'avviso

Seguire questa procedura se sono stati attivati uno o più avvisi **Low Read-only watermark override**. È inoltre possibile utilizzare queste istruzioni se si utilizzano impostazioni personalizzate per la filigrana e si desidera iniziare a utilizzare impostazioni ottimizzate anche se non sono stati attivati avvisi.

Prima di iniziare

- L'aggiornamento a StorageGRID 11.6 o versione successiva è stato completato.
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

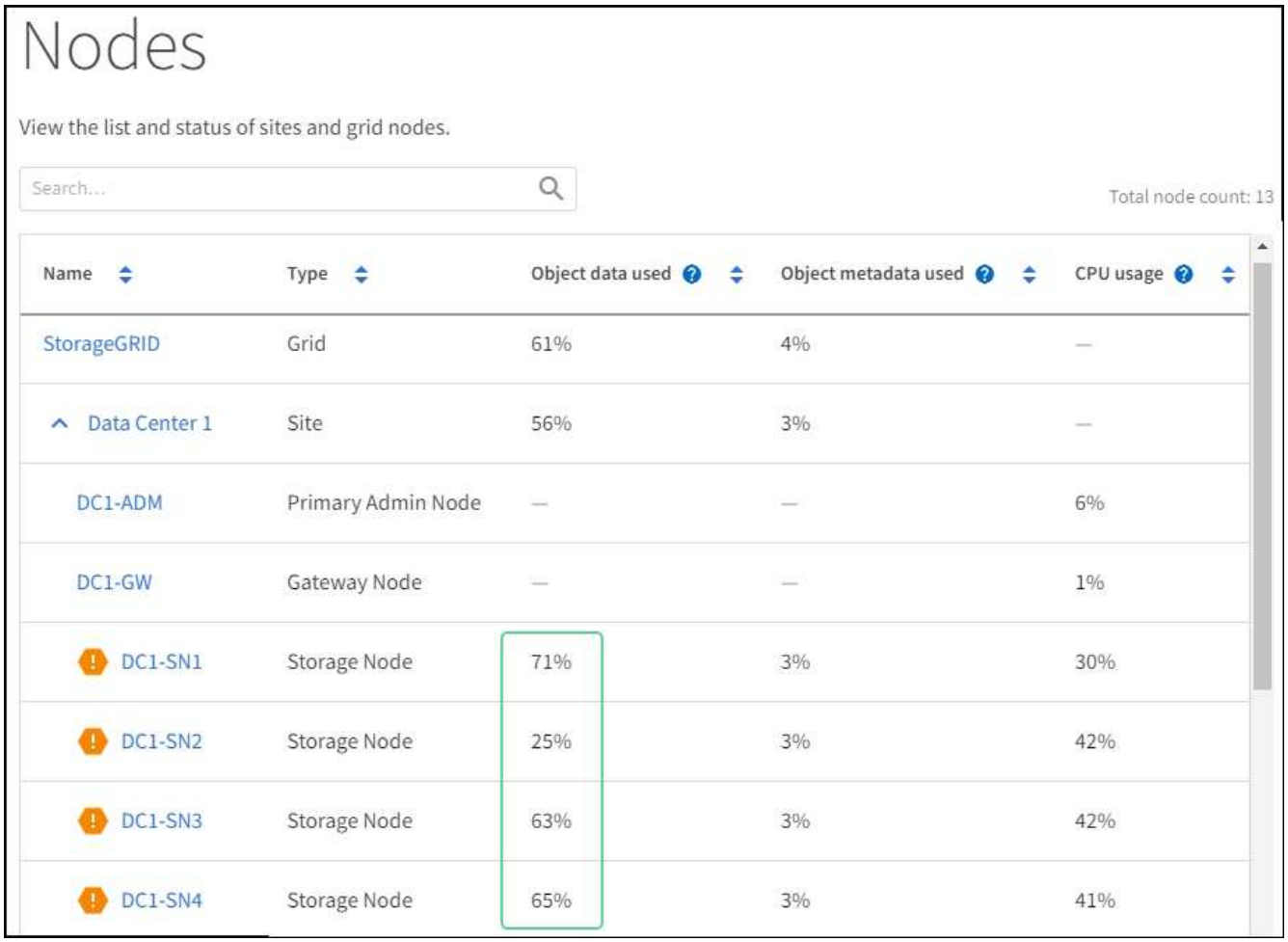
È possibile risolvere l'avviso **deroga filigrana di sola lettura bassa** aggiornando le impostazioni di filigrana personalizzate con le nuove sostituzioni della filigrana. Tuttavia, se uno o più nodi di storage sono quasi pieni o si hanno requisiti ILM speciali, è necessario prima visualizzare le filigrane di storage ottimizzate e determinare se è sicuro utilizzarle.

Valutare l'utilizzo dei dati a oggetti per l'intero grid

Fasi

1. Selezionare **NODI**.

2. Per ogni sito nella griglia, espandere l'elenco dei nodi.
3. Esaminare i valori percentuali mostrati nella colonna **dati oggetto utilizzati** per ciascun nodo di storage in ogni sito.



4. Seguire la procedura appropriata:
   a. Se nessuno dei nodi di storage è quasi pieno (ad esempio, tutti i valori **dati oggetto utilizzati** sono inferiori al 80%), è possibile iniziare a utilizzare le impostazioni di override. Passare a. Utilizzare filigrane ottimizzate.
   b. Se le regole ILM utilizzano un comportamento di acquisizione rigoroso o se i pool di storage specifici sono quasi completi, eseguire i passaggi descritti in Visualizza filigrane di storage ottimizzate e. Determinare se è possibile utilizzare filigrane ottimizzate.

Visualizza filigrane di memorizzazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati che ha calcolato per la filigrana di sola lettura del volume di storage **Soft Read-only**. È possibile visualizzare i valori minimi e massimi ottimizzati per ciascun nodo di storage nella griglia.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Metrics**.
2. Nella sezione Prometheus, selezionare il collegamento per accedere all'interfaccia utente Prometheus.
3. Per visualizzare la filigrana minima di sola lettura soft consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore minimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage. Se questo valore è superiore all'impostazione personalizzata per **Storage Volume Soft Read-Only Watermark**, viene attivato l'avviso **Low Read-only watermark override** per il nodo di storage.

4. Per visualizzare la filigrana di sola lettura soft massima consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore massimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage.

5. Nota sul valore massimo ottimizzato per ciascun nodo di storage.

[[determina-filigrane ottimizzate]]determinare se è possibile utilizzare filigrane ottimizzate

Fasi

1. Selezionare **NODI**.
2. Ripetere questi passaggi per ogni nodo di storage online:
   a. Selezionare ***Storage Node*** > **Storage**.
   b. Scorrere verso il basso fino alla tabella degli archivi di oggetti.
   c. Confrontare il valore **Available** per ciascun archivio di oggetti (volume) con il watermark ottimizzato massimo annotato per quel nodo di storage.
3. Se almeno un volume su ogni nodo di storage online ha più spazio disponibile rispetto al watermark ottimizzato massimo per quel nodo, visitare il sito Web Utilizzare filigrane ottimizzate per iniziare a utilizzare le filigrane ottimizzate.

   In caso contrario, espandere la griglia il prima possibile. Entrambi "aggiungere volumi di storage" a un nodo esistente o. "Aggiungere nuovi nodi di storage". Quindi, passare a. Utilizzare filigrane ottimizzate per aggiornare le impostazioni della filigrana.

4. Se è necessario continuare a utilizzare valori personalizzati per le filigrane del volume di storage, "silenzio" oppure "disattiva" L'avviso **deroga filigrana di sola lettura bassa**.

> Gli stessi valori di watermark personalizzati vengono applicati a ogni volume di storage su ogni nodo di storage. L'utilizzo di valori inferiori a quelli consigliati per le filigrane dei volumi di storage potrebbe causare l'inaccessibilità di alcuni volumi di storage (automaticamente smontati) quando il nodo raggiunge la capacità.

utilizza filigrane ottimizzate

Fasi

1. Andare a **SUPPORT** > **other** > **Storage Watermarks**.
2. Selezionare la casella di controllo **Usa valori ottimizzati**.
3. Selezionare **Salva**.

Le impostazioni ottimizzate del watermark del volume di storage sono ora attive per ciascun volume di storage,

in base alle dimensioni del nodo di storage e alla capacità relativa del volume.

Risolvere i problemi relativi all'allarme Storage Status (SST)

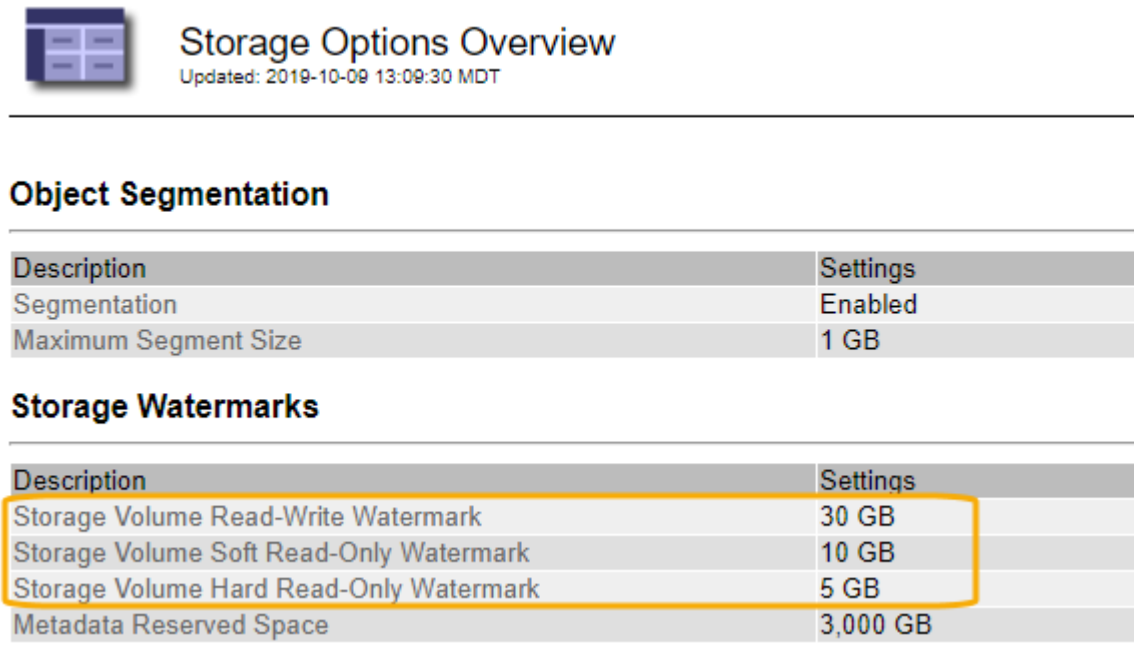
L'allarme Storage Status (SST) viene attivato se un nodo di storage non dispone di spazio libero sufficiente per lo storage a oggetti.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

L'allarme SSTS (Storage Status) viene attivato a livello di Notice quando la quantità di spazio libero su ogni volume in un nodo di storage scende al di sotto del valore del watermark Storage Volume Soft Read Only (**CONFIGURATION** > **System** > **Storage options**).



Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

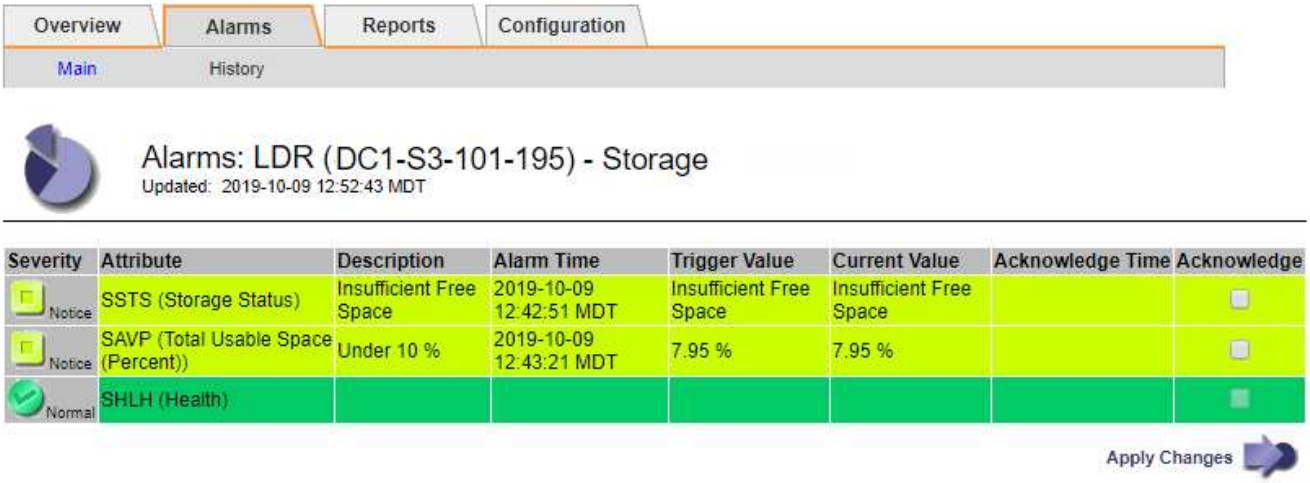
Ad esempio, si supponga che la filigrana Storage Volume Soft Read-Only sia impostata su 10 GB, che è il valore predefinito. L'allarme SSTS viene attivato se su ciascun volume di storage nel nodo di storage rimangono meno di 10 GB di spazio utilizzabile. Se uno dei volumi dispone di almeno 10 GB di spazio disponibile, l'allarme non viene attivato.

Se è stato attivato un allarme SSTS, è possibile seguire questa procedura per comprendere meglio il problema.

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.
2. Dalla colonna Service (Servizio), selezionare il data center, il nodo e il servizio associati all'allarme SSTS.

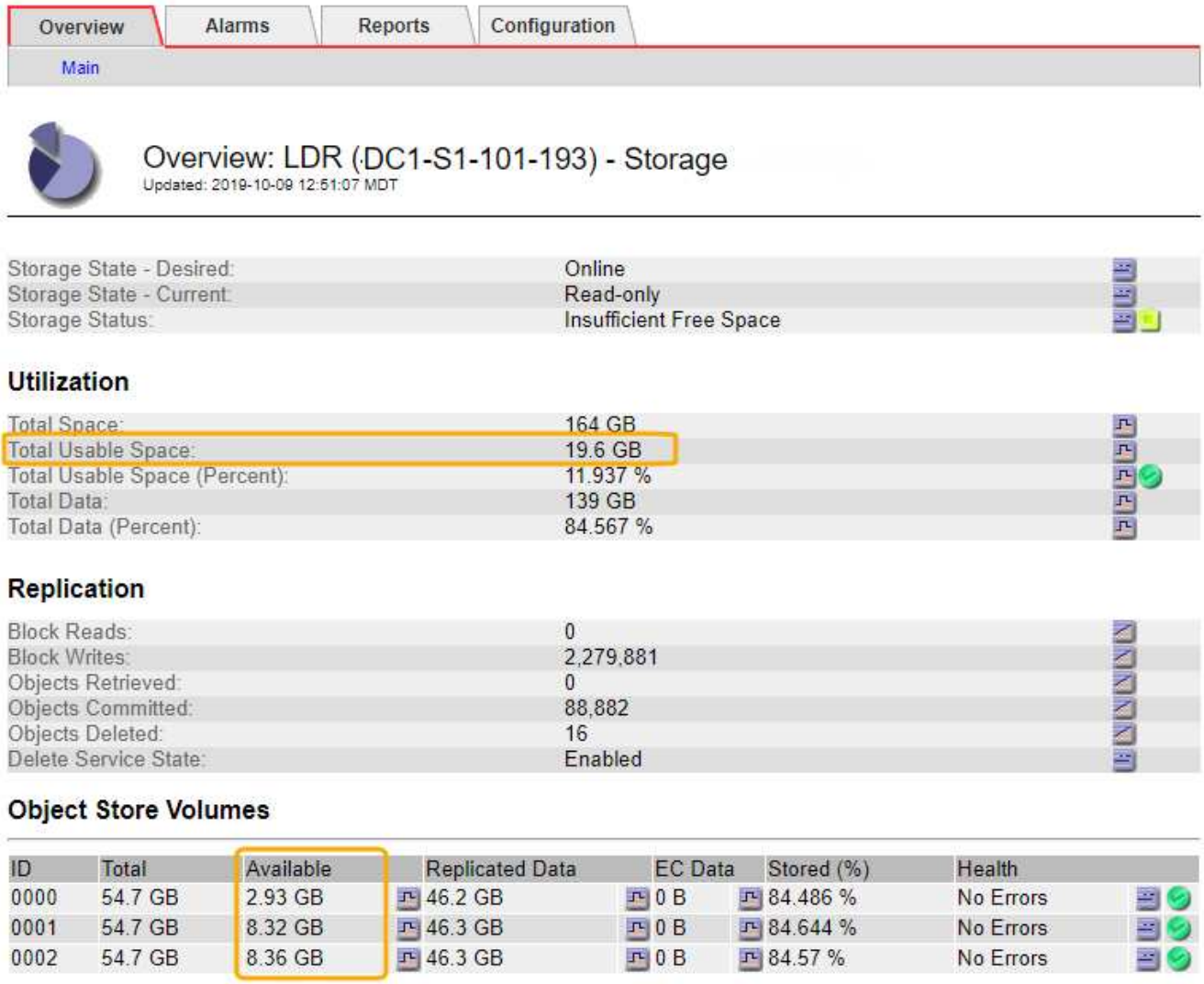
   Viene visualizzata la pagina Grid Topology (topologia griglia). La scheda Allarmi mostra gli allarmi attivi per il nodo e il servizio selezionato.



In questo esempio, gli allarmi SST (Storage Status) e SAVP (Total usable Space (Percent)) sono stati attivati a livello di notifica.

> In genere, sia l'allarme SSTS che l'allarme SAVP vengono attivati circa contemporaneamente; tuttavia, l'attivazione di entrambi gli allarmi dipende dall'impostazione del watermark in GB e dall'impostazione dell'allarme SAVP in percentuale.

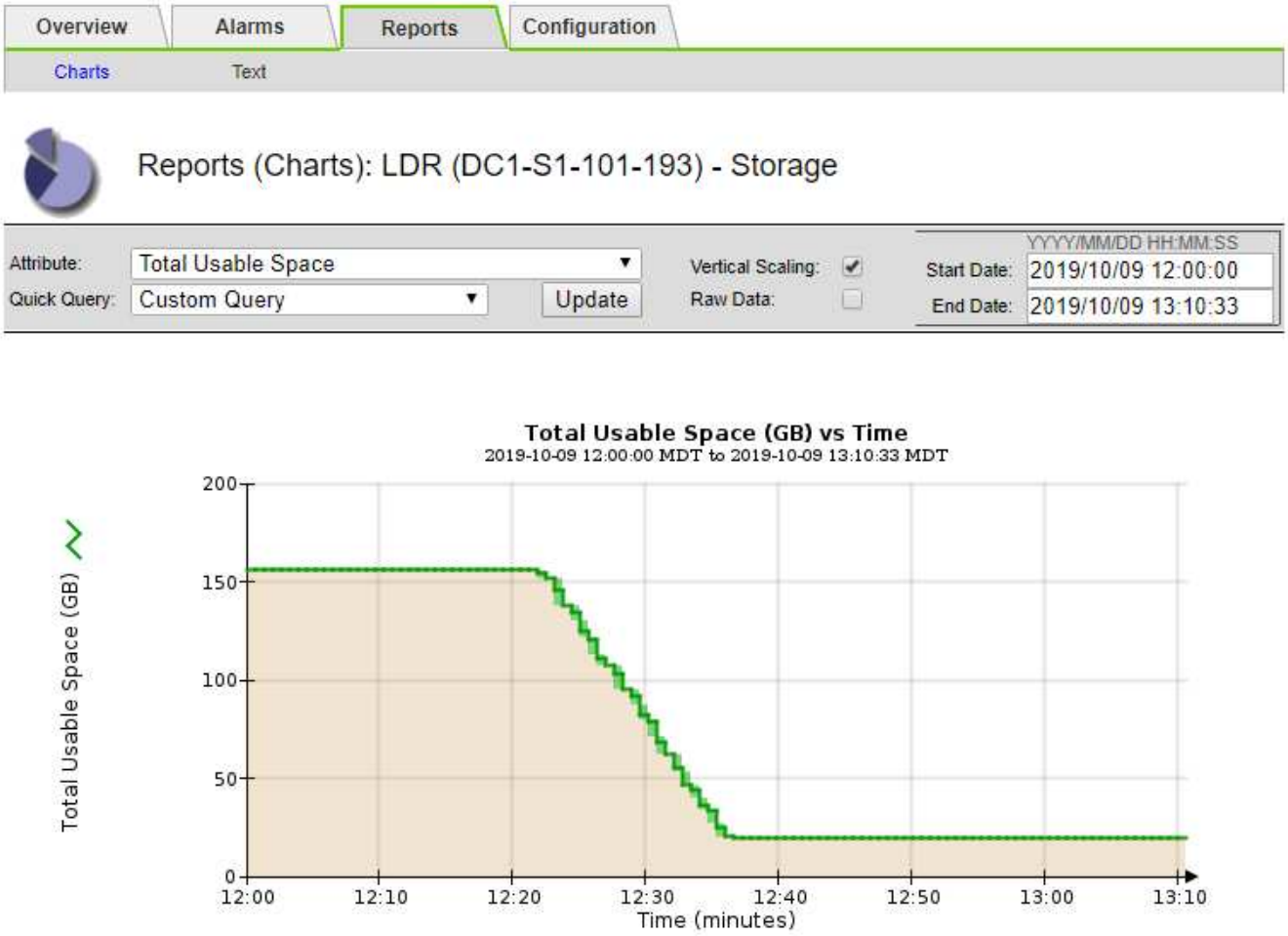
3. Per determinare la quantità di spazio utilizzabile effettivamente disponibile, selezionare **LDR** > **Storage** > **Overview** e individuare l'attributo Total Usable Space (STAS).



In questo esempio, rimangono disponibili solo 19.6 GB dei 164 GB di spazio su questo nodo di storage. Si noti che il valore totale è la somma dei valori **Available** per i tre volumi dell'archivio di oggetti. L'allarme SSTS è stato attivato perché ciascuno dei tre volumi di storage aveva meno di 10 GB di spazio disponibile.

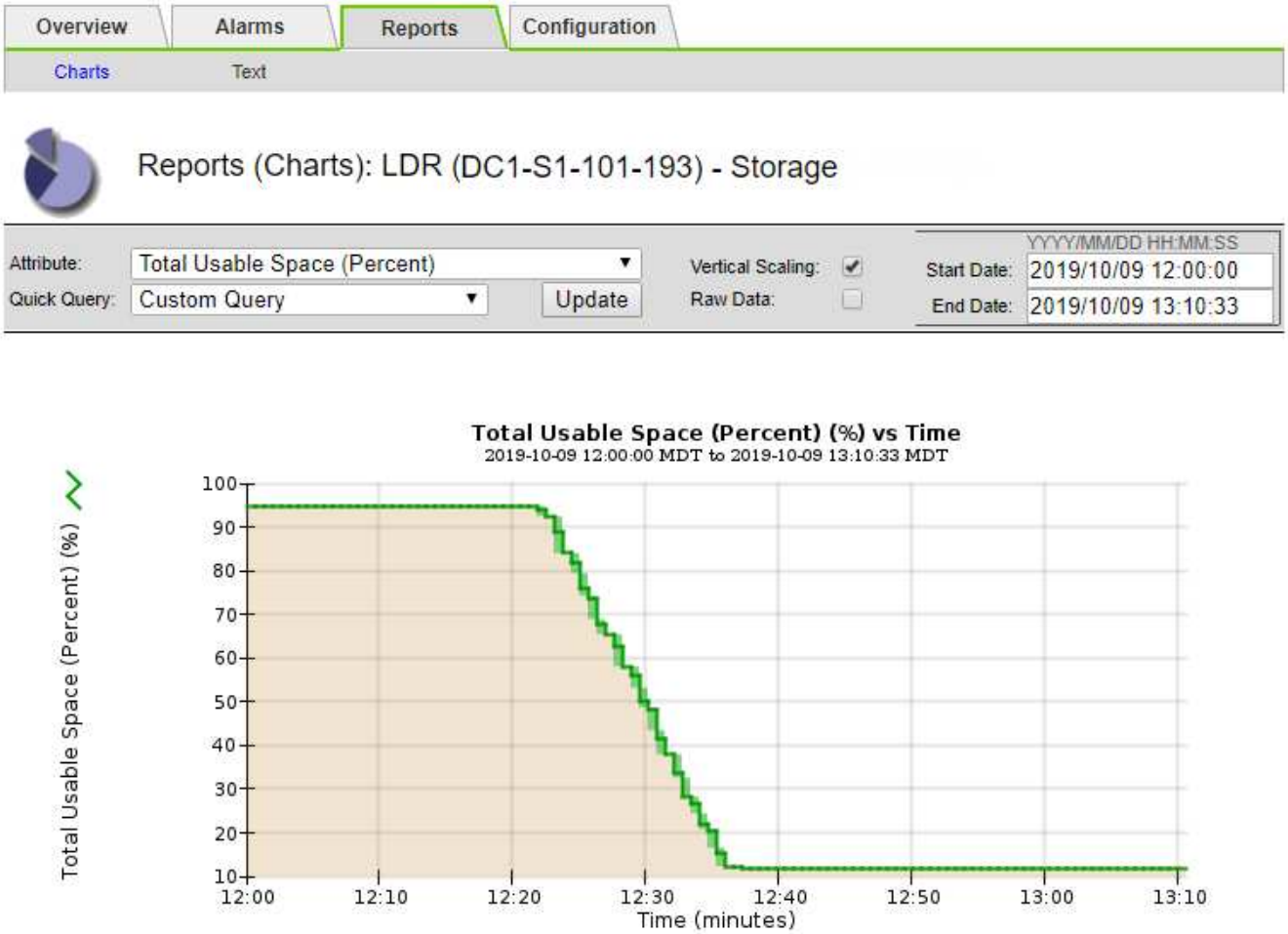
4. Per capire come lo storage è stato utilizzato nel tempo, selezionare la scheda **Report** e tracciare lo spazio utilizzabile totale nelle ultime ore.

   In questo esempio, lo spazio utilizzabile totale è sceso da circa 155 GB a 12:00 a 20 GB a 12:35, il che corrisponde al momento in cui è stato attivato l'allarme SSTS.



5. Per comprendere come lo storage viene utilizzato come percentuale del totale, tracciare lo spazio utilizzabile totale (percentuale) nelle ultime ore.

   In questo esempio, lo spazio utilizzabile totale è sceso dal 95% a poco più del 10% circa contemporaneamente.



6. Secondo necessità, "aggiungere capacità di storage".

   Vedere anche "Gestire nodi storage completi".

Risoluzione dei problemi relativi all'erogazione dei messaggi dei servizi della piattaforma (allarme SMTT)

L'allarme SMTT (Total Events) viene attivato in Grid Manager se un messaggio di servizio della piattaforma viene inviato a una destinazione che non può accettare i dati.

A proposito di questa attività

Ad esempio, il caricamento di un S3 multipart può avere successo anche se la replica o il messaggio di notifica associati non possono essere inviati all'endpoint configurato. In alternativa, un messaggio per la replica di CloudMirror potrebbe non essere recapitato se i metadati sono troppo lunghi.

L'allarme SMTT contiene un messaggio Last Event (ultimo evento) che indica: `Failed to publish notifications for bucket-name object key` per l'ultimo oggetto la cui notifica non è riuscita.

I messaggi degli eventi sono elencati anche in `/var/local/log/bycast-err.log` file di log. Vedere "Riferimenti ai file di log".

Per ulteriori informazioni, consultare "Risolvere i problemi relativi ai servizi della piattaforma". Potrebbe essere necessario "Accedere al tenant dal tenant manager" per eseguire il debug di un errore del servizio della piattaforma.

Fasi

1. Per visualizzare l'allarme, selezionare **NODES** > ***Site*** > ***Grid Node*** > **Events**.
2. Visualizza ultimo evento nella parte superiore della tabella.

   I messaggi degli eventi sono elencati anche nella `/var/local/log/bycast-err.log`.

3. Seguire le indicazioni fornite nel contenuto degli allarmi SMTT per correggere il problema.
4. Selezionare **Reset event count** (Ripristina conteggi eventi).
5. Notificare al tenant gli oggetti i cui messaggi dei servizi della piattaforma non sono stati recapitati.
6. Chiedere al tenant di attivare la replica o la notifica non riuscita aggiornando i metadati o i tag dell'oggetto.

Risolvere i problemi relativi ai metadati

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi ai metadati.

Avviso di spazio di archiviazione dei metadati insufficiente

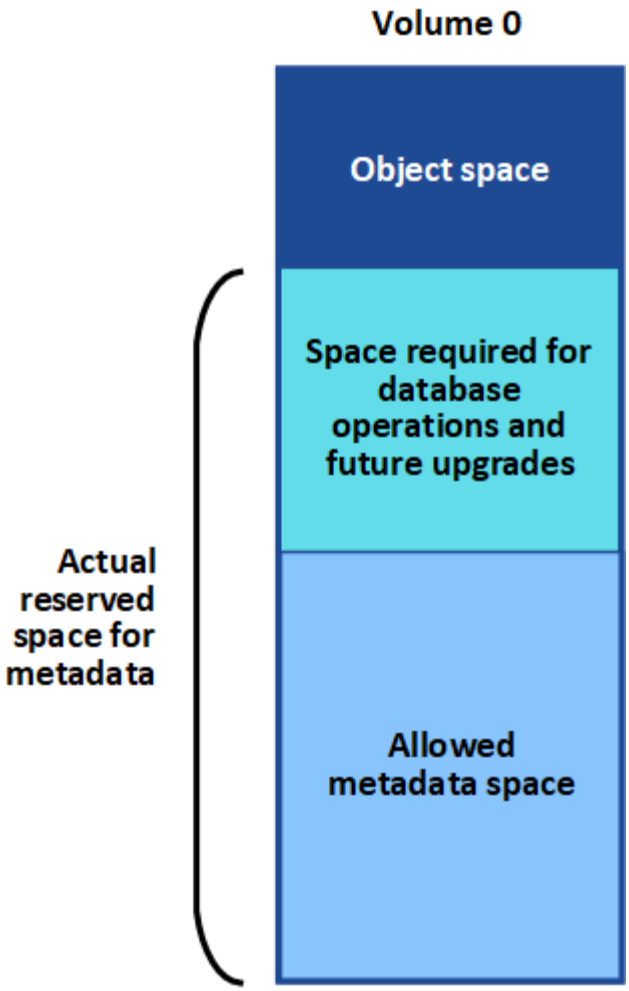
Se viene attivato l'avviso **Low metadata storage**, è necessario aggiungere nuovi nodi di storage.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

StorageGRID riserva una certa quantità di spazio sul volume 0 di ciascun nodo di storage per i metadati dell'oggetto. Questo spazio è noto come spazio riservato effettivo e viene suddiviso nello spazio consentito per i metadati dell'oggetto (lo spazio consentito per i metadati) e nello spazio richiesto per le operazioni essenziali del database, come la compattazione e la riparazione. Lo spazio consentito per i metadati regola la capacità complessiva degli oggetti.



Se i metadati degli oggetti consumano più del 100% dello spazio consentito per i metadati, le operazioni del database non possono essere eseguite in modo efficiente e si verificano errori.

È possibile "Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage" per aiutarti a prevenire gli errori e correggerli prima che si verifichino.

StorageGRID utilizza la seguente metrica Prometheus per misurare la quantità di spazio consentito per i metadati:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

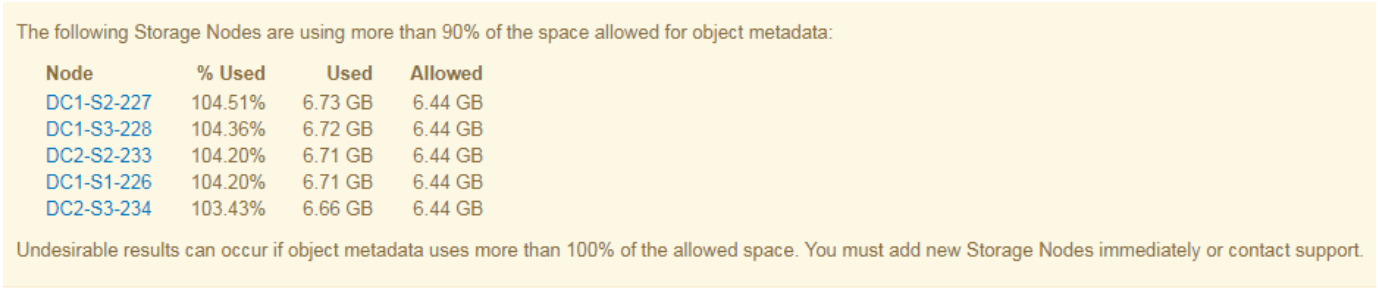
Quando l'espressione Prometheus raggiunge determinate soglie, viene attivato l'avviso **Low metadata storage**.

- **Minore**: I metadati degli oggetti utilizzano almeno il 70% dello spazio consentito per i metadati. È necessario aggiungere nuovi nodi di storage il prima possibile.
- **Major**: I metadati degli oggetti utilizzano almeno il 90% dello spazio consentito per i metadati. È necessario aggiungere immediatamente nuovi nodi di storage.

Quando i metadati dell'oggetto utilizzano almeno il 90% dello spazio consentito per i metadati, viene visualizzato un avviso sul dashboard. Se viene visualizzato questo avviso, è necessario aggiungere immediatamente nuovi nodi di storage. Non è mai necessario consentire ai metadati degli oggetti di utilizzare più del 100% dello spazio consentito.

- **Critico**: I metadati degli oggetti utilizzano almeno il 100% dello spazio consentito e stanno iniziando a consumare lo spazio necessario per le operazioni essenziali del database. È necessario interrompere l'acquisizione di nuovi oggetti e aggiungere immediatamente nuovi nodi di storage.

Nell'esempio seguente, i metadati degli oggetti utilizzano oltre il 100% dello spazio consentito per i metadati. Si tratta di una situazione critica, che può causare errori e operazioni inefficienti del database.



Se la dimensione del volume 0 è inferiore all'opzione di storage Metadata Reserved Space (ad esempio, in un ambiente non in produzione), il calcolo dell'avviso **Low metadata storage** potrebbe essere impreciso.

Fasi

1. Selezionare **ALERTS** > **current**.
2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low metadata storage**, se necessario, e selezionare l'avviso specifico che si desidera visualizzare.
3. Esaminare i dettagli nella finestra di dialogo degli avvisi.
4. Se è stato attivato un avviso importante o critico **Low metadata storage**, eseguire un'espansione per aggiungere immediatamente i nodi di storage.

   Poiché StorageGRID conserva copie complete di tutti i metadati degli oggetti in ogni sito, la capacità dei metadati dell'intera griglia è limitata dalla capacità dei metadati del sito più piccolo. Se devi aggiungere capacità di metadati a un sito, dovresti anche "espandere qualsiasi altro sito" Dello stesso numero di nodi di storage.

   Dopo aver eseguito l'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti nei nuovi nodi, aumentando così la capacità complessiva dei metadati della griglia. Non è richiesta alcuna azione da parte dell'utente. L'avviso **Low metadata storage** viene cancellato.

Servizi: Stato - allarme Cassandra (SVST)

L'allarme servizi: Stato - Cassandra (SVST) indica che potrebbe essere necessario ricostruire il database Cassandra per un nodo di storage. Cassandra viene utilizzato come archivio di metadati per StorageGRID.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

- È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

Se Cassandra viene arrestato per più di 15 giorni (ad esempio, il nodo di storage viene spento), Cassandra non si avvia quando il nodo viene riportato in linea. È necessario ricostruire il database Cassandra per il servizio DDS interessato.

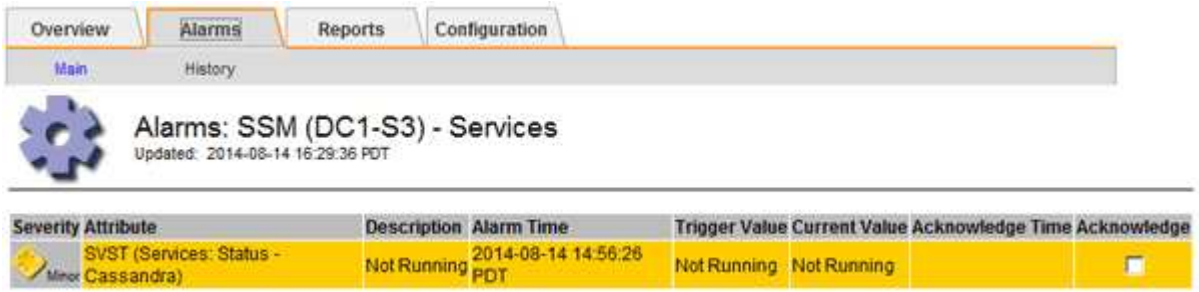
È possibile "eseguire la diagnostica" per ottenere ulteriori informazioni sullo stato corrente della griglia.

> Se due o più servizi di database Cassandra rimangono inutilizzati per più di 15 giorni, contattare il supporto tecnico e non procedere con la procedura riportata di seguito.

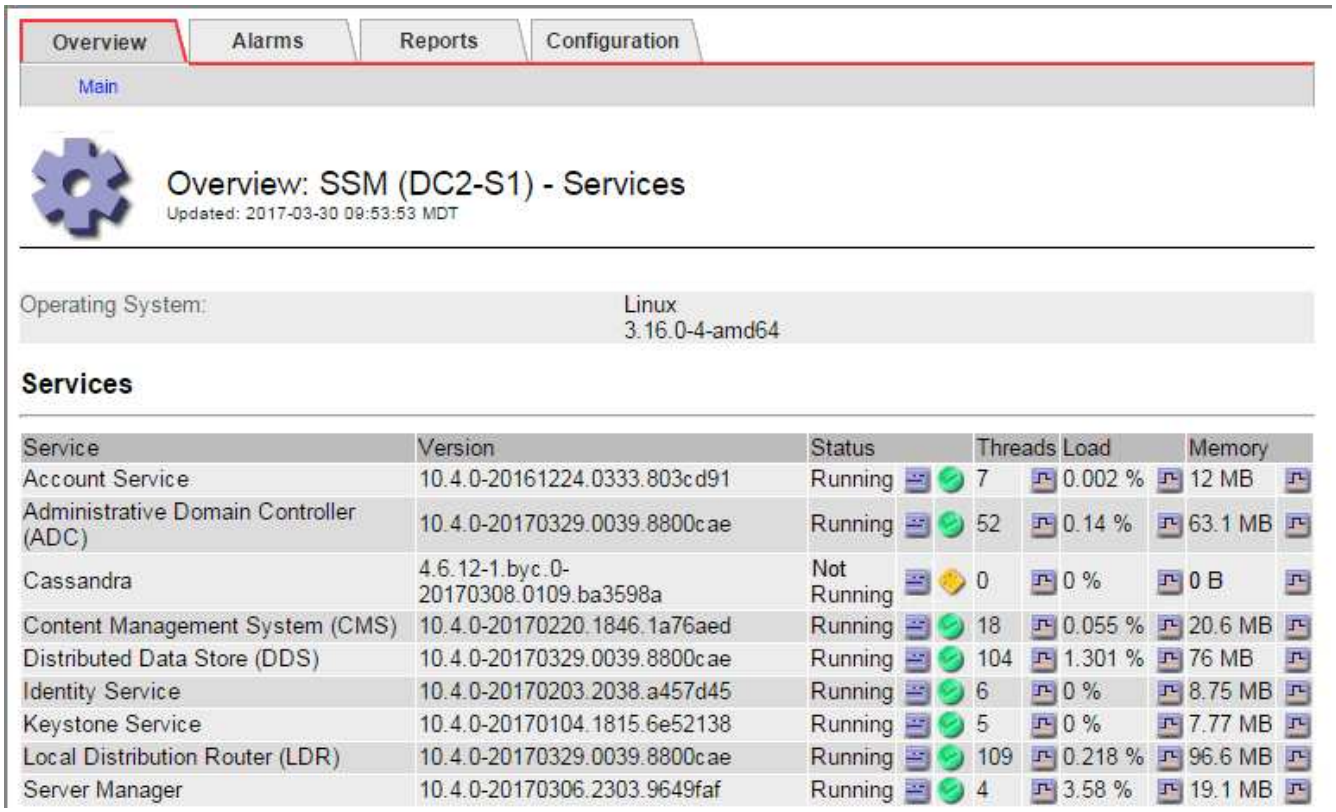
Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > ***Storage Node*** > **SSM** > **Services** > **Alarms** > **Main** per visualizzare gli allarmi.

   Questo esempio mostra che l'allarme SVST è stato attivato.



   La pagina principale dei servizi SSM indica inoltre che Cassandra non è in esecuzione.



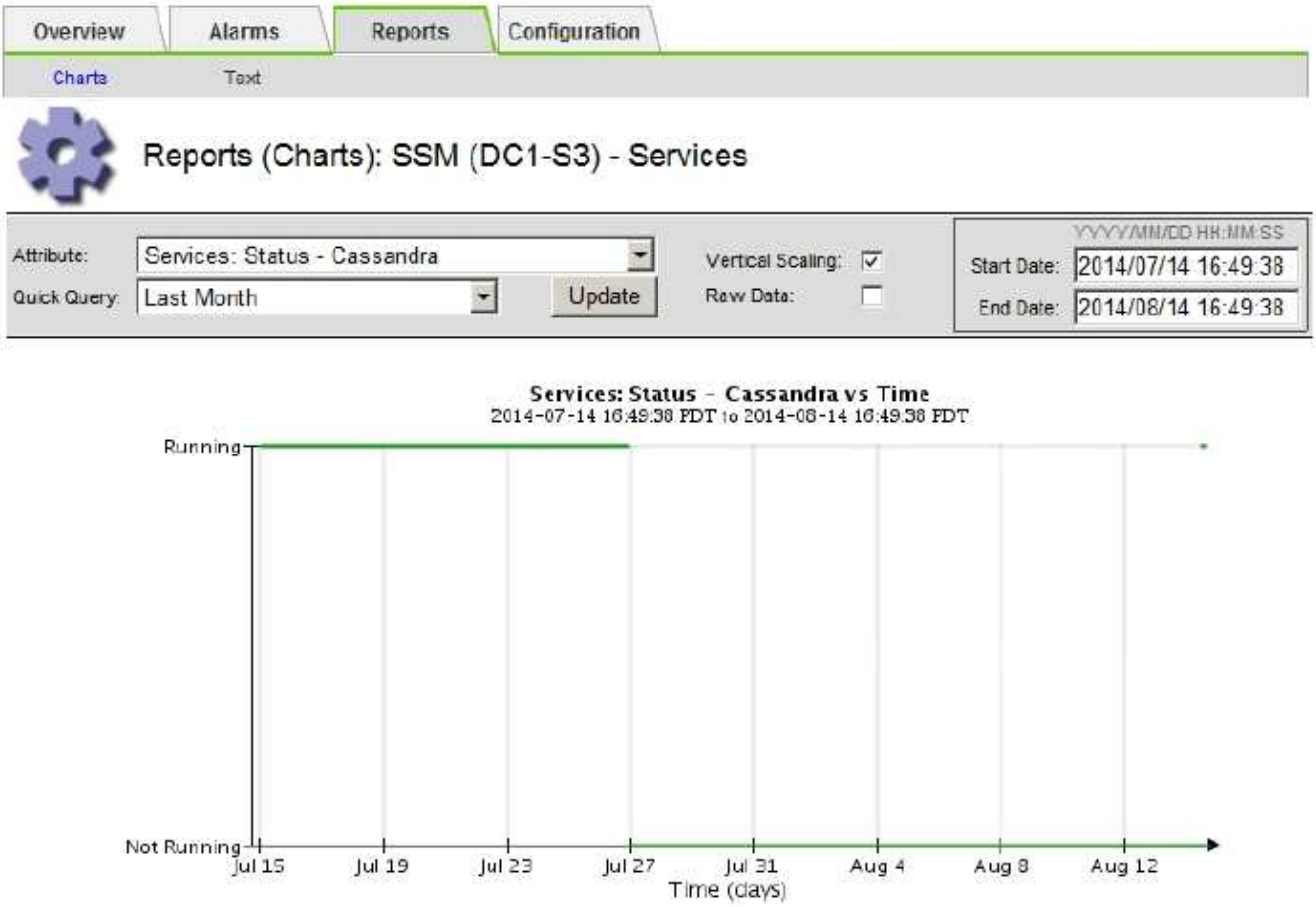
3. prova a riavviare Cassandra dal nodo di storage:
   a. Accedere al nodo Grid:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file.
      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
   b. Inserire: `/etc/init.d/cassandra status`
   c. Se Cassandra non è in esecuzione, riavviarlo: `/etc/init.d/cassandra restart`
4. Se Cassandra non si riavvia, determinare per quanto tempo Cassandra è rimasto inattivo. Se Cassandra è rimasto inattivo per più di 15 giorni, è necessario ricostruire il database Cassandra.

   > Se due o più servizi di database Cassandra non sono disponibili, contattare il supporto tecnico e non procedere con la procedura riportata di seguito.

   È possibile determinare per quanto tempo Cassandra è rimasta inattiva, inserendolo nella cartella o esaminando il file servermanager.log.

5. Per inserire il grafico Cassandra:
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Storage Node*** > **SSM** > **servizi** > **Report** > **grafici**.
   b. Selezionare **attributo** > **Servizio: Stato - Cassandra**.
   c. Per **Data di inizio**, immettere una data che sia almeno 16 giorni prima della data corrente. Per **Data di fine**, inserire la data corrente.
   d. Fare clic su **Aggiorna**.
   e. Se il grafico mostra Cassandra come inattivo per più di 15 giorni, ricostruire il database Cassandra.

      L'esempio seguente mostra che Cassandra è rimasta inattiva per almeno 17 giorni.



6. Per esaminare il file servermanager.log sul nodo di storage:

   a. Accedere al nodo Grid:

      i. Immettere il seguente comando: `ssh admin@grid_node_IP`

      ii. Immettere la password elencata in `Passwords.txt` file.

      iii. Immettere il seguente comando per passare a root: `su -`

      iv. Immettere la password elencata in `Passwords.txt` file.
      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

   b. Inserire: `cat /var/local/log/servermanager.log`

      Viene visualizzato il contenuto del file servermanager.log.

      Se Cassandra rimane inattivo per più di 15 giorni, nel file servermanager.log viene visualizzato il seguente messaggio:

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

   a. Assicurarsi che la data e l'ora del messaggio siano quelle in cui si è tentato di riavviare Cassandra, come indicato al punto Riavviare Cassandra dal nodo di storage.

Per Cassandra possono essere presenti più voci; è necessario individuare la voce più recente.

b. Se Cassandra è rimasto inattivo per più di 15 giorni, è necessario ricostruire il database Cassandra.

   Per istruzioni, vedere "Recovery Storage Node Down per più di 15 giorni".

c. Contattare il supporto tecnico se gli allarmi non vengono disattivati dopo la ricostruzione di Cassandra.

Errori di memoria esaurita di Cassandra (allarme SMTT)

Un allarme SMTT (Total Events) viene attivato quando il database Cassandra presenta un errore di memoria esaurita. Se si verifica questo errore, contattare il supporto tecnico per risolvere il problema.

A proposito di questa attività

Se si verifica un errore di memoria insufficiente per il database Cassandra, viene creato un dump heap, viene attivato un allarme SMTT (Total Events) e il conteggio degli errori Cassandra Heap out of Memory viene incrementato di uno.

Fasi

1. Guarda l'evento:
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Espandi il sito, quindi seleziona ***grid_node***.
   c. Selezionare **SSM**, quindi selezionare **Eventi** > **Configurazione**.
2. Verificare che il conteggio degli errori di memoria esaurita di Cassandra sia pari o superiore a 1.

   È possibile "eseguire la diagnostica" per ottenere ulteriori informazioni sullo stato corrente della griglia.

3. Accedi al nodo selezionato come "admin" tramite SSH e passa all'utente root locale.
4. Passare a. `/var/local/core/`, comprimere `Cassandra.hprof` e inviarla al supporto tecnico.
5. Eseguire un backup di `Cassandra.hprof` ed eliminarlo da `/var/local/core/ directory`.

   Questo file può avere una dimensione massima di 24 GB, quindi è necessario rimuoverlo per liberare spazio.

6. Una volta risolto il problema, selezionare la casella di controllo **Reset** (Ripristina) per il conteggio degli errori Cassandra Heap out of Memory (heap Cassandra fuori memoria). Quindi selezionare **Apply Changes** (Applica modifiche).

   Per reimpostare i conteggi degli eventi, è necessario disporre dell'autorizzazione di configurazione della pagina topologia griglia.

Risolvere gli errori del certificato

Se si verifica un problema di sicurezza o certificato quando si tenta di connettersi a StorageGRID utilizzando un browser Web, un client S3 o Swift o uno strumento di monitoraggio esterno, controllare il certificato.

A proposito di questa attività

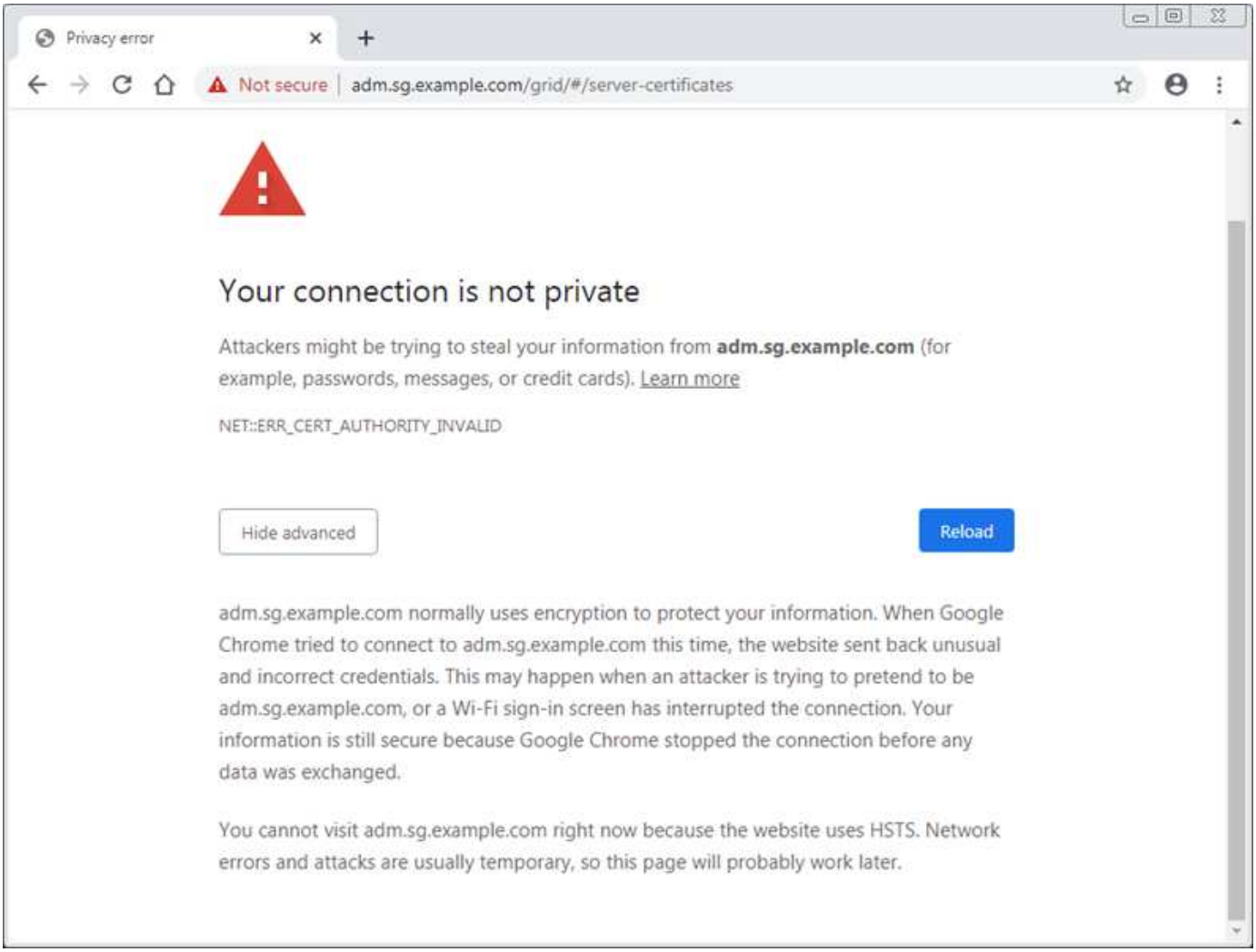
Gli errori dei certificati possono causare problemi quando si tenta di connettersi a StorageGRID utilizzando

Gestione griglia, API di gestione griglia, Gestore tenant o API di gestione tenant. Gli errori di certificato possono verificarsi anche quando si tenta di connettersi a un client S3 o Swift o a uno strumento di monitoraggio esterno.

Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Viene ripristinato da un certificato dell'interfaccia di gestione personalizzata al certificato del server predefinito.

L'esempio seguente mostra un errore di certificato quando il certificato dell'interfaccia di gestione personalizzata è scaduto:



Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** viene attivato quando il certificato del server sta per scadere.

Quando si utilizzano certificati client per l'integrazione esterna di Prometheus, gli errori dei certificati possono essere causati dal certificato dell'interfaccia di gestione di StorageGRID o dai certificati client. L'avviso **scadenza dei certificati client configurati nella pagina certificati** viene attivato quando un certificato client sta per scadere.

Fasi

Se si riceve una notifica di avviso relativa a un certificato scaduto, accedere ai dettagli del certificato:
. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi "selezionare la scheda del certificato appropriata".

1. Controllare il periodo di validità del certificato.
   Alcuni browser Web e client S3 o Swift non accettano certificati con un periodo di validità superiore a 398 giorni.
2. Se il certificato è scaduto o scadrà a breve, caricare o generare un nuovo certificato.
   - Per un certificato del server, consultare la procedura per "Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager".
   - Per un certificato client, vedere la procedura per "configurazione di un certificato client".
3. In caso di errori del certificato del server, provare una o entrambe le seguenti opzioni:
   - Assicurarsi che il campo Subject alternative Name (SAN) del certificato sia compilato e che LA SAN corrisponda all'indirizzo IP o al nome host del nodo a cui si sta effettuando la connessione.
   - Se si sta tentando di connettersi a StorageGRID utilizzando un nome di dominio:
     i. Inserire l'indirizzo IP del nodo di amministrazione invece del nome di dominio per evitare l'errore di connessione e accedere a Grid Manager.
     ii. Da Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi "selezionare la scheda del certificato appropriata" per installare un nuovo certificato personalizzato o continuare con il certificato predefinito.
     iii. Nelle istruzioni per l'amministrazione di StorageGRID, vedere la procedura per "Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager".

Risolvere i problemi relativi al nodo di amministrazione e all'interfaccia utente

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi ai nodi di amministrazione e all'interfaccia utente di StorageGRID.

Errori di accesso

Se si verifica un errore durante l'accesso a un nodo amministrativo StorageGRID, il sistema potrebbe avere un problema con "configurazione della federazione delle identità", a. "networking" oppure "hardware" problema, un problema con "Servizi del nodo di amministrazione"o un "Problema con il database Cassandra" Sui nodi di storage connessi.

Prima di iniziare

- Hai il `Passwords.txt` file.
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Utilizzare queste linee guida per la risoluzione dei problemi se viene visualizzato uno dei seguenti messaggi di errore quando si tenta di accedere a un nodo amministratore:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete`

`your request. Please try again. If the problem persists, contact Technical Support.`

- `Unable to communicate with server. Reloading page…`

Fasi

1. Attendere 10 minuti e riprovare a effettuare l'accesso.

   Se l'errore non viene risolto automaticamente, passare alla fase successiva.

2. Se il sistema StorageGRID dispone di più di un nodo amministratore, provare ad accedere al gestore della griglia da un altro nodo amministratore.
   - Se sei in grado di effettuare l'accesso, puoi utilizzare le opzioni **Dashboard**, **NODES**, **Alerts** e **SUPPORT** per determinare la causa dell'errore.
   - Se si dispone di un solo nodo di amministrazione o non si riesce ancora ad accedere, passare alla fase successiva.
3. Determinare se l'hardware del nodo non è in linea.
4. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID in uso, fare riferimento alla procedura descritta in "configurazione del single sign-on".

   Potrebbe essere necessario disattivare temporaneamente e riattivare SSO per un singolo nodo di amministrazione per risolvere eventuali problemi.

   > Se SSO è attivato, non è possibile accedere utilizzando una porta con restrizioni. È necessario utilizzare la porta 443.

5. Determinare se l'account in uso appartiene a un utente federato.

   Se l'account utente federated non funziona, provare ad accedere a Grid Manager come utente locale, ad esempio root.

   - Se l'utente locale può effettuare l'accesso:
     i. Esaminare gli eventuali allarmi visualizzati.
     ii. Selezionare **CONFIGURATION** > **Access Control** > **Identity Federation**.
     iii. Fare clic su **Test Connection** (verifica connessione) per convalidare le impostazioni di connessione per il server LDAP.
     iv. Se il test non riesce, risolvere eventuali errori di configurazione.
   - Se l'utente locale non riesce ad accedere e si è certi che le credenziali siano corrette, passare alla fase successiva.
6. Utilizzare Secure Shell (ssh) per accedere al nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

7. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo grid: `storagegrid-status`

   Assicurarsi che i servizi api nms, mi, nginx e mgmt siano tutti in esecuzione.

   L'output viene aggiornato immediatamente se lo stato di un servizio cambia.

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0         Verified
Operating System Environment   Debian 10.1    Verified
StorageGRID Webscale Release   11.4.0         Verified
Networking                                    Verified
Storage Subsystem                             Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0         Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0         Running
cmn                            11.4.0         Running
nms                            11.4.0         Running
ssm                            11.4.0         Running
mi                             11.4.0         Running
dynip                          11.4.0         Running
nginx                          1.10.3         Running
tomcat                         9.0.27         Running
grafana                        6.4.3          Running
mgmt api                       11.4.0         Running
prometheus                     11.4.0         Running
persistence                    11.4.0         Running
ade exporter                   11.4.0         Running
alertmanager                   11.4.0         Running
attrDownPurge                  11.4.0         Running
attrDownSamp1                  11.4.0         Running
attrDownSamp2                  11.4.0         Running
node exporter                  0.17.0+ds      Running
sg snmp agent                  11.4.0         Running
```

8. Verificare che il servizio nginx-gw sia in esecuzione `# service nginx-gw status`
9. Usa Lumberjack per raccogliere i log: `# /usr/local/sbin/lumberjack.rb`

   Se l'autenticazione non è riuscita in passato, è possibile utilizzare le opzioni di script --start e --end Lumberjack per specificare l'intervallo di tempo appropriato. Utilizzare lumberjack -h per i dettagli su queste opzioni.

   L'output sul terminale indica dove è stato copiato l'archivio di log.

10. Rivedi i seguenti log:

- /var/local/log/bycast.log
- /var/local/log/bycast-err.log
- /var/local/log/nms.log
- **/*commands.txt

11. Se non si riesce a identificare alcun problema con il nodo di amministrazione, eseguire uno dei seguenti comandi per determinare gli indirizzi IP dei tre nodi di storage che eseguono il servizio ADC presso la propria sede. In genere, si tratta dei primi tre nodi di storage installati nel sito.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

I nodi di amministrazione utilizzano il servizio ADC durante il processo di autenticazione.

12. Dal nodo di amministrazione, accedere a ciascuno dei nodi di storage ADC, utilizzando gli indirizzi IP identificati.
    a. Immettere il seguente comando: `ssh admin@grid_node_IP`
    b. Immettere la password elencata in `Passwords.txt` file.
    c. Immettere il seguente comando per passare a root: `su -`
    d. Immettere la password elencata in `Passwords.txt` file.

    Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

13. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo grid: `storagegrid-status`

    Assicurarsi che i servizi idnt, acct, nginx e cassandra siano tutti in esecuzione.

14. Ripetere i passaggi Utilizzare Lumberjack per raccogliere i registri e. Esaminare i registri Per rivedere i log sui nodi di storage.
15. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

    Fornire al supporto tecnico i registri raccolti. Vedere anche "Riferimenti ai file di log".

Problemi dell'interfaccia utente

L'interfaccia utente di Grid Manager o Tenant Manager potrebbe non rispondere come previsto dopo l'aggiornamento del software StorageGRID.

Fasi

1. Assicurarsi di utilizzare un "browser web supportato".

> Il supporto del browser può cambiare con ogni release di StorageGRID. Verificare che si stia utilizzando un browser supportato dalla versione di StorageGRID in uso.

2. Cancellare la cache del browser Web.

   La cancellazione della cache rimuove le risorse obsolete utilizzate dalla versione precedente del software StorageGRID e consente all'interfaccia utente di funzionare nuovamente correttamente. Per istruzioni, consultare la documentazione del browser Web.

Nodo amministratore non disponibile

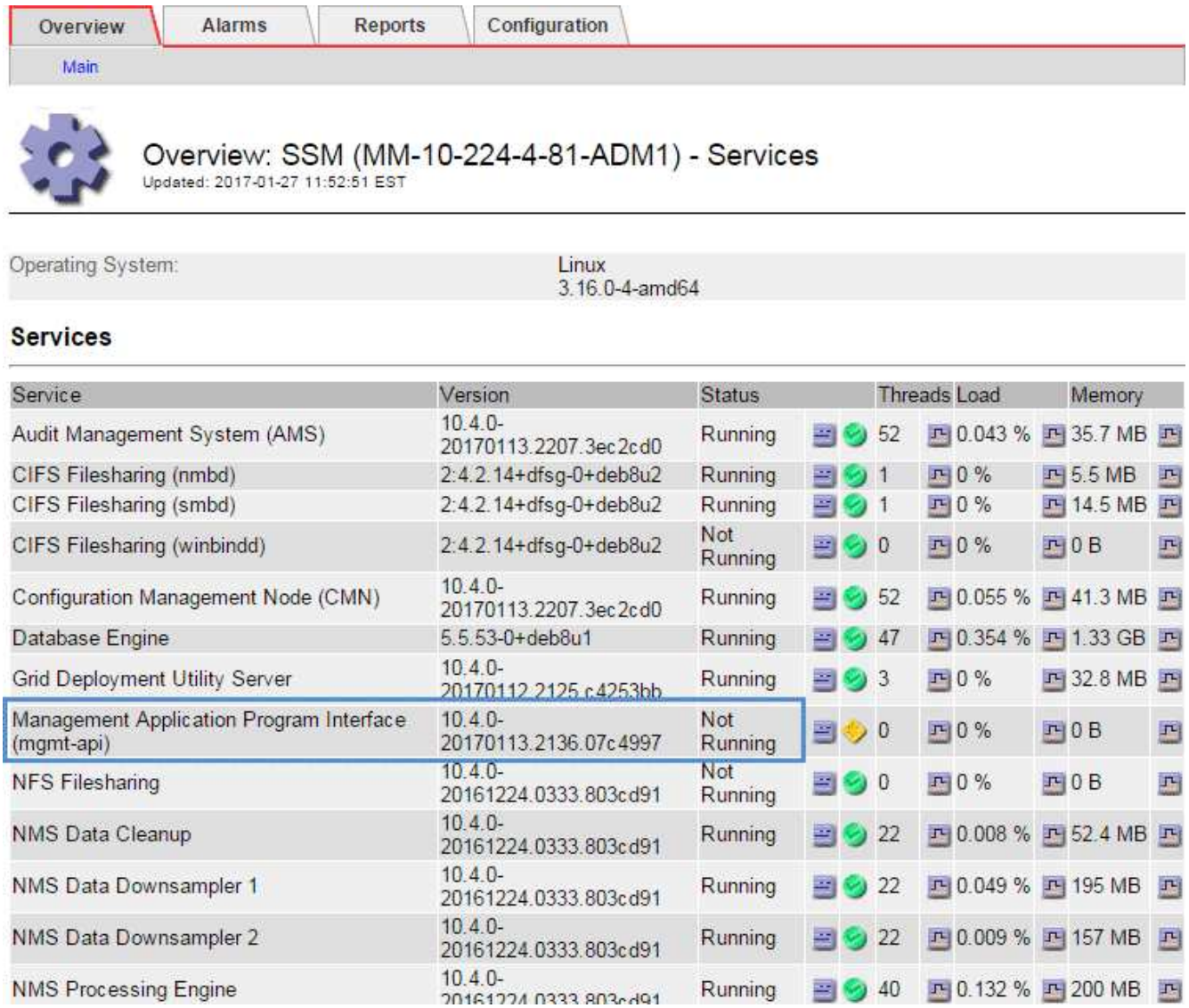
Se il sistema StorageGRID include più nodi di amministrazione, è possibile utilizzare un altro nodo di amministrazione per controllare lo stato di un nodo di amministrazione non disponibile.

Prima di iniziare

Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Da un nodo Admin disponibile, accedere a Grid Manager utilizzando un "browser web supportato".
2. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
3. Selezionare ***Site*** **> non disponibile Admin Node** > **SSM** > **servizi** > **Panoramica** > **principale**.
4. Cercare i servizi con stato non in esecuzione e che potrebbero essere visualizzati anche in blu.



5. Determinare se gli allarmi sono stati attivati.
6. Intraprendere le azioni appropriate per risolvere il problema.

Risolvere i problemi di rete, hardware e piattaforma

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi a problemi di rete, hardware e piattaforma StorageGRID.

Errori "422: Entità non elaborabile"

L'errore 422: Unprocessable Entity può verificarsi per diversi motivi. Controllare il messaggio di errore per determinare la causa del problema.

Se viene visualizzato uno dei messaggi di errore elencati, eseguire l'azione consigliata.

Messaggio di errore	Causa principale e azione correttiva

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	Questo messaggio potrebbe essere visualizzato se si seleziona l'opzione **non utilizzare TLS** per Transport Layer Security (TLS) durante la configurazione della federazione delle identità utilizzando Windows Active Directory (ad).
	
	L'utilizzo dell'opzione **non utilizzare TLS** non è supportato per l'utilizzo con i server ad che applicano la firma LDAP. Selezionare l'opzione **Use STARTTLS** (Usa STARTTLS*) o l'opzione **Use LDAPS** (Usa LDAPS* per TLS).

Messaggio di errore	Causa principale e azione correttiva

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	Questo messaggio viene visualizzato se si tenta di utilizzare una crittografia non supportata per stabilire una connessione TLS (Transport Layer Security) da StorageGRID a un sistema esterno utilizzato per identificare la federazione o i pool di storage cloud.
	
	Controllare le cifre offerte dal sistema esterno. Il sistema deve utilizzare uno dei "Crittografia supportata da StorageGRID" Per le connessioni TLS in uscita, come mostrato nelle istruzioni per l'amministrazione di StorageGRID.

Avviso di mancata corrispondenza MTU della rete griglia

L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato quando l'impostazione Maximum Transmission Unit (MTU) per l'interfaccia Grid Network (eth0) differisce significativamente tra i nodi della griglia.

A proposito di questa attività

Le differenze nelle impostazioni MTU potrebbero indicare che alcune, ma non tutte, reti eth0 sono configurate per i frame jumbo. Una mancata corrispondenza delle dimensioni MTU superiore a 1000 potrebbe causare problemi di performance di rete.

Fasi

1. Elencare le impostazioni MTU per eth0 su tutti i nodi.
   - Utilizzare la query fornita in Grid Manager.
   - Selezionare *`primary Admin Node IP address`*`/metrics/graph` e immettere la seguente query: `node_network_mtu_bytes{device="eth0"}`
2. "Modificare le impostazioni MTU" Come necessario per garantire che siano gli stessi per l'interfaccia Grid Network (eth0) su tutti i nodi.
   - Per i nodi basati su Linux e VMware, utilizzare il seguente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     Esempio: `change-ip.py -n node 1500 grid admin`

     Nota: Nei nodi basati su Linux, se il valore MTU desiderato per la rete nel container supera il valore già configurato sull'interfaccia host, è necessario prima configurare l'interfaccia host in modo che abbia il valore MTU desiderato, quindi utilizzare `change-ip.py` Script per modificare il valore MTU della rete nel container.

     Utilizzare i seguenti argomenti per modificare la MTU su nodi basati su Linux o VMware.

Argomenti di posizione	Descrizione
`mtu`	MTU da impostare. Deve essere compreso tra 1280 e 9216.
`network`	Le reti a cui applicare la MTU. Includere uno o più dei seguenti tipi di rete: • griglia • amministratore • client

+

Argomenti facoltativi	Descrizione
`-h, – help`	Visualizzare il messaggio della guida e uscire.
`-n node, --node node`	Il nodo. L'impostazione predefinita è il nodo locale.

Allarme NRER (Network Receive Error)

Gli allarmi NRER (Network Receive Error) possono essere causati da problemi di connettività tra StorageGRID e l'hardware di rete. In alcuni casi, gli errori NRER possono essere corretti senza l'intervento manuale. Se gli errori non vengono corretti, eseguire le azioni consigliate.

A proposito di questa attività

Gli allarmi NRER possono essere causati dai seguenti problemi relativi all'hardware di rete che si collega a StorageGRID:

- La funzione FEC (Forward Error Correction) è obbligatoria e non in uso
- Mancata corrispondenza tra porta dello switch e MTU della scheda NIC
- Elevati tassi di errore di collegamento
- Buffer di anello NIC scaduto

Fasi

1. Seguire i passaggi per la risoluzione dei problemi relativi a tutte le potenziali cause dell'allarme NRER in base alla configurazione di rete.
2. A seconda della causa dell'errore, attenersi alla seguente procedura:

Mancata corrispondenza FEC

> Questi passaggi sono applicabili solo agli errori NRER causati da mancata corrispondenza FEC sulle appliance StorageGRID.

a. Controllare lo stato FEC della porta dello switch collegato all'appliance StorageGRID.
b. Controllare l'integrità fisica dei cavi che collegano l'apparecchio allo switch.
c. Se si desidera modificare le impostazioni FEC per tentare di risolvere l'allarme NRER, assicurarsi innanzitutto che l'appliance sia configurata per la modalità **auto** nella pagina di configurazione del collegamento del programma di installazione dell'appliance StorageGRID (consultare le istruzioni relative all'appliance:
   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 e SG1100"
   - "SG100 e SG1000"
d. Modificare le impostazioni FEC sulle porte dello switch. Le porte dell'appliance StorageGRID regoleranno le impostazioni FEC in modo che corrispondano, se possibile.

   Non è possibile configurare le impostazioni FEC sulle appliance StorageGRID. Le appliance tentano invece di rilevare e duplicare le impostazioni FEC sulle porte dello switch a cui sono collegate. Se i collegamenti sono forzati a velocità di rete 25-GbE o 100-GbE, lo switch e la NIC potrebbero non riuscire a negoziare un'impostazione FEC comune. Senza un'impostazione FEC comune, la rete torna alla modalità "no-FEC". Quando la funzione FEC non è attivata, le connessioni sono più soggette a errori causati da disturbi elettrici.

   > Le appliance StorageGRID supportano Firecode (FC) e Reed Solomon (RS) FEC, oltre che FEC.

Mancata corrispondenza tra porta dello switch e MTU della scheda NIC

Se l'errore è causato da una mancata corrispondenza tra la porta dello switch e la MTU della NIC, verificare che le dimensioni MTU configurate sul nodo corrispondano all'impostazione MTU per la porta dello switch.

La dimensione MTU configurata sul nodo potrebbe essere inferiore all'impostazione sulla porta dello switch a cui è connesso il nodo. Se un nodo StorageGRID riceve un frame Ethernet più grande del relativo MTU, cosa possibile con questa configurazione, potrebbe essere segnalato l'allarme NRER. Se si ritiene che questo sia quanto accade, modificare la MTU della porta dello switch in modo che corrisponda alla MTU dell'interfaccia di rete StorageGRID oppure modificare la MTU dell'interfaccia di rete StorageGRID in modo che corrisponda alla porta dello switch, in base agli obiettivi o ai requisiti della MTU end-to-end.

Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete. Vedere Risolvere i problemi relativi all'avviso di mancata corrispondenza MTU della rete griglia per ulteriori informazioni.

Vedere anche "Modificare l'impostazione MTU".

Elevati tassi di errore di collegamento

a. Attivare FEC, se non è già attivato.
b. Verificare che il cablaggio di rete sia di buona qualità e non sia danneggiato o collegato in modo errato.
c. Se i cavi non sembrano essere il problema, contattare il supporto tecnico.

In un ambiente con elevati livelli di rumore elettrico, potrebbero verificarsi errori elevati.

Buffer di anello NIC scaduto

Se l'errore è un buffer di anello della scheda di rete in eccesso, contattare il supporto tecnico.

Il buffer circolare può essere sovraccarico quando il sistema StorageGRID è sovraccarico e non è in grado di elaborare gli eventi di rete in modo tempestivo.

3. Dopo aver risolto il problema sottostante, reimpostare il contatore degli errori.
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **Main**.
   c. Selezionare **Ripristina conteggio errori di ricezione** e fare clic su **Applica modifiche**.

Informazioni correlate

"Riferimento allarmi (sistema legacy)"

Errori di sincronizzazione dell'ora

Potrebbero verificarsi problemi con la sincronizzazione dell'ora nella griglia.

Se si verificano problemi di sincronizzazione dell'ora, verificare di aver specificato almeno quattro origini NTP esterne, ciascuna con uno strato 3 o un riferimento migliore, e che tutte le origini NTP esterne funzionino normalmente e siano accessibili dai nodi StorageGRID.

Quando "Specifica dell'origine NTP esterna" Per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Windows Time (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Time sulle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'utilizzo in ambienti ad alta precisione, come StorageGRID.

Linux: Problemi di connettività di rete

Potrebbero verificarsi problemi di connettività di rete per i nodi StorageGRID ospitati su host Linux.

Clonazione indirizzo MAC

In alcuni casi, i problemi di rete possono essere risolti utilizzando la clonazione dell'indirizzo MAC. Se si utilizzano host virtuali, impostare il valore della chiave di clonazione dell'indirizzo MAC per ciascuna rete su "true" nel file di configurazione del nodo. Questa impostazione fa in modo che l'indirizzo MAC del container StorageGRID utilizzi l'indirizzo MAC dell'host. Per creare i file di configurazione del nodo, consultare le istruzioni per "Red Hat Enterprise Linux" oppure "Ubuntu o Debian".

> Creare interfacce di rete virtuali separate per l'utilizzo da parte del sistema operativo host Linux. L'utilizzo delle stesse interfacce di rete per il sistema operativo host Linux e per il container StorageGRID potrebbe rendere il sistema operativo host irraggiungibile se la modalità promiscua non è stata attivata sull'hypervisor.

Per ulteriori informazioni sull'attivazione della clonazione MAC, consultare le istruzioni per "Red Hat Enterprise Linux" oppure "Ubuntu o Debian".

Modalità promiscua

Se non si desidera utilizzare la clonazione dell'indirizzo MAC e si desidera consentire a tutte le interfacce di ricevere e trasmettere dati per indirizzi MAC diversi da quelli assegnati dall'hypervisor, Assicurarsi che le proprietà di sicurezza a livello di switch virtuale e gruppo di porte siano impostate su **Accept** per modalità promiscuous, modifiche indirizzo MAC e trasmissione forgiata. I valori impostati sullo switch virtuale possono essere sovrascritti dai valori a livello di gruppo di porte, quindi assicurarsi che le impostazioni siano le stesse in entrambe le posizioni.

Per ulteriori informazioni sull'utilizzo della modalità promiscua, consultare le istruzioni di "Red Hat Enterprise Linux" oppure "Ubuntu o Debian".

Linux: Lo stato del nodo è "orfano"

Un nodo Linux in uno stato orfano di solito indica che il servizio StorageGRID o il daemon del nodo StorageGRID che controlla il contenitore del nodo sono morti inaspettatamente.

A proposito di questa attività

Se un nodo Linux segnala che si trova in uno stato orfano, è necessario:

- Controllare i registri per verificare la presenza di errori e messaggi.
- Tentare di riavviare il nodo.
- Se necessario, utilizzare i comandi del motore dei container per arrestare il contenitore di nodi esistente.
- Riavviare il nodo.

Fasi

1. Controllare i log sia per il daemon di servizio che per il nodo orfano per verificare la presenza di errori evidenti o messaggi relativi all'uscita imprevista.
2. Accedere all'host come root o utilizzando un account con autorizzazione sudo.
3. Tentare di riavviare il nodo eseguendo il seguente comando: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Se il nodo è orfano, la risposta è

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Da Linux, arrestare il motore dei container e qualsiasi processo di controllo del nodo storagegrid. Ad esempio:`sudo docker stop --time secondscontainer-name`

   Per `seconds`, immettere il numero di secondi che si desidera attendere per l'arresto del container (in genere 15 minuti o meno). Ad esempio:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Riavviare il nodo: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

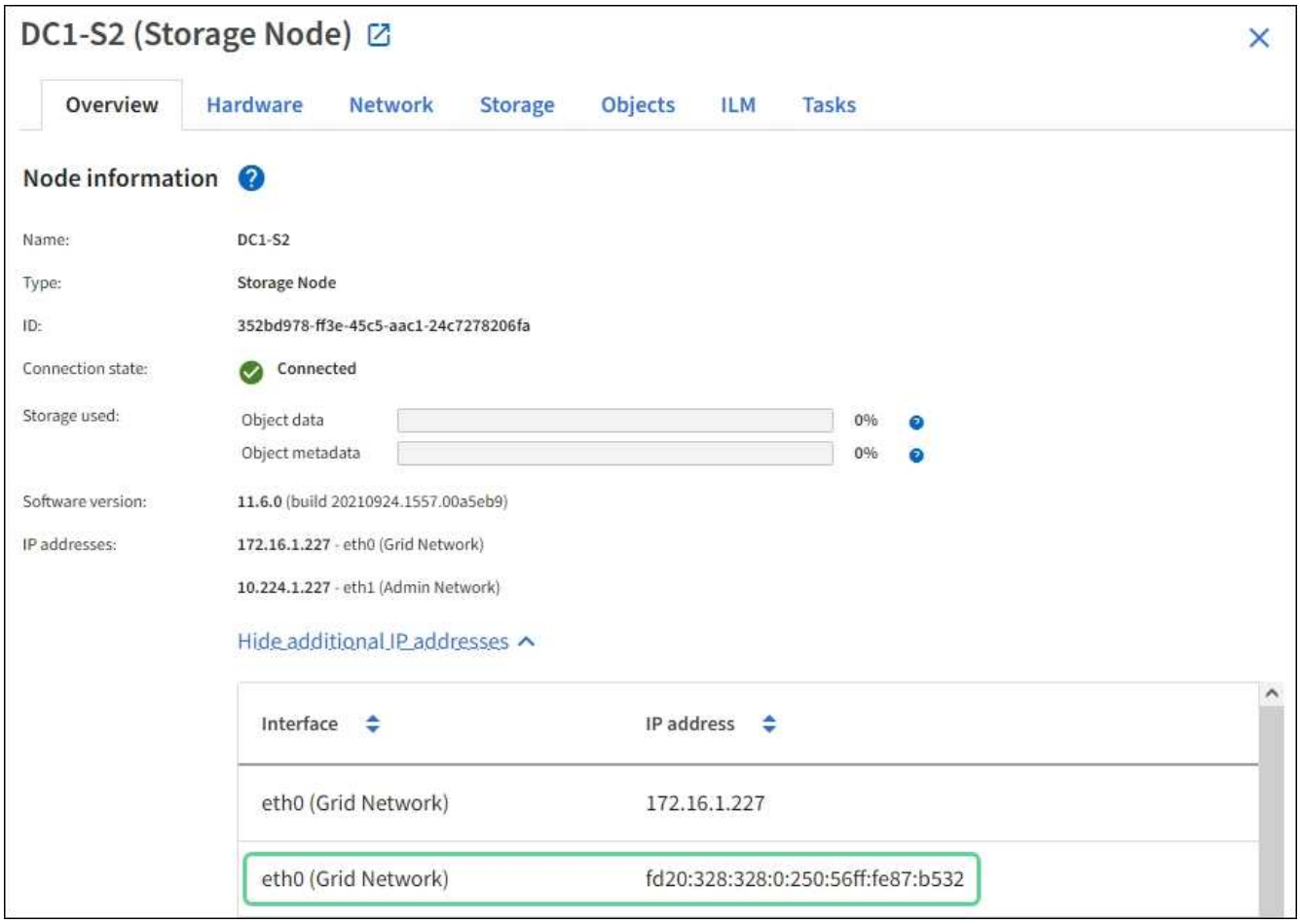
Linux: Risoluzione dei problemi relativi al supporto IPv6

Potrebbe essere necessario abilitare il supporto IPv6 nel kernel se sono stati installati nodi StorageGRID su host Linux e si nota che gli indirizzi IPv6 non sono stati assegnati ai contenitori di nodi come previsto.

A proposito di questa attività

È possibile visualizzare l'indirizzo IPv6 assegnato a un nodo Grid nelle seguenti posizioni in Grid Manager:

- Selezionare **NODI** e selezionare il nodo. Quindi, selezionare **Mostra altri** accanto a **indirizzi IP** nella scheda Panoramica.



- Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi, selezionare ***node*** > **SSM** > **risorse**. Se è stato assegnato un indirizzo IPv6, questo viene elencato sotto l'indirizzo IPv4 nella sezione **indirizzi di rete**.

Se l'indirizzo IPv6 non viene visualizzato e il nodo è installato su un host Linux, seguire questa procedura per abilitare il supporto IPv6 nel kernel.

Fasi

1. Accedere all'host come root o utilizzando un account con autorizzazione sudo.
2. Eseguire il seguente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

   Il risultato deve essere 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

   Se il risultato non è 0, consultare la documentazione relativa al sistema operativo in uso per le modifiche `sysctl` impostazioni. Quindi, modificare il valore su 0 prima di continuare.

3. Inserire il contenitore di nodi StorageGRID: `storagegrid node enter node-name`

4. Eseguire il seguente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Il risultato deve essere 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> Se il risultato non è 1, questa procedura non si applica. Contattare il supporto tecnico.

5. Uscire dal container: `exit`

```
root@DC1-S1:~ # exit
```

6. Come root, modificare il seguente file: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Individuare le due righe seguenti e rimuovere i tag di commento. Quindi, salvare e chiudere il file.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Eseguire questi comandi per riavviare il container StorageGRID:

```
storagegrid node stop node-name
```

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

Risolvere i problemi di un server syslog esterno

La tabella seguente descrive i messaggi di errore che potrebbero essere correlati a un server syslog esterno ed elenca le azioni correttive.

Questi errori vengono visualizzati dalla procedura guidata Configura server syslog esterno se si verificano problemi durante l'invio di messaggi di prova per convalidare la corretta configurazione del server syslog esterno.

Problemi in fase di esecuzione potrebbero essere segnalati dal"Errore di inoltro del server syslog esterno" allerta. Se ricevi questo avviso, segui le istruzioni contenute nell'avviso per inviare nuovamente i messaggi di prova e ottenere messaggi di errore dettagliati.

Per ulteriori informazioni sull'invio di informazioni di audit a un server syslog esterno, consultare:

- "Considerazioni sull'utilizzo di un server syslog esterno"
- "Configurare i messaggi di controllo e il server syslog esterno"

Messaggio di errore	Descrizione e azioni consigliate
Impossibile risolvere il nome host	Impossibile risolvere l'FQDN immesso per il server syslog in un indirizzo IP. 1. Controllare il nome host immesso. Se è stato immesso un indirizzo IP, assicurarsi che sia un indirizzo IP valido con la notazione W.X.Y.Z ("decimale separato da punti"). 2. Verificare che i server DNS siano configurati correttamente. 3. Verificare che ciascun nodo possa accedere agli indirizzi IP del server DNS.
Connessione rifiutata	Una connessione TCP o TLS al server syslog è stata rifiutata. Sulla porta TCP o TLS dell'host potrebbe non essere presente alcun servizio o un firewall potrebbe bloccare l'accesso. 1. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Verificare che l'host del servizio syslog stia eseguendo un daemon syslog in attesa sulla porta specificata. 3. Verificare che un firewall non blocchi l'accesso alle connessioni TCP/TLS dai nodi all'IP e alla porta del server syslog.
Rete non raggiungibile	Il server syslog non si trova su una subnet collegata direttamente. Un router ha restituito un messaggio di errore ICMP per indicare che non è stato possibile inoltrare i messaggi di test dai nodi elencati al server syslog. 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Per ciascun nodo elencato, selezionare Grid Network Subnet List (elenco subnet rete griglia), Admin Networks Subnet Lists (elenchi subnet reti amministrative) e Client Network Gateway (Gateway di rete client). Verificare che siano configurati per instradare il traffico al server syslog attraverso l'interfaccia di rete e il gateway previsti (Grid, Admin o Client).
Host non raggiungibile	Il server syslog si trova su una subnet collegata direttamente (subnet utilizzata dai nodi elencati per gli indirizzi IP Grid, Admin o Client). I nodi hanno tentato di inviare messaggi di test, ma non hanno ricevuto risposte alle richieste ARP per l'indirizzo MAC del server syslog. 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Verificare che l'host che esegue il servizio syslog sia attivo.

Messaggio di errore	Descrizione e azioni consigliate
Timeout della connessione	È stato eseguito un tentativo di connessione TCP/TLS, ma non è stata ricevuta alcuna risposta dal server syslog per molto tempo. Potrebbe esserci un errore di configurazione del routing o un firewall potrebbe interrompere il traffico senza inviare alcuna risposta (una configurazione comune). 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Per ciascun nodo elencato, selezionare Grid Network Subnet List (elenco subnet rete griglia), Admin Networks Subnet Lists (elenchi subnet reti amministrative) e Client Network Gateway (Gateway di rete client). Verificare che siano configurati per indirizzare il traffico al server syslog utilizzando l'interfaccia di rete e il gateway (Grid, Admin o Client) su cui si prevede di raggiungere il server syslog. 3. Verificare che un firewall non blocchi l'accesso alle connessioni TCP/TLS dai nodi elencati all'IP e alla porta del server syslog.
Connessione chiusa dal partner	Una connessione TCP al server syslog è stata stabilita correttamente, ma in seguito è stata chiusa. I motivi potrebbero includere: • Il server syslog potrebbe essere stato riavviato o riavviato. • Il nodo e il server syslog potrebbero avere impostazioni TCP/TLS diverse. • Un firewall intermedio potrebbe chiudere le connessioni TCP inattive. • Un server non syslog in ascolto sulla porta del server syslog potrebbe aver chiuso la connessione. Per risolvere questo problema: 1. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Se si utilizza TLS, verificare che anche il server syslog utilizzi TLS. Se si utilizza il protocollo TCP, verificare che anche il server syslog utilizzi il protocollo TCP. 3. Verificare che un firewall intermedio non sia configurato per chiudere le connessioni TCP inattive.
Errore certificato TLS	Il certificato del server ricevuto dal server syslog non era compatibile con il bundle di certificati CA e con il certificato client forniti. 1. Verificare che il bundle di certificati CA e il certificato client (se presente) siano compatibili con il certificato server sul server syslog. 2. Verificare che le identità nel certificato del server dal server syslog includano i valori IP o FQDN previsti.
Inoltro sospeso	I record syslog non vengono più inoltrati al server syslog e StorageGRID non è in grado di rilevare il motivo. Esaminare i log di debug forniti con questo errore per cercare di determinare la causa principale.

Messaggio di errore	Descrizione e azioni consigliate
Sessione TLS terminata	Il server syslog ha terminato la sessione TLS e StorageGRID non è in grado di rilevare il motivo. 1. Esaminare i log di debug forniti con questo errore per cercare di determinare la causa principale. 2. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 3. Se si utilizza TLS, verificare che anche il server syslog utilizzi TLS. Se si utilizza il protocollo TCP, verificare che anche il server syslog utilizzi il protocollo TCP. 4. Verificare che il bundle di certificati CA e il certificato client (se presente) siano compatibili con il certificato server dal server syslog. 5. Verificare che le identità nel certificato del server dal server syslog includano i valori IP o FQDN previsti.
Query dei risultati non riuscita	Il nodo di amministrazione utilizzato per la configurazione e il test del server syslog non è in grado di richiedere i risultati del test dai nodi elencati. Uno o più nodi potrebbero non essere attivi. 1. Seguire le procedure standard per la risoluzione dei problemi per assicurarsi che i nodi siano online e che tutti i servizi previsti siano in esecuzione. 2. Riavviare il servizio miscd sui nodi elencati.

Esaminare i registri di audit

Esaminare i registri di audit: Panoramica

Queste istruzioni contengono informazioni sulla struttura e sul contenuto dei messaggi di audit e dei registri di audit di StorageGRID. È possibile utilizzare queste informazioni per leggere e analizzare il registro di controllo dell'attività del sistema.

Queste istruzioni sono destinate agli amministratori responsabili della produzione di report sull'attività e sull'utilizzo del sistema che richiedono l'analisi dei messaggi di audit del sistema StorageGRID.

Per utilizzare il file di log di testo, è necessario disporre dell'accesso alla condivisione di audit configurata nel nodo di amministrazione.

Per informazioni sulla configurazione dei livelli dei messaggi di controllo e sull'utilizzo di un server syslog esterno, vedere "Configurare i messaggi di audit e le destinazioni dei log".

Controllare il flusso e la conservazione dei messaggi

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. È necessario comprendere in che modo questi messaggi di audit vengono spostati nel sistema StorageGRID `audit.log` file.

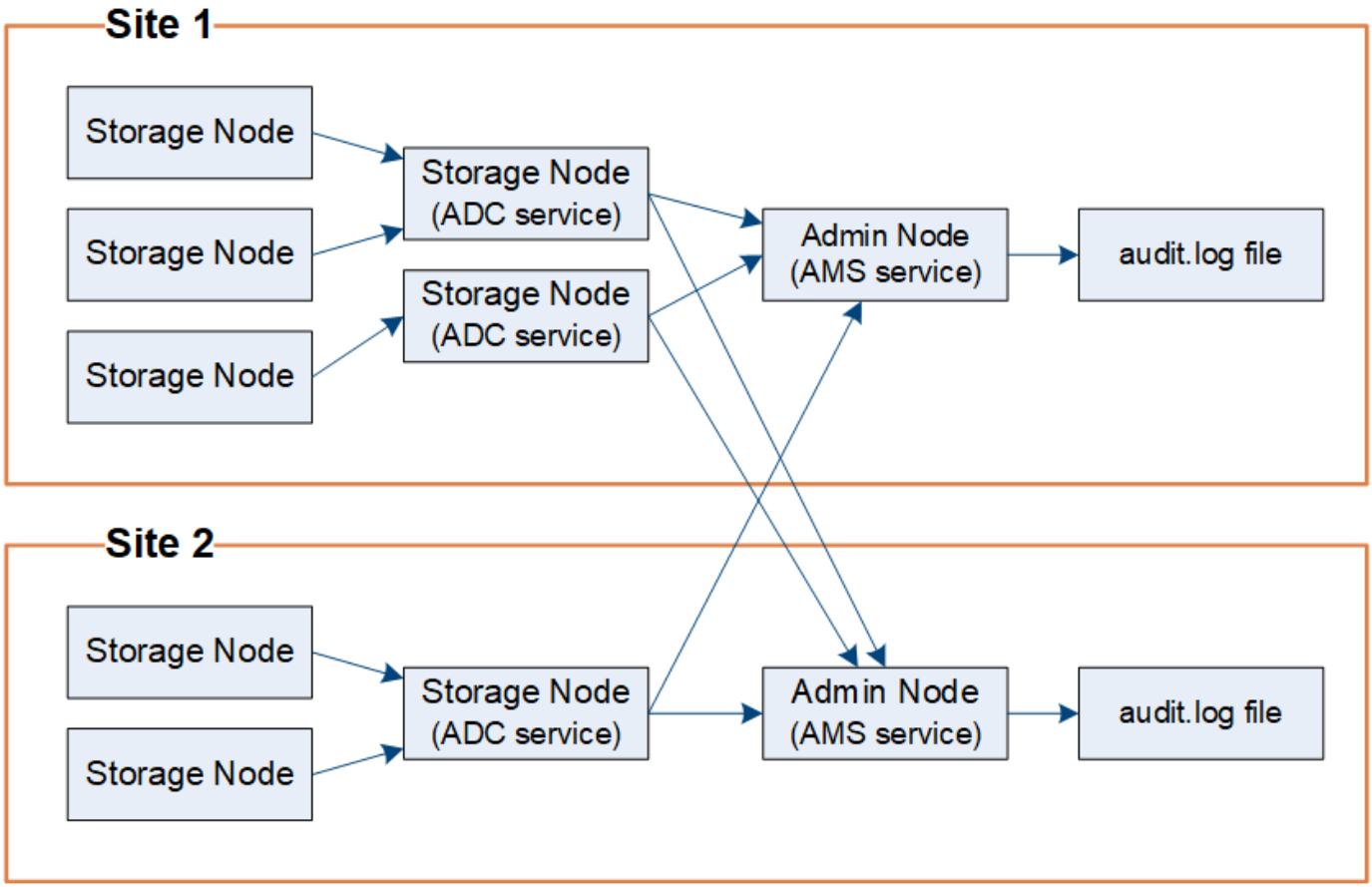
Controllare il flusso dei messaggi

I messaggi di audit vengono elaborati dai nodi di amministrazione e dai nodi di storage che dispongono di un servizio ADC (Administrative Domain Controller).

Come mostrato nel diagramma di flusso dei messaggi di audit, ciascun nodo StorageGRID invia i propri messaggi di audit a uno dei servizi ADC nel sito del data center. Il servizio ADC viene attivato automaticamente per i primi tre nodi di storage installati in ogni sito.

A sua volta, ogni servizio ADC agisce come un relay e invia la propria raccolta di messaggi di audit a ogni nodo amministrativo nel sistema StorageGRID, che fornisce a ciascun nodo amministrativo un record completo dell'attività del sistema.

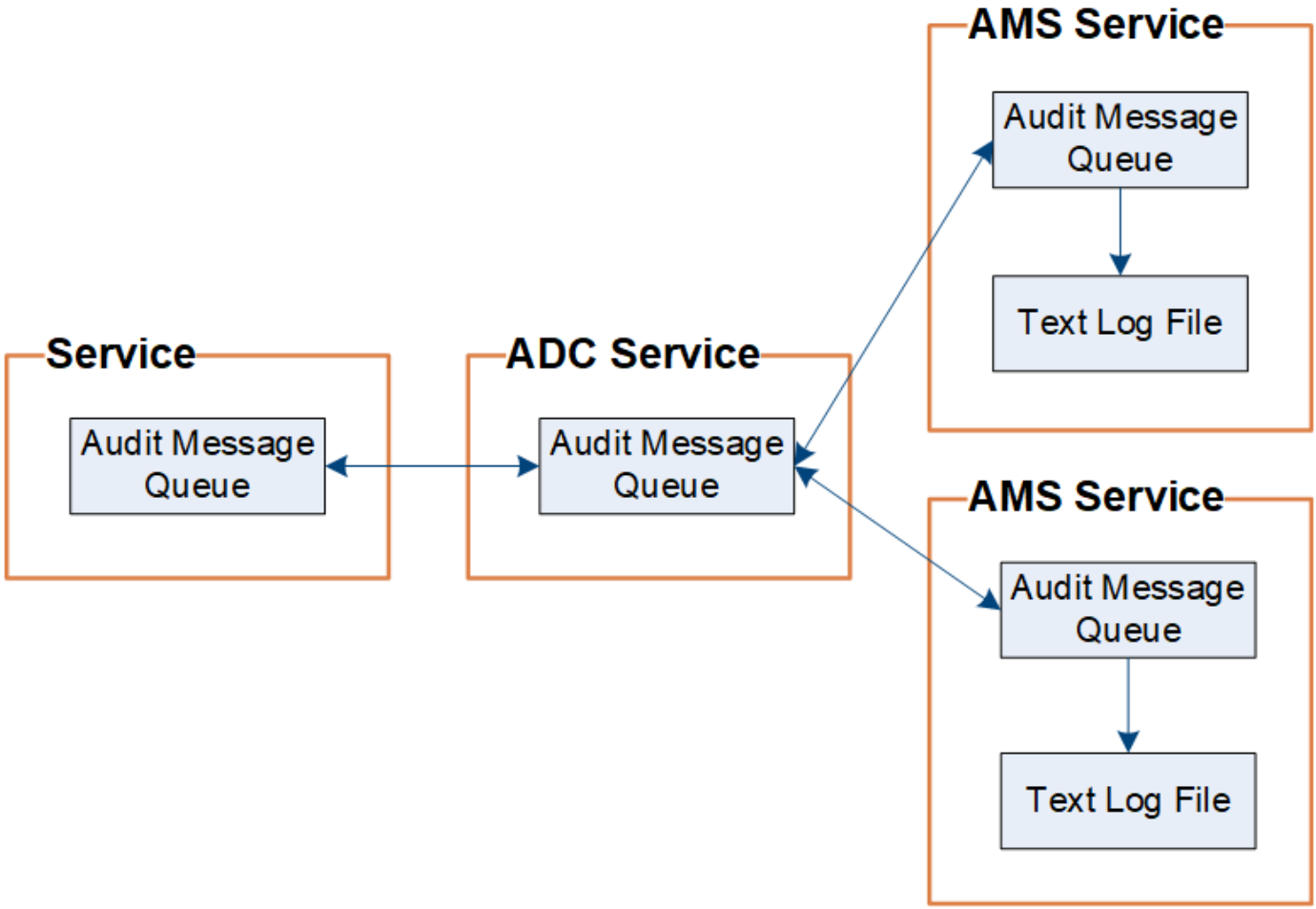
Ogni nodo amministrativo memorizza i messaggi di audit in file di log di testo; il file di log attivo viene denominato `audit.log`.



Controllare la conservazione dei messaggi

StorageGRID utilizza un processo di copia e cancellazione per garantire che non vengano persi messaggi di controllo prima di poter essere scritti nel registro di controllo.

Quando un nodo genera o inoltra un messaggio di audit, il messaggio viene memorizzato in una coda di messaggi di audit sul disco di sistema del nodo Grid. Una copia del messaggio viene sempre mantenuta in una coda di messaggi di audit fino a quando il messaggio non viene scritto nel file di log di audit nel nodo di amministrazione `/var/local/log` directory. In questo modo si evita la perdita di un messaggio di audit durante il trasporto.



La coda dei messaggi di audit può aumentare temporaneamente a causa di problemi di connettività di rete o di capacità di audit insufficiente. Man mano che le code aumentano, consumano più spazio disponibile in ogni nodo `/var/local/` directory. Se il problema persiste e la directory dei messaggi di controllo di un nodo diventa troppo piena, i singoli nodi assegneranno la priorità all'elaborazione del proprio backlog e diventeranno temporaneamente non disponibili per i nuovi messaggi.

In particolare, potrebbero verificarsi i seguenti comportamenti:

- Se il `/var/local/log` La directory utilizzata da un nodo amministratore diventa piena, il nodo amministratore viene contrassegnato come non disponibile per i nuovi messaggi di audit fino a quando la directory non è più piena. Le richieste dei client S3 e Swift non sono interessate. L'allarme XAMS (Unreachable Audit Repository) viene attivato quando un repository di audit non è raggiungibile.
- Se il `/var/local/` La directory utilizzata da un nodo di storage con il servizio ADC diventa piena al 92%, il nodo viene contrassegnato come non disponibile per i messaggi di controllo fino a quando la directory non è piena al 87%. Le richieste dei client S3 e Swift ad altri nodi non sono interessate. L'allarme NRLY (Available Audit Relay) viene attivato quando i relè di audit non sono raggiungibili.

> Se non sono disponibili nodi di storage con il servizio ADC, i nodi di storage memorizzano i messaggi di audit in locale in `/var/local/log/localaudit.log` file.

- Se il `/var/local/` La directory utilizzata da un nodo di storage diventa piena al 85%, il nodo inizia a rifiutare le richieste dei client S3 e Swift con `503 Service Unavailable`.

I seguenti tipi di problemi possono causare un aumento delle code dei messaggi di audit:

- Interruzione di un nodo amministrativo o di un nodo di storage con il servizio ADC. Se uno dei nodi del sistema non è attivo, i nodi rimanenti potrebbero diventare backlogged.
- Tasso di attività sostenuta che supera la capacità di audit del sistema.
- Il `/var/local/` Lo spazio su un nodo di storage ADC diventa pieno per motivi non correlati ai messaggi di audit. In questo caso, il nodo smette di accettare nuovi messaggi di audit e assegna la priorità al backlog corrente, che può causare backlog su altri nodi.

Avviso di coda di audit estesa e allarme di messaggi di audit in coda (AMQS)

Per facilitare il monitoraggio delle dimensioni delle code dei messaggi di controllo nel tempo, l'avviso **Large audit queue** e l'allarme AMQS legacy vengono attivati quando il numero di messaggi in una coda Storage Node o Admin Node raggiunge determinate soglie.

Se viene attivato l'avviso **Large audit queue** o l'allarme AMQS legacy, iniziare controllando il carico sul sistema. Se si è verificato un numero significativo di transazioni recenti, l'avviso e l'allarme devono essere risolti nel tempo e possono essere ignorati.

Se l'avviso o l'allarme persiste e aumenta di severità, visualizzare un grafico delle dimensioni della coda. Se il numero aumenta costantemente nel corso di ore o giorni, il carico di audit ha probabilmente superato la capacità di audit del sistema. Ridurre la velocità di funzionamento del client o diminuire il numero di messaggi di audit registrati modificando il livello di audit per le scritture del client e le letture del client su Error (errore) o Off. Vedere "Configurare i messaggi di audit e le destinazioni dei log".

Messaggi duplicati

Il sistema StorageGRID adotta un approccio conservativo in caso di guasto di rete o nodo. Per questo motivo, nel registro di controllo potrebbero essere presenti messaggi duplicati.

Accedere al file di log di audit

La condivisione di audit contiene il attivo `audit.log` file ed eventuali file di log di audit compressi. È possibile accedere ai file di log di controllo direttamente dalla riga di comando del nodo amministrativo.

Prima di iniziare

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

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Accedere alla directory contenente i file di log di controllo:

   ```
   cd /var/local/log
   ```

3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

Controllo della rotazione del file di log

I file di log di audit vengono salvati in un nodo di amministrazione `/var/local/log` directory. I file di log di audit attivi sono denominati `audit.log`.

> In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno. Vedere "Configurare i messaggi di audit e le destinazioni dei log".

Una volta al giorno, il attivo `audit.log` il file viene salvato e viene visualizzato un nuovo `audit.log` il file viene avviato. Il nome del file salvato indica quando è stato salvato, nel formato *`yyyy-mm-dd.txt`*. Se in un singolo giorno vengono creati più log di audit, i nomi dei file utilizzano la data in cui il file è stato salvato, aggiunto da un numero, nel formato *`yyyy-mm-dd.txt.n`*. Ad esempio, `2018-04-15.txt` e. `2018-04-15.txt.1` Sono il primo e il secondo file di log creati e salvati il 15 aprile 2018.

Dopo un giorno, il file salvato viene compresso e rinominato, nel formato *`yyyy-mm-dd.txt.gz`*, che conserva la data originale. Con il passare del tempo, ciò comporta un consumo di storage allocato per i registri di controllo sul nodo di amministrazione. Uno script monitora il consumo di spazio nel registro di controllo ed elimina i file di registro in base alle necessità per liberare spazio in `/var/local/log` directory. I registri di audit vengono cancellati in base alla data di creazione, con la data in cui sono stati cancellati per prima. È possibile monitorare le azioni dello script nel seguente file: `/var/local/log/manage-audit.log`.

In questo esempio viene visualizzato il valore attivo `audit.log` file del giorno precedente (`2018-04-15.txt`) e il file compresso per il giorno precedente (`2018-04-14.txt.gz`).

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

Formato del file di log di audit

Formato del file di log di audit: Panoramica

I file di log di audit si trovano in ogni nodo di amministrazione e contengono una raccolta di singoli messaggi di audit.

Ogni messaggio di audit contiene quanto segue:

- Il tempo universale coordinato (UTC) dell'evento che ha attivato il messaggio di audit (ATIM) in formato ISO 8601, seguito da uno spazio:

  `YYYY-MM-DDTHH:MM:SS.UUUUUU`, dove *`UUUUUU`* sono microsecondi.

- Il messaggio di audit, racchiuso tra parentesi quadre e che inizia con `AUDT`.

L'esempio seguente mostra tre messaggi di audit in un file di log di audit (interruzioni di riga aggiunte per la leggibilità). Questi messaggi sono stati generati quando un tenant ha creato un bucket S3 e aggiunto due oggetti a tale bucket.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Nel loro formato predefinito, i messaggi di audit nei file di log di audit non sono facili da leggere o interpretare. È possibile utilizzare "tool di verifica-spiegazione" per ottenere riepiloghi semplificati dei messaggi di audit nel log di audit. È possibile utilizzare "tool audit-sum" riepilogare il numero di operazioni di scrittura, lettura ed

eliminazione registrate e il tempo impiegato da tali operazioni.

Utilizzare lo strumento di verifica e spiegazione

È possibile utilizzare `audit-explain` strumento per convertire i messaggi di audit nel log di audit in un formato di facile lettura.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

A proposito di questa attività

Il `audit-explain` Tool, disponibile nel nodo di amministrazione principale, fornisce riepiloghi semplificati dei messaggi di audit in un registro di audit.

> Il `audit-explain` lo strumento è destinato principalmente all'utilizzo da parte del supporto tecnico durante le operazioni di troubleshooting. Elaborazione in corso `audit-explain` Le query possono consumare una grande quantità di potenza della CPU, con un conseguente impatto sulle operazioni StorageGRID.

Questo esempio mostra l'output tipico di `audit-explain` tool. Questi quattro "SPUT" I messaggi di audit sono stati generati quando il tenant S3 con ID account 92484777680322627870 utilizzava S3 PUT Requests per creare un bucket denominato "bucket1" e aggiungere tre oggetti a quel bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Il `audit-explain` lo strumento può eseguire le seguenti operazioni:

- Elaborazione di registri di audit semplici o compressi. Ad esempio:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Elaborazione simultanea di più file. Ad esempio:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/log/*
  ```

- Accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando `grep` comando o altro mezzo. Ad esempio:

```
grep SPUT audit.log | audit-explain

grep bucket-name audit.log | audit-explain
```

Poiché i log di audit possono essere molto grandi e lenti da analizzare, è possibile risparmiare tempo filtrando le parti che si desidera esaminare ed eseguire `audit-explain` sulle parti, invece dell'intero file.

> Il `audit-explain` lo strumento non accetta i file compressi come input di tipo pipped. Per elaborare i file compressi, specificare i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` per decomprimere prima i file. Ad esempio:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Utilizzare `help (-h)` per visualizzare le opzioni disponibili. Ad esempio:

```
$ audit-explain -h
```

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Immettere il seguente comando, dove `/var/local/log/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   Il `audit-explain` consente di stampare interpretazioni leggibili di tutti i messaggi contenuti nel file o nei file specificati.

   > Per ridurre le lunghezze delle linee e agevolare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se si desidera visualizzare gli indicatori di data e ora, utilizzare l'indicatore di data e ora (`-t`).

Utilizzare lo strumento audit-sum

È possibile utilizzare `audit-sum` strumento per contare i messaggi di audit di scrittura, lettura, testa ed eliminazione e per visualizzare il tempo (o la dimensione) minimo, massimo e medio per ciascun tipo di operazione.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- È necessario disporre di `Passwords.txt` file.

- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

A proposito di questa attività

Il `audit-sum` Tool, disponibile sul nodo di amministrazione primario, riepiloga il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo impiegato da tali operazioni.

> Il `audit-sum` lo strumento è destinato principalmente all'utilizzo da parte del supporto tecnico durante le operazioni di troubleshooting. Elaborazione in corso `audit-sum` Le query possono consumare una grande quantità di potenza della CPU, con un conseguente impatto sulle operazioni StorageGRID.

Questo esempio mostra l'output tipico di `audit-sum` tool. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Il `audit-sum` Lo strumento fornisce conteggi e tempi per i seguenti messaggi di audit S3, Swift e ILM in un registro di audit:

Codice	Descrizione	Fare riferimento a.
ARCT	Recupero archivio da Cloud-Tier	"ARCT: Recupero archivio da Cloud-Tier"
ASTT	Archivio Store Cloud-Tier	"ASCT: Archivio Store Cloud-Tier"
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Registra quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: Eliminazione avviata da ILM"
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket.	"SDEL: ELIMINAZIONE S3"

Codice	Descrizione	Fare riferimento a.
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	"SHEA: TESTA S3"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket.	"SPUT: S3 PUT"
WDEL	Eliminazione rapida: Registra una transazione riuscita per eliminare un oggetto o un container.	"WDEL: ELIMINAZIONE rapida"
WGET	Swift GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un container.	"WGET: Swift GET"
WHEA	Swift HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un container.	"WHEA: TESTA veloce"
WPUT	Swift PUT: Registra una transazione riuscita per creare un nuovo oggetto o container.	"WPUT: MESSA rapida"

Il `audit-sum` lo strumento può eseguire le seguenti operazioni:

- Elaborazione di registri di audit semplici o compressi. Ad esempio:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Elaborazione simultanea di più file. Ad esempio:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/log/*
```

- Accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando `grep` comando o altro mezzo. Ad esempio:

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

Questo strumento non accetta i file compressi come input di tipo pipped. Per elaborare i file compressi, specificare i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` per decomprimere prima i file. Ad esempio:

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

È possibile utilizzare le opzioni della riga di comando per riepilogare le operazioni sui bucket separatamente dalle operazioni sugli oggetti o per raggruppare i riepiloghi dei messaggi in base al nome del bucket, al periodo di tempo o al tipo di destinazione. Per impostazione predefinita, i riepiloghi mostrano il tempo di funzionamento minimo, massimo e medio, ma è possibile utilizzare `size (-s)` opzione per esaminare invece la dimensione dell'oggetto.

Utilizzare `help (-h)` per visualizzare le opzioni disponibili. Ad esempio:

```
$ audit-sum -h
```

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Se si desidera analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, testa ed eliminazione, attenersi alla seguente procedura:
   a. Immettere il seguente comando, dove `/var/local/log/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      Questo esempio mostra l'output tipico di `audit-sum` tool. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

In questo esempio, le operazioni SGET (S3 GET) sono le più lente in media a 1.13 secondi, ma le operazioni SGET e SPUT (S3 PUT) mostrano tempi lunghi nel caso peggiore di circa 1,770 secondi.

b. Per visualizzare le 10 operazioni di recupero più lente, utilizzare il comando grep per selezionare solo i messaggi SGET e aggiungere l'opzione di output lungo (`-l`) per includere i percorsi degli oggetti:

   ```
   grep SGET audit.log | audit-sum -l
   ```

   I risultati includono il tipo (oggetto o bucket) e il percorso, che consentono di eseguire il grep del log di audit per altri messaggi relativi a questi oggetti specifici.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
Da questo esempio di output, è possibile notare che le tre richieste S3 GET più lente erano per oggetti di dimensioni pari a circa 5 GB, che sono molto più grandi degli altri oggetti. Le grandi dimensioni rappresentano i tempi di recupero lenti dei casi peggiori.

3. Se si desidera determinare le dimensioni degli oggetti da acquisire e recuperare dalla griglia, utilizzare l'opzione size (dimensione) (`-s`):

   ```
   audit-sum -s audit.log
   ```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

In questo esempio, la dimensione media degli oggetti per SPUT è inferiore a 2.5 MB, ma la dimensione media per SGET è molto maggiore. Il numero di messaggi SPUT è molto superiore al numero di messaggi SGET, a indicare che la maggior parte degli oggetti non viene mai recuperata.

4. Se si desidera determinare se i recuperi sono stati lenti ieri:

   a. Eseguire il comando sul registro di controllo appropriato e utilizzare l'opzione group-by-time (`-gt`), seguito dal periodo di tempo (ad esempio, 15M, 1H, 10S):

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Questi risultati mostrano che S3 OTTIENE un incremento del traffico tra le 06:00 e le 07:00. Anche in questi casi, i tempi massimi e medi sono notevolmente più elevati e non sono aumentati gradualmente con l'aumentare del numero. Ciò suggerisce che la capacità è stata superata da qualche parte, ad esempio nella rete o nella capacità della rete di elaborare le richieste.

b. Per determinare le dimensioni degli oggetti recuperati ogni ora di ieri, aggiungere l'opzione size (dimensione) (`-s`) al comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Questi risultati indicano che si sono verificati alcuni recuperi molto grandi quando il traffico di recupero complessivo era al massimo.

c. Per ulteriori dettagli, utilizzare "tool di verifica-spiegazione" Per rivedere tutte le operazioni SGET in quell'ora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se si prevede che l'output del comando grep sia costituito da molte righe, aggiungere `less` comando per visualizzare il contenuto del file di log di audit una pagina (una schermata) alla volta.

5. Se si desidera determinare se le operazioni SPUT sui bucket sono più lente delle operazioni SPUT per gli oggetti:

a. Iniziare utilizzando `-go` opzione, che raggruppa i messaggi per le operazioni a oggetti e a bucket separatamente:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

I risultati mostrano che le operazioni SPUT per i bucket hanno caratteristiche di performance diverse rispetto alle operazioni SPUT per gli oggetti.

b. Per determinare quali bucket hanno le operazioni SPUT più lente, utilizzare `-gb` opzione, che raggruppa i messaggi per bucket:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Per determinare quali bucket hanno la dimensione maggiore dell'oggetto SPUT, utilizzare entrambi i campi `-gb` e a. `-s` opzioni:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Formato del messaggio di audit

Formato del messaggio di audit: Panoramica

I messaggi di audit scambiati all'interno del sistema StorageGRID includono informazioni standard comuni a tutti i messaggi e contenuti specifici che descrivono l'evento o l'attività da segnalare.

Se le informazioni di riepilogo fornite da "audit-spiegare" e. "audit-sum" gli strumenti non sono sufficienti. fare riferimento a questa sezione per comprendere il formato generale di tutti i messaggi di audit.

Di seguito viene riportato un esempio di messaggio di audit che potrebbe essere visualizzato nel file di log dell'audit:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Ogni messaggio di audit contiene una stringa di elementi di attributo. L'intera stringa è racchiusa tra parentesi (`[ ]`), e ogni elemento di attributo nella stringa ha le seguenti caratteristiche:

- Racchiuso tra parentesi `[ ]`
- Introdotto dalla stringa `AUDT`, che indica un messaggio di audit
- Senza delimitatori (senza virgole o spazi) prima o dopo
- Terminato da un carattere di avanzamento riga `\n`

Ogni elemento include un codice di attributo, un tipo di dati e un valore che vengono riportati in questo formato:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Il numero di elementi di attributo nel messaggio dipende dal tipo di evento del messaggio. Gli elementi dell'attributo non sono elencati in un ordine specifico.

L'elenco seguente descrive gli elementi degli attributi:

- `ATTR` è un codice di quattro caratteri per l'attributo da segnalare. Esistono alcuni attributi comuni a tutti i messaggi di audit e ad altri specifici degli eventi.
- `type` È un identificatore di quattro caratteri del tipo di dati di programmazione del valore, ad esempio UI64, FC32 e così via. Il tipo è racchiuso tra parentesi `( )`.
- `value` è il contenuto dell'attributo, in genere un valore numerico o di testo. I valori seguono sempre i due punti (`:`). I valori del tipo di dati CSTR sono racchiusi tra virgolette doppie " ".

Tipi di dati

Per memorizzare le informazioni nei messaggi di audit vengono utilizzati diversi tipi di dati.

Tipo	Descrizione
UI32	Intero senza segno (32 bit); può memorizzare i numeri da 0 a 4,294,967,295.
UI64	Numero intero doppio senza segno (64 bit); può memorizzare i numeri da 0 a 18,446,744,073,709,551,615.
FC32	Costante di quattro caratteri; un valore intero senza segno a 32 bit rappresentato da quattro caratteri ASCII, ad esempio "ABCD".
IPAD	Utilizzato per gli indirizzi IP.
CSTR	Matrice a lunghezza variabile di caratteri UTF-8. È possibile eseguire l'escape dei caratteri con le seguenti convenzioni: • La barra rovesciata è • Il ritorno a capo è • Le virgolette doppie sono ". • L'avanzamento riga (nuova riga) è il n. • I caratteri possono essere sostituiti dai rispettivi equivalenti esadecimali (nel formato HH, dove HH è il valore esadecimale che rappresenta il carattere).

Dati specifici dell'evento

Ogni messaggio di audit nel registro di audit registra i dati specifici di un evento di sistema.

Dopo l'apertura `[AUDT:` container che identifica il messaggio stesso, il successivo set di attributi fornisce informazioni sull'evento o sull'azione descritti dal messaggio di audit. Questi attributi sono evidenziati nel seguente esempio:

2018-12-05T08:24:45,921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[ORA\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA="\]
\[SUSR\(CSTR\):"urn:sgws:Identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"ACCOUNT"\]\[S3BK\(CSTR\):"BUCKET"\]
\[S3KY\(CSTR\):"oggetto"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]

Il `ATYP` element (sottolineato nell'esempio) identifica l'evento che ha generato il messaggio. Questo messaggio di esempio include "SHEA" Codice del messaggio ([ATYP(FC32):SHEA]), che indica che è stato generato da una richiesta S3 HEAD riuscita.

Elementi comuni nei messaggi di audit

Tutti i messaggi di audit contengono gli elementi comuni.

Codice	Tipo	Descrizione
IN MEZZO	FC32	Module ID (ID modulo): Identificatore di quattro caratteri dell'ID modulo che ha generato il messaggio. Indica il segmento di codice all'interno del quale è stato generato il messaggio di audit.
ANID	UI32	Node ID (ID nodo): L'ID del nodo della griglia assegnato al servizio che ha generato il messaggio. A ciascun servizio viene assegnato un identificatore univoco al momento della configurazione e dell'installazione del sistema StorageGRID. Impossibile modificare questo ID.
ASE	UI64	Audit Session Identifier (identificatore sessione di audit): Nelle release precedenti, questo elemento indica l'ora in cui il sistema di audit è stato inizializzato dopo l'avvio del servizio. Questo valore di tempo è stato misurato in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). **Nota:** questo elemento è obsoleto e non compare più nei messaggi di audit.

Codice	Tipo	Descrizione
ASQN	UI64	Sequence Count (Conteggio sequenze): Nelle release precedenti, questo contatore è stato incrementato per ogni messaggio di audit generato sul nodo della griglia (ANID) e azzerato al riavvio del servizio. **Nota:** questo elemento è obsoleto e non compare più nei messaggi di audit.
ATID	UI64	Trace ID (ID traccia): Identificatore condiviso dalla serie di messaggi attivati da un singolo evento.
ATIM	UI64	Timestamp: L'ora in cui è stato generato l'evento che ha attivato il messaggio di audit, misurata in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Si noti che la maggior parte degli strumenti disponibili per la conversione dell'indicatore data e ora in data e ora locali si basano su millisecondi. Potrebbe essere richiesto l'arrotondamento o il troncamento dell'indicatore data e ora registrato. L'ora di lettura umana visualizzata all'inizio del messaggio di audit in `audit.log` File è l'attributo ATIM nel formato ISO 8601. La data e l'ora sono rappresentate come *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, dove il `T` è un carattere di stringa letterale che indica l'inizio del segmento temporale della data. *`UUUUUU`* sono microsecondi.
ATYP	FC32	Event Type (tipo di evento): Identificatore di quattro caratteri dell'evento registrato. Questo regola il contenuto "payload" del messaggio: Gli attributi che sono inclusi.
MEDIA	UI32	Version (versione): La versione del messaggio di audit. Man mano che il software StorageGRID si evolve, le nuove versioni dei servizi potrebbero incorporare nuove funzionalità nei report di audit. Questo campo consente la compatibilità con le versioni precedenti del servizio AMS per l'elaborazione dei messaggi provenienti da versioni precedenti dei servizi.
RSLT	FC32	Risultato: Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

Esempi di messaggi di audit

È possibile trovare informazioni dettagliate in ciascun messaggio di audit. Tutti i messaggi di audit utilizzano lo stesso formato.

Di seguito è riportato un messaggio di controllo di esempio come potrebbe essere visualizzato nella `audit.log` file:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Il messaggio di audit contiene informazioni sull'evento registrato, nonché informazioni sul messaggio di audit stesso.

Per identificare l'evento registrato dal messaggio di audit, cercare l'attributo ATYP (evidenziato di seguito):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

Il valore dell'attributo ATYP è SPUT. "SPUT" Rappresenta una transazione S3 PUT, che registra l'acquisizione di un oggetto in un bucket.

Il seguente messaggio di audit mostra anche il bucket a cui è associato l'oggetto:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Per scoprire quando si è verificato l'evento PUT, prendere nota dell'indicatore orario UTC (Universal Coordinated Time) all'inizio del messaggio di audit. Questo valore è una versione leggibile dell'attributo ATIM del messaggio di audit stesso:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM registra il tempo, in microsecondi, dall'inizio dell'epoca UNIX. Nell'esempio, il valore `1405631878959669` Tradotto a Giovedì, 17-lug-2014 21:17:59 UTC.

Messaggi di audit e ciclo di vita degli oggetti

Quando vengono generati i messaggi di audit?

I messaggi di audit vengono generati ogni volta che un oggetto viene acquisito, recuperato o eliminato. È possibile identificare queste transazioni nel registro di controllo individuando i messaggi di audit specifici dell'API (S3 o Swift).

I messaggi di audit sono collegati tramite identificatori specifici di ciascun protocollo.

Protocollo	Codice
Collegamento delle operazioni S3	S3BK (bucket), S3KY (chiave) o entrambi
Collegamento delle operazioni Swift	WCON (contenitore), WOBJ (oggetto) o entrambi
Collegamento delle operazioni interne	CBID (identificatore interno dell'oggetto)

Tempistiche dei messaggi di audit

A causa di fattori come le differenze di tempo tra i nodi della griglia, le dimensioni degli oggetti e i ritardi di rete, l'ordine dei messaggi di controllo generati dai diversi servizi può variare rispetto a quello mostrato negli esempi di questa sezione.

Nodi di archiviazione

La serie di messaggi di audit generati quando un nodo di archiviazione invia dati a oggetti a un sistema di storage di archiviazione esterno è simile a quella dei nodi di storage, ad eccezione del fatto che non esiste alcun messaggio SCMT (Store Object Commit), Inoltre, vengono generati i messaggi ATCE (Archive Object Store Begin) e ASCE (Archive Object Store End) per ogni copia archiviata dei dati dell'oggetto.

La serie di messaggi di controllo generati quando un nodo di archiviazione recupera i dati degli oggetti da un sistema di storage di archiviazione esterno è simile a quella dei nodi di storage, ad eccezione del fatto che i messaggi ARCB (Archive Object Retrieve Begin) e ARCE (Archive Object Retrieve End) vengono generati per ogni copia recuperata dei dati degli oggetti.

La serie di messaggi di controllo generati quando un nodo di archiviazione elimina i dati degli oggetti da un

sistema di storage di archiviazione esterno è simile a quella dei nodi di storage, ad eccezione del fatto che non è presente alcun messaggio SREM (Object Store Remove) e che è presente un messaggio AREM (Archive Object Remove) per ogni richiesta di eliminazione.

Transazioni di acquisizione degli oggetti

È possibile identificare le transazioni di acquisizione dei client nel registro di audit individuando i messaggi di audit specifici dell'API (S3 o Swift).

Non tutti i messaggi di audit generati durante una transazione di acquisizione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di acquisizione.

S3: Acquisizione di messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SPUT	Transazione S3 PUT	Una transazione S3 PUT ingest è stata completata correttamente.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regole oggetto soddisfatte	Il criterio ILM è stato soddisfatto per questo oggetto.	CBID	"ORLM: Regole oggetto soddisfatte"

Acquisizione rapida di messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
WPUT	Transazione SWIFT PUT	Una transazione Swift PUT Ingest è stata completata correttamente.	CBID, WCON, WOBJ	"WPUT: MESSA rapida"
ORLM	Regole oggetto soddisfatte	Il criterio ILM è stato soddisfatto per questo oggetto.	CBID	"ORLM: Regole oggetto soddisfatte"

Esempio: Acquisizione di oggetti S3

La serie di messaggi di controllo riportata di seguito è un esempio dei messaggi di controllo generati e salvati nel registro di controllo quando un client S3 acquisisce un oggetto in un nodo di storage (servizio LDR).

In questo esempio, il criterio ILM attivo include la regola ILM Make 2 Copies.

> Non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di acquisizione S3 (SPUT).

Questo esempio presuppone che sia stato precedentemente creato un bucket S3.

SPUT: S3 PUT

Il messaggio SPUT viene generato per indicare che è stata emessa una transazione S3 PUT per creare un

oggetto in un bucket specifico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Regole oggetto soddisfatte

Il messaggio ORLM indica che il criterio ILM è stato soddisfatto per questo oggetto. Il messaggio include il CBID dell'oggetto e il nome della regola ILM applicata.

Per gli oggetti replicati, il campo LOCS include l'ID del nodo LDR e l'ID del volume delle posizioni degli oggetti.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Per gli oggetti sottoposti a erasure coding, il campo LOCS include l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Il campo PATH include informazioni sul bucket S3 e sulla chiave o informazioni sul container Swift e sull'oggetto, a seconda dell'API utilizzata.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Transazioni di eliminazione degli oggetti

È possibile identificare le transazioni di eliminazione degli oggetti nel registro di audit individuando i messaggi di audit specifici dell'API (S3 e Swift).

Non tutti i messaggi di audit generati durante una transazione di eliminazione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di eliminazione.

S3 eliminare i messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SDEL	S3 Elimina	Richiesta di eliminazione dell'oggetto da un bucket.	CBID, S3KY	"SDEL: ELIMINAZIONE S3"

Eliminazione rapida dei messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
WDEL	Eliminazione rapida	Richiesta di eliminazione dell'oggetto da un container o dal container.	CBID, WOBJ	"WDEL: ELIMINAZIONE rapida"

Esempio: Eliminazione di oggetti S3

Quando un client S3 elimina un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.

> Non tutti i messaggi di audit generati durante una transazione di eliminazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di eliminazione S3 (SDEL).

SDEL: S3 Elimina

L'eliminazione degli oggetti ha inizio quando il client invia una richiesta DeleteObject a un servizio LDR. Il messaggio contiene il bucket da cui eliminare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificare l'oggetto.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Transazioni di recupero degli oggetti

È possibile identificare le transazioni di recupero degli oggetti nel registro di audit individuando i messaggi di audit specifici dell'API (S3 e Swift).

Non tutti i messaggi di audit generati durante una transazione di recupero sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di recupero.

Messaggi di controllo per il recupero S3

Codice	Nome	Descrizione	Traccia	Vedere
SGET	S3 GET	Richiesta di recupero di un oggetto da un bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Messaggi di audit per il recupero rapido

Codice	Nome	Descrizione	Traccia	Vedere
WGET	OTTENERE rapidamente	Richiesta di recupero di un oggetto da un container.	CBID, WCON, WOBJ	"WGET: Swift GET"

Esempio: Recupero di oggetti S3

Quando un client S3 recupera un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.

Si noti che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di recupero S3 (SGET).

SGET: S3 GET

Il recupero degli oggetti ha inizio quando il client invia una richiesta GetObject a un servizio LDR. Il messaggio contiene il bucket da cui recuperare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificare l'oggetto.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se la policy bucket lo consente, un client può recuperare in modo anonimo oggetti o recuperare oggetti da un bucket di proprietà di un account tenant diverso. Il messaggio di audit contiene informazioni sull'account tenant del proprietario del bucket, in modo da poter tenere traccia di queste richieste anonime e multiaccount.

Nel seguente messaggio di esempio, il client invia una richiesta GetObject per un oggetto memorizzato in un bucket che non possiede. I valori di SBAI e SBAC registrano l'ID e il nome dell'account tenant del bucket Owner, che differiscono dall'ID dell'account tenant e dal nome del client registrati in S3AI e SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Esempio: S3 selezionare su un oggetto

Quando un client S3 esegue una query S3 Select su un oggetto, i messaggi di audit vengono generati e salvati nel registro di audit.

Si noti che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione S3 Select (SelectObjectContent).

Ogni query genera due messaggi di audit: Uno che esegue l'autorizzazione della richiesta S3 Select (il campo S3SR è impostato su "Select") e un'operazione GET standard successiva che recupera i dati dallo storage durante l'elaborazione.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messaggi di aggiornamento dei metadati

I messaggi di audit vengono generati quando un client S3 aggiorna i metadati di un oggetto.

I metadati S3 aggiornano i messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SUPD	Metadati S3 aggiornati	Generato quando un client S3 aggiorna i metadati di un oggetto acquisito.	CBID, S3KY, HTRH	"SUPD: Metadati S3 aggiornati"

Esempio: Aggiornamento dei metadati S3

L'esempio mostra una transazione riuscita per aggiornare i metadati di un oggetto S3 esistente.

SUPD: Aggiornamento dei metadati S3

Il client S3 effettua una richiesta (SUPD) per aggiornare i metadati specificati (`x-amz-meta-\*`) Per l'oggetto S3 (S3KY). In questo esempio, le intestazioni delle richieste sono incluse nel campo HTRH perché è stato configurato come intestazione del protocollo di audit (**CONFIGURAZIONE** > **monitoraggio** > **server di audit e syslog**). Vedere "Configurare i messaggi di audit e le destinazioni dei log".

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Messaggi di audit

Messaggi di audit: Panoramica

Le descrizioni dettagliate dei messaggi di controllo restituiti dal sistema sono elencate nelle sezioni seguenti. Ciascun messaggio di audit viene elencato per primo in una tabella che raggruppa i messaggi correlati in base alla classe di attività rappresentata dal messaggio. Questi raggruppamenti sono utili sia per comprendere i tipi di attività sottoposte a audit che per selezionare il tipo di filtro dei messaggi di audit desiderato.

I messaggi di audit sono anche elencati in ordine alfabetico in base ai codici a quattro caratteri. Questo elenco alfabetico consente di trovare informazioni su messaggi specifici.

I codici a quattro caratteri utilizzati in questo capitolo sono i valori ATYP presenti nei messaggi di controllo, come mostrato nel seguente messaggio di esempio:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Per informazioni sull'impostazione dei livelli dei messaggi di controllo, sulla modifica delle destinazioni dei log e sull'utilizzo di un server syslog esterno per le informazioni di controllo, vedere "Configurare i messaggi di audit e le destinazioni dei log"

Controllare le categorie dei messaggi

Messaggi di audit del sistema

I messaggi di audit appartenenti alla categoria di audit del sistema vengono utilizzati per gli eventi correlati al sistema di audit stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema (attività della griglia) e alle operazioni di backup del servizio.

Codice	Titolo e descrizione del messaggio	Vedere
ECMC	Manca un frammento di dati con erasure coding: Indica che è stato rilevato un frammento di dati con erasure coding mancante.	"ECMC: Frammento di dati con codice di cancellazione mancante"
ECOC	Fragment di dati con erasure coding corrotto: Indica che è stato rilevato un frammento di dati sottoposto a erasure coding corrotto.	"ECOC: Frammento di dati con codice di cancellazione corrotto"
ETAF	Autenticazione di sicurezza non riuscita: Tentativo di connessione con Transport Layer Security (TLS) non riuscito.	"ETAF: Autenticazione di sicurezza non riuscita"
GNRG	Registrazione GNDS: Un servizio aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.	"GNRG: Registrazione GNDS"
NUR	Annullamento registrazione GNDS: Un servizio non si è registrato dal sistema StorageGRID.	"GNUR: Annullamento registrazione GNDS"
GTED	Grid Task Ended (attività griglia terminata): Il servizio CMN ha terminato l'elaborazione dell'attività Grid.	"GTED: Task Grid terminato"
GTST	Grid Task Started (attività griglia avviata): Il servizio CMN ha avviato l'elaborazione dell'attività Grid.	"GTST: Task Grid avviato"
GTSU	Grid Task Submitted (attività griglia inviata): È stata inviata un'attività Grid al servizio CMN.	"GTSU: Task Grid inviato"

Codice	Titolo e descrizione del messaggio	Vedere
LLST	Location Lost (posizione persa): Questo messaggio di audit viene generato quando una posizione viene persa.	"LLST: Località persa"
OLST	Object Lost (oggetti persi): Non è possibile individuare un oggetto richiesto all'interno del sistema StorageGRID.	"OLST: Il sistema ha rilevato un oggetto perso"
SADD	Security Audit Disable (Disattiva controllo protezione): La registrazione del messaggio di controllo è stata disattivata.	"SADD: Disattivazione dell'audit di sicurezza"
SADE	Security Audit Enable (attiva controllo di sicurezza): La registrazione del messaggio di controllo è stata ripristinata.	"SADE: Abilitazione controllo di sicurezza"
SVRF	Verifica archivio oggetti non riuscita: Un blocco di contenuto non ha superato i controlli di verifica.	"SVRF: Verifica archivio oggetti non riuscita"
SVRU	Object Store Verify Unknown (verifica archivio oggetti sconosciuto): Dati di oggetti imprevisti rilevati nell'archivio oggetti.	"SVRU: Verifica archivio oggetti sconosciuta"
SYSD	Node Stop (arresto nodo): È stato richiesto lo spegnimento.	"SYSD: Interruzione nodo"
SIST	Node stopping (interruzione nodo): Un servizio ha avviato un'interruzione senza interruzioni.	"SYST: Interruzione del nodo"
SISU	Node Start (Avvio nodo): Un servizio avviato; la natura dello shutdown precedente viene indicata nel messaggio.	"SYSU: Avvio nodo"

Messaggi di audit dello storage a oggetti

I messaggi di audit appartenenti alla categoria di audit dello storage a oggetti vengono utilizzati per gli eventi correlati allo storage e alla gestione degli oggetti all'interno del sistema StorageGRID. Tra cui storage a oggetti e recuperi, trasferimenti da grid-node a grid-node e verifiche.

Codice	Descrizione	Vedere
APCT	Eliminazione dell'archivio dal livello cloud: I dati degli oggetti archiviati vengono cancellati da un sistema storage di archiviazione esterno, che si connette a StorageGRID tramite l'API S3.	"APCT: Eliminazione dell'archivio dal Cloud-Tier"

Codice	Descrizione	Vedere
ARCB	Archive Object Retrieve Begin (inizio recupero oggetto archivio): Il servizio ARC avvia il recupero dei dati oggetto dal sistema di storage di archiviazione esterno.	"ARCB: Inizio recupero oggetto archivio"
ARCE	Archive Object Retrieve End (fine recupero oggetto archivio): I dati dell'oggetto sono stati recuperati da un sistema di storage di archiviazione esterno e il servizio ARC segnala lo stato dell'operazione di recupero.	"ARCE: Fine recupero oggetto archivio"
ARCT	Recupero archivio dal livello cloud: I dati degli oggetti archiviati vengono recuperati da un sistema storage di archiviazione esterno, che si connette a StorageGRID tramite l'API S3.	"ARCT: Recupero archivio da Cloud-Tier"
AREM	Archive Object Remove (Rimozione oggetto archivio): Un blocco di contenuto è stato eliminato correttamente o senza successo dal sistema di storage di archiviazione esterno.	"AREM: Rimozione dell'oggetto di archiviazione"
ASCE	Archive Object Store End (fine archivio oggetti): Un blocco di contenuto è stato scritto nel sistema di storage di archiviazione esterno e il servizio ARC segnala lo stato dell'operazione di scrittura.	"ASCE: Fine archivio oggetti"
ASTT	Livello cloud archivio: I dati degli oggetti vengono memorizzati in un sistema storage di archiviazione esterno, che si connette a StorageGRID tramite l'API S3.	"ASCT: Archivio Store Cloud-Tier"
ATCE	Archive Object Store Begin (inizio archivio: Scrittura di un blocco di contenuto in uno storage di archiviazione esterno).	"ATCE: Inizio archivio oggetti"
AVCC	Archive Validate Cloud-Tier Configuration (convalida archivio configurazione livello cloud): Le impostazioni dell'account e del bucket fornite sono state validate correttamente o senza successo.	"AVCC: Convalida archivio configurazione Cloud-Tier"
BROR	Bucket Read Only Request (richiesta di sola lettura bucket): Un bucket è entrato o è uscito dalla modalità di sola lettura.	"BROR: Richiesta di sola lettura bucket"
CBSE	Object Send End (fine invio oggetto): L'entità di origine ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	"CBSE: Fine invio oggetto"

Codice	Descrizione	Vedere
CBRE	Object Receive End (fine ricezione oggetto): L'entità di destinazione ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	"CBRE: Fine ricezione oggetto"
CGRR	Richiesta di replica cross-grid: StorageGRID ha tentato un'operazione di replica cross-grid per replicare gli oggetti tra bucket in una connessione a federazione di grid.	"CGRR: Richiesta di replica cross-grid"
EBDL	Empty bucket Delete (Elimina bucket vuoto): Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione bucket vuoto).	"EBDL: Eliminazione bucket vuoto"
EBKR	Empty bucket Request (richiesta bucket vuoto): Un utente ha inviato una richiesta per attivare o disattivare il bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di oggetti).	"EBKR: Richiesta bucket vuoto"
SCMT	Commit dell'archivio oggetti: Un blocco di contenuto è stato completamente memorizzato e verificato e può essere richiesto.	"SCMT: Richiesta di commit dell'archivio di oggetti"
SREM	Rimozione archivio oggetti: Un blocco di contenuto è stato cancellato da un nodo griglia e non può più essere richiesto direttamente.	"SREM: Rimozione dell'archivio di oggetti"

Messaggi di audit in lettura del client

I messaggi di audit in lettura del client vengono registrati quando un'applicazione client S3 o Swift richiede di recuperare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
S3SL	S3 Select request (richiesta S3 Select): Registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere messaggi di errore e dettagli del codice di errore. La richiesta potrebbe non essere riuscita.	Client S3	"S3SL: Richiesta S3 Select"
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket. **Nota:** se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SGET: S3 GET"

Codice	Descrizione	Utilizzato da	Vedere
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	Client S3	"SHEA: TESTA S3"
WGET	Swift GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un container.	Client Swift	"WGET: Swift GET"
WHEA	Swift HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un container.	Client Swift	"WHEA: TESTA veloce"

Messaggi di audit di scrittura del client

I messaggi di audit di scrittura del client vengono registrati quando un'applicazione client S3 o Swift richiede di creare o modificare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
OVWR	Object Overwrite: Registra una transazione per sovrascrivere un oggetto con un altro oggetto.	S3 e Swift	"OVWR: Sovrascrittura degli oggetti"
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket. **Nota:** se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SDEL: ELIMINAZIONE S3"
SPOS	S3 POST: Registra una transazione riuscita per ripristinare un oggetto dallo storage AWS Glacier a un Cloud Storage Pool.	Client S3	"SPOS: POST S3"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket. **Nota:** se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SPUT: S3 PUT"
SUPD	S3 Metadata Updated: Registra una transazione riuscita per aggiornare i metadati di un oggetto o bucket esistente.	Client S3	"SUPD: Metadati S3 aggiornati"
WDEL	Eliminazione rapida: Registra una transazione riuscita per eliminare un oggetto o un container.	Client Swift	"WDEL: ELIMINAZIONE rapida"
WPUT	Swift PUT: Registra una transazione riuscita per creare un nuovo oggetto o container.	Client Swift	"WPUT: MESSA rapida"

Messaggio di audit della gestione

La categoria Gestione registra le richieste degli utenti all'API di gestione.

Codice	Titolo e descrizione del messaggio	Vedere
MGAU	Messaggio di audit API di gestione: Un registro delle richieste degli utenti.	"MGAU: Messaggio di audit della gestione"

Messaggi di controllo ILM

I messaggi di audit appartenenti alla categoria di audit ILM vengono utilizzati per gli eventi relativi alle operazioni ILM (Information Lifecycle Management).

Codice	Titolo e descrizione del messaggio	Vedere
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Questo messaggio di controllo viene generato quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: Eliminazione avviata da ILM"
LKCU	Pulitura oggetto sovrascritto. Questo messaggio di audit viene generato quando un oggetto sovrascritto viene rimosso automaticamente per liberare spazio di storage.	"LKCU: Pulitura oggetto sovrascritta"
ORLM	Regole oggetto soddisfatte: Questo messaggio di audit viene generato quando i dati oggetto vengono memorizzati come specificato dalle regole ILM.	"ORLM: Regole oggetto soddisfatte"

Riferimento del messaggio di audit

APCT: Eliminazione dell'archivio dal Cloud-Tier

Questo messaggio viene generato quando i dati degli oggetti archiviati vengono cancellati da un sistema di storage di archiviazione esterno, che si connette a StorageGRID attraverso l'API S3.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto eliminato.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto in byte. Restituisce sempre 0.
RSLT	Codice risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.

Codice	Campo	Descrizione
SUID	Identificatore univoco dello storage	Identificatore univoco (UUID) del cloud-Tier da cui l'oggetto è stato cancellato.

ARCB: Inizio recupero oggetto archivio

Questo messaggio viene generato quando viene effettuata una richiesta di recupero dei dati dell'oggetto archiviato e inizia il processo di recupero. Le richieste di recupero vengono elaborate immediatamente, ma possono essere riordinate per migliorare l'efficienza del recupero da supporti lineari come il nastro.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto da recuperare dal sistema di storage di archiviazione esterno.
RSLT	Risultato	Indica il risultato dell'avvio del processo di recupero dell'archivio. Il valore attualmente definito è:SUCS: La richiesta di contenuto è stata ricevuta e messa in coda per il recupero.

Questo messaggio di audit indica l'ora del recupero di un archivio. Consente di associare il messaggio a un corrispondente messaggio ARCE End per determinare la durata del recupero dell'archivio e se l'operazione è stata eseguita correttamente.

ARCE: Fine recupero oggetto archivio

Questo messaggio viene generato quando viene completato un tentativo da parte del nodo di archiviazione di recuperare i dati dell'oggetto da un sistema di storage di archiviazione esterno. Se l'esito è positivo, il messaggio indica che i dati dell'oggetto richiesti sono stati letti completamente dalla posizione di archiviazione ed è stato verificato correttamente. Una volta recuperati e verificati i dati dell'oggetto, questi vengono consegnati al servizio richiedente.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto da recuperare dal sistema di storage di archiviazione esterno.
VLID	Identificatore del volume	L'identificativo del volume su cui sono stati archiviati i dati. Se non viene trovata una posizione di archiviazione per il contenuto, viene restituito un ID volume pari a 0.

Codice	Campo	Descrizione
RSLT	Risultato del recupero	Lo stato di completamento del processo di recupero dell'archivio: • SUC: Riuscito • VRFL: Non riuscito (errore di verifica dell'oggetto) • ARUN: Errore (sistema storage di archiviazione esterno non disponibile) • CANC: Non riuscito (operazione di recupero annullata) • GERR: Failed (errore generale)

La corrispondenza di questo messaggio con il corrispondente messaggio ARCB può indicare il tempo necessario per eseguire il recupero dell'archivio. Questo messaggio indica se il recupero è riuscito e, in caso di errore, la causa del mancato recupero del blocco di contenuto.

ARCT: Recupero archivio da Cloud-Tier

Questo messaggio viene generato quando i dati degli oggetti archiviati vengono recuperati da un sistema di storage di archiviazione esterno, che si connette a StorageGRID attraverso l'API S3.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto recuperato.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto in byte. Il valore è preciso solo per i recuperi riusciti.
RSLT	Codice risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.
SUID	Identificatore univoco dello storage	Identificatore univoco (UUID) del sistema di storage di archiviazione esterno.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.

AREM: Rimozione dell'oggetto di archiviazione

Il messaggio di controllo Archive Object Remove (Rimozione oggetto archivio) indica che un blocco di contenuto è stato eliminato correttamente o senza successo da un nodo di archivio. Se il risultato è positivo, il nodo di archiviazione ha informato correttamente il sistema di storage di archiviazione esterno che StorageGRID ha rilasciato una posizione dell'oggetto. La rimozione dell'oggetto dal sistema di storage di archiviazione esterno dipende dal tipo di sistema e dalla relativa configurazione.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuti da recuperare dal sistema di supporti di archiviazione esterno.
VLID	Identificatore del volume	L'identificativo del volume su cui sono stati archiviati i dati dell'oggetto.
RSLT	Risultato	Lo stato di completamento del processo di rimozione dell'archivio: • SUC: Riuscito • ARUN: Errore (sistema storage di archiviazione esterno non disponibile) • GERR: Failed (errore generale)

ASCE: Fine archivio oggetti

Questo messaggio indica che la scrittura di un blocco di contenuto in un sistema di storage di archiviazione esterno è terminata.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore del blocco di contenuto memorizzato nel sistema di storage di archiviazione esterno.
VLID	Identificatore del volume	L'identificatore univoco del volume di archivio in cui vengono scritti i dati dell'oggetto.
VREN	Verifica abilitata	Indica se viene eseguita la verifica per i blocchi di contenuto. I valori attualmente definiti sono: • VENA: La verifica è attivata • VDSA: Verifica disattivata
MCLS	Classe di gestione	Stringa che identifica la classe di gestione TSM a cui viene assegnato il blocco di contenuto, se applicabile.
RSLT	Risultato	Indica il risultato del processo di archiviazione. I valori attualmente definiti sono: • SUC: Riuscito (processo di archiviazione riuscito) • OFFL: Non riuscito (archiviazione offline) • VRFL: Non riuscito (verifica oggetto non riuscita) • ARUN: Errore (sistema storage di archiviazione esterno non disponibile) • GERR: Failed (errore generale)

Questo messaggio di audit indica che il blocco di contenuto specificato è stato scritto nel sistema di storage di archiviazione esterno. Se la scrittura non riesce, il risultato fornisce informazioni di base sulla risoluzione dei problemi relativi alla posizione in cui si è verificato l'errore. Informazioni più dettagliate sugli errori di archiviazione sono disponibili esaminando gli attributi del nodo di archiviazione nel sistema StorageGRID.

ASCT: Archivio Store Cloud-Tier

Questo messaggio viene generato quando i dati degli oggetti archiviati vengono memorizzati in un sistema storage di archiviazione esterno, che si connette a StorageGRID attraverso l'API S3.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto recuperato.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto in byte.
RSLT	Codice risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.
SUID	Identificatore univoco dello storage	Identificatore univoco (UUID) del livello cloud in cui è stato memorizzato il contenuto.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.

ATCE: Inizio archivio oggetti

Questo messaggio indica che è stata avviata la scrittura di un blocco di contenuto in uno storage di archiviazione esterno.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto da archiviare.
VLID	Identificatore del volume	Identificatore univoco del volume in cui viene scritto il blocco di contenuto. Se l'operazione non riesce, viene restituito un ID volume pari a 0.

Codice	Campo	Descrizione
RSLT	Risultato	Indica il risultato del trasferimento del blocco di contenuto. I valori attualmente definiti sono: • SUC: Riuscito (blocco di contenuto memorizzato correttamente) • EXIS: Ignorato (blocco di contenuto già memorizzato) • ISFD: Errore (spazio su disco insufficiente) • STER: Failed (errore durante la memorizzazione del CBID) • OFFL: Non riuscito (archiviazione offline) • GERR: Failed (errore generale)

AVCC: Convalida archivio configurazione Cloud-Tier

Questo messaggio viene generato quando le impostazioni di configurazione vengono validate per un tipo di destinazione Cloud Tiering - Simple Storage Service (S3).

Codice	Campo	Descrizione
RSLT	Codice risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.
SUID	Identificatore univoco dello storage	UUID associato al sistema di storage di archiviazione esterno da validare.

BROR: Richiesta di sola lettura bucket

Il servizio LDR genera questo messaggio di audit quando un bucket entra o esce dalla modalità di sola lettura. Ad esempio, un bucket entra in modalità di sola lettura mentre tutti gli oggetti vengono cancellati.

Codice	Campo	Descrizione
BKHD	UUID bucket	L'ID bucket.
BROV	Valore della richiesta di sola lettura del bucket	Se il bucket viene reso di sola lettura o se esce dallo stato di sola lettura (1 = sola lettura, 0 = non di sola lettura).
BROS	Motivo di sola lettura del bucket	Il motivo per cui il bucket viene reso di sola lettura o viene lasciato lo stato di sola lettura. Ad esempio, emptyBucket.
S3AI	ID account tenant S3	L'ID dell'account tenant che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

CBRB: Inizio ricezione oggetto

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

CBRE: Fine ricezione oggetto

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo

messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati. CONL: Connessione persa durante il trasferimento CTMO: Timeout della connessione durante la creazione o il trasferimento UNRE: ID nodo di destinazione non raggiungibile CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono

essere utilizzate per tenere traccia del flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare i conteggi delle repliche.

CBSB: Inizio invio oggetto

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

CBSE: Fine invio oggetto

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati. CONL: Connessione persa durante il trasferimento CTMO: Timeout della connessione durante la creazione o il trasferimento UNRE: ID nodo di destinazione non raggiungibile CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a

nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare i conteggi delle repliche.

CGRR: Richiesta di replica cross-grid

Questo messaggio viene generato quando StorageGRID tenta di eseguire un'operazione di replica cross-grid per replicare gli oggetti tra bucket in una connessione a federazione di griglie.

Codice	Campo	Descrizione
CSIZ	Dimensione oggetto	La dimensione dell'oggetto in byte. L'attributo CSIZ è stato introdotto in StorageGRID 11,8. Di conseguenza, le richieste di replica cross-grid su un aggiornamento da StorageGRID 11,7 a 11,8 potrebbero presentare dimensioni totali degli oggetti imprecise.
S3AI	ID account tenant S3	L'ID dell'account tenant proprietario del bucket da cui l'oggetto viene replicato.
GFID	ID connessione federazione griglia	L'ID della connessione a federazione di griglie utilizzata per la replica cross-grid.
OPER	Funzionamento CGR	Il tipo di operazione di replica cross-grid che è stata tentata: • 0 = oggetto replicato • 1 = Replica oggetto multiparte • 2 = marcatore di eliminazione replicato
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket.
VSID	ID versione	L'ID versione della versione specifica di un oggetto replicato.
RSLT	Codice risultato	Restituisce Successful (SUCS) o General error (GERR).

EBDL: Eliminazione bucket vuoto

Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione bucket vuota).

Codice	Campo	Descrizione
CSIZ	Dimensione oggetto	La dimensione dell'oggetto in byte.
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
SGC	UUID container	UUID del container per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
RSLT	Risultato dell'operazione di eliminazione	Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

EBKR: Richiesta bucket vuoto

Questo messaggio indica che un utente ha inviato una richiesta per attivare o disattivare il bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di oggetti).

Codice	Campo	Descrizione
BUID (BUID)	UUID bucket	L'ID bucket.
EBJS	Configurazione JSON bucket vuoto	Contiene il JSON che rappresenta la configurazione vuota corrente del bucket.
S3AI	ID account tenant S3	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

ECMC: Frammento di dati con codice di cancellazione mancante

Questo messaggio di audit indica che il sistema ha rilevato un frammento di dati con codifica di cancellazione mancante.

Codice	Campo	Descrizione
VCMC	ID VCS	Il nome del VCS che contiene il blocco mancante.
MCID	ID chunk	L'identificatore del frammento con codifica di cancellazione mancante.

Codice	Campo	Descrizione
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non è pertinente per questo particolare messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

ECOC: Frammento di dati con codice di cancellazione corrotto

Questo messaggio di audit indica che il sistema ha rilevato un frammento di dati corrotto con codifica di cancellazione.

Codice	Campo	Descrizione
VCCO	ID VCS	Il nome del VCS che contiene il blocco corrotto.
VLID	ID volume	Volume RangeDB contenente il frammento corrotto con codifica di cancellazione.
CCID	ID chunk	L'identificatore del frammento corrotto con codifica in cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non è pertinente per questo particolare messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

ETAF: Autenticazione di sicurezza non riuscita

Questo messaggio viene generato quando un tentativo di connessione con Transport Layer Security (TLS) non riesce.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP su cui l'autenticazione non è riuscita.
MALEDUCATO	Identità dell'utente	Identificatore dipendente dal servizio che rappresenta l'identità dell'utente remoto.

Codice	Campo	Descrizione
RSLT	Codice di motivazione	Il motivo del guasto: SCNI: Connessione sicura non riuscita. CERM: Certificato mancante. CERT: Certificato non valido. CERE: Certificato scaduto. CER: Certificato revocato. CSGN: Firma del certificato non valida. CSGU: Il firmatario del certificato non era noto. UCRM: Credenziali utente mancanti. UCRI: Credenziali utente non valide. UCRU: Le credenziali dell'utente non sono consentite. TOUT: Timeout dell'autenticazione.

Quando viene stabilita una connessione a un servizio sicuro che utilizza TLS, le credenziali dell'entità remota vengono verificate utilizzando il profilo TLS e la logica aggiuntiva integrata nel servizio. Se l'autenticazione non riesce a causa di certificati o credenziali non validi, imprevisti o non consentiti, viene registrato un messaggio di audit. Ciò consente di eseguire query per tentativi di accesso non autorizzati e altri problemi di connessione correlati alla sicurezza.

Il messaggio potrebbe derivare da un'entità remota con una configurazione errata o da tentativi di presentare credenziali non valide o non consentite al sistema. Questo messaggio di audit deve essere monitorato per rilevare i tentativi di accesso non autorizzato al sistema.

GNRG: Registrazione GNDS

Il servizio CMN genera questo messaggio di audit quando un servizio ha aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUC: Riuscito • SUNV: Servizio non disponibile • GERR: Altro guasto
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.

Codice	Campo	Descrizione
GNTP	Tipo di dispositivo	Il tipo di dispositivo del nodo Grid (ad esempio, BLDR per un servizio LDR).
GNDV	Versione del modello del dispositivo	Stringa che identifica la versione del modello di dispositivo del nodo Grid nel bundle DMDL.
GNGP	Gruppo	Il gruppo a cui appartiene il nodo grid (nel contesto dei costi di collegamento e della classificazione delle query di servizio).
GNIA	Indirizzo IP	L'indirizzo IP del nodo della griglia.

Questo messaggio viene generato ogni volta che un nodo della griglia aggiorna la propria voce nel bundle dei nodi della griglia.

GNUR: Annullamento registrazione GNDS

Il servizio CMN genera questo messaggio di audit quando un servizio ha informazioni non registrate su se stesso dal sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUC: Riuscito • SUNV: Servizio non disponibile • GERR: Altro guasto
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.

GTED: Task Grid terminato

Questo messaggio di audit indica che il servizio CMN ha terminato l'elaborazione dell'attività di griglia specificata e che l'attività è stata spostata nella tabella Cronologia. Se il risultato è SUCS, ABRT o ROLF, verrà visualizzato un messaggio di audit Grid Task Started (attività griglia avviata) corrispondente. Gli altri risultati indicano che l'elaborazione di questa attività della griglia non è mai stata avviata.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in modo univoco un'attività Grid generata e consente di gestire l'attività Grid nel suo ciclo di vita. **Nota:** l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.
RSLT	Risultato	Risultato finale dello stato dell'attività Grid: • SUCS: L'attività Grid è stata completata correttamente. • ABRT: L'attività Grid è stata terminata senza un errore di rollback. • ROLF: L'attività Grid è stata terminata e non è stato possibile completare il processo di rollback. • CANC: L'attività della griglia è stata annullata dall'utente prima dell'avvio. • EXPR: L'attività Grid è scaduta prima dell'avvio. • IVLD: L'attività della griglia non era valida. • AUTH: L'attività della rete non è stata autorizzata. • DUPL: L'attività Grid è stata rifiutata come duplicata.

GTST: Task Grid avviato

Questo messaggio di audit indica che il servizio CMN ha avviato l'elaborazione dell'attività Grid specificata. Il messaggio di audit segue immediatamente il messaggio Grid Task Submitted per le attività Grid avviate dal servizio interno Grid Task Submission e selezionate per l'attivazione automatica. Per le attività della griglia inoltrate nella tabella Pending (in sospeso), questo messaggio viene generato quando l'utente avvia l'attività della griglia.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in maniera univoca un'attività grid generata e consente di gestirne l'intero ciclo di vita. **Nota:** l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.
RSLT	Risultato	Il risultato. Questo campo ha un solo valore: • SUCS: L'attività Grid è stata avviata correttamente.

GTSU: Task Grid inviato

Questo messaggio di audit indica che un'attività Grid è stata inviata al servizio CMN.

Codice	Campo	Descrizione
TSID	ID attività	Identifica in modo univoco un'attività grid generata e consente di gestarla per l'intero ciclo di vita. **Nota:** l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.
TTIP	Tipo di attività	Il tipo di attività della griglia.
VER	Versione attività	Un numero che indica la versione dell'attività Grid.
TDSC	Descrizione dell'attività	Una descrizione leggibile dell'attività Grid.
VAT	Valido dopo l'indicatore di data e ora	Il primo tempo (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui l'attività grid è valida.
VBTS	Valido prima dell'indicatore di data e ora	L'ultima ora (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui è valida l'attività grid.
TSRC	Origine	L'origine dell'attività: • TXTB: L'attività Grid è stata inviata tramite il sistema StorageGRID come blocco di testo firmato. • GRID: L'attività Grid è stata inviata tramite il Grid Task Submission Service interno.
ACTV	Tipo di attivazione	Il tipo di attivazione: • AUTO: L'attività della griglia è stata inviata per l'attivazione automatica. • PEND: L'attività Grid è stata inviata alla tabella in sospeso. Questa è l'unica possibilità per l'origine TXTB.
RSLT	Risultato	Risultato dell'invio: • SUCS: L'attività Grid è stata inviata correttamente. • ERRORE: L'attività è stata spostata direttamente nella tabella storica.

IDEL: Eliminazione avviata da ILM

Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto.

Il messaggio IDEL viene generato in una delle seguenti situazioni:

- **Per gli oggetti nei bucket S3 conformi**: Questo messaggio viene generato quando ILM avvia il processo di eliminazione automatica di un oggetto perché il relativo periodo di conservazione è scaduto (supponendo che l'impostazione di eliminazione automatica sia attivata e che la sospensione legale sia disattivata).
- **Per oggetti in bucket S3 o container Swift non conformi**. Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto poiché all'oggetto non sono attualmente applicate istruzioni di posizionamento nei criteri ILM attivi.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CMPA	Compliance: Eliminazione automatica	Solo per oggetti nei bucket S3 conformi. 0 (false) o 1 (true), che indica se un oggetto conforme deve essere cancellato automaticamente al termine del periodo di conservazione, a meno che il bucket non sia sottoposto a una conservazione legale.
CMPL	Compliance: Conservazione a fini legali	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), che indica se il bucket è attualmente in stato di conservazione legale.
CMPR	Conformità: Periodo di conservazione	Solo per oggetti nei bucket S3 conformi. La durata del periodo di conservazione dell'oggetto in minuti.
CTME	Compliance: Tempo di acquisizione	Solo per oggetti nei bucket S3 conformi. Il tempo di acquisizione dell'oggetto. È possibile aggiungere il periodo di conservazione in minuti a questo valore per determinare quando l'oggetto può essere cancellato dal bucket.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.

Codice	Campo	Descrizione
LOCS	Posizioni	La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato). CLEC: Per gli oggetti sottoposti a erasure coding, l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding applicati ai dati dell'oggetto. CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.
PERCORSO	ID bucket/chiave S3 o container/oggetto Swift	Il nome del bucket S3 e il nome della chiave S3 oppure il nome del container Swift e l'identificatore dell'oggetto Swift.
RSLT	Risultato	Risultato dell'operazione ILM. SUCS: Operazione ILM riuscita.
REGOLA	Etichetta regole	• Se un oggetto in un bucket S3 conforme viene cancellato automaticamente perché il suo periodo di conservazione è scaduto, questo campo è vuoto. • Se l'oggetto viene eliminato perché non sono presenti ulteriori istruzioni di posizionamento attualmente applicabili all'oggetto, questo campo mostra l'etichetta leggibile dell'ultima regola ILM applicata all'oggetto.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

LKCU: Pulitura oggetto sovrascritta

Questo messaggio viene generato quando StorageGRID rimuove un oggetto sovrascritto che in precedenza richiedeva la pulizia per liberare spazio di storage. Un oggetto viene sovrascritto quando un client S3 o Swift scrive un oggetto in un percorso che già contiene un oggetto. Il processo di rimozione avviene automaticamente e in background.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LTYP	Tipo di pulizia	*Solo per uso interno.*
LUID	UUID oggetto rimosso	L'identificativo dell'oggetto rimosso.
PERCORSO	ID bucket/chiave S3 o container/oggetto Swift	Il nome del bucket S3 e il nome della chiave S3 oppure il nome del container Swift e l'identificatore dell'oggetto Swift.
SGC	UUID container	UUID del container per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Universally Unique Identifier	L'identificativo dell'oggetto ancora esistente. Questo valore è disponibile solo se l'oggetto non è stato eliminato.

LLST: Località persa

Questo messaggio viene generato ogni volta che non è possibile trovare una posizione per una copia dell'oggetto (replicata o con erasure coding).

Codice	Campo	Descrizione
CBIL	CBID	Il CBID interessato.
ECPR	Profilo di erasure coding	Per i dati degli oggetti con codifica erasure. L'ID del profilo di erasure coding utilizzato.
LTYP	Tipo di ubicazione	CLDI (online): Per i dati degli oggetti replicati CLEC (Online): Per i dati degli oggetti con codifica erasure CLNL (Nearline): Per i dati degli oggetti replicati archiviati
NOID. (NOIDE	ID nodo di origine	L'ID del nodo in cui sono state perse le posizioni.
PCLD	Percorso dell'oggetto replicato	Il percorso completo alla posizione del disco dei dati dell'oggetto perso. Viene restituito solo quando LTYP ha un valore di CLDI (vale a dire, per gli oggetti replicati). Prende la forma `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`

Codice	Campo	Descrizione
RSLT	Risultato	SEMPRE NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
TSRC	Fonte di attivazione	UTENTE: Attivato dall'utente SYST: Attivato dal sistema
UUID	ID universalamente univoco	L'identificativo dell'oggetto interessato nel sistema StorageGRID.

MGAU: Messaggio di audit della gestione

La categoria Gestione registra le richieste degli utenti all'API di gestione. Ogni richiesta che non è UNA richiesta GET o HEAD all'API registra una risposta con il nome utente, l'IP e il tipo di richiesta all'API.

Codice	Campo	Descrizione
MDIP	Indirizzo IP di destinazione	L'indirizzo IP del server (destinazione).
MDNA	Nome di dominio	Il nome del dominio host.
MPAT	PERCORSO di richiesta	Il percorso della richiesta.
MPQP	Parametri di query della richiesta	I parametri di query per la richiesta.

Codice	Campo	Descrizione
MRBD	Corpo della richiesta	Il contenuto dell'organismo di richiesta. Mentre il corpo della risposta viene registrato per impostazione predefinita, il corpo della richiesta viene registrato in alcuni casi quando il corpo della risposta è vuoto. Poiché le seguenti informazioni non sono disponibili nel corpo della risposta, vengono prese dal corpo della richiesta per i seguenti metodi POST: • Nome utente e ID account in **POST authorize** • Nuova configurazione delle subnet in **POST /grid/grid-networks/update** • Nuovi server NTP in **POST /grid/ntp-servers/update** • ID server decommissionati in **POST /grid/servers/decommissionation** **Nota:** le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).
MRMD	Metodo di richiesta	Il metodo di richiesta HTTP: • POST • IN PRIMO PIANO • ELIMINARE • PATCH
MRSC	Codice di risposta	Il codice di risposta.
MRSP	Corpo di risposta	Il contenuto della risposta (il corpo della risposta) viene registrato per impostazione predefinita. **Nota:** le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).
MSIP	Indirizzo IP di origine	L'indirizzo IP (di origine) del client.
MUN	URN utente	L'URN (Uniform resource name) dell'utente che ha inviato la richiesta.
RSLT	Risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.

OLST: Il sistema ha rilevato un oggetto perso

Questo messaggio viene generato quando il servizio DDS non riesce a individuare alcuna copia di un oggetto all'interno del sistema StorageGRID.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto perso.
NOID. (NOIDE	ID nodo	Se disponibile, l'ultima posizione nota diretta o near-line dell'oggetto perso. Se le informazioni sul volume non sono disponibili, è possibile avere solo l'ID nodo senza un ID volume.
PERCORSO	ID bucket/chiave S3 o container/oggetto Swift	Se disponibili, il nome del bucket S3 e il nome della chiave S3 oppure il nome del container Swift e l'identificatore dell'oggetto Swift.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
UUID	ID universalamente univoco	L'identificativo dell'oggetto perso nel sistema StorageGRID.
VOLO	ID volume	Se disponibile, l'ID del volume del nodo di storage o del nodo di archiviazione per l'ultima posizione nota dell'oggetto perso.

ORLM: Regole oggetto soddisfatte

Questo messaggio viene generato quando l'oggetto viene memorizzato e copiato correttamente come specificato dalle regole ILM.

> Il messaggio ORLM non viene generato quando un oggetto viene memorizzato correttamente dalla regola predefinita Make 2 Copies se un'altra regola del criterio utilizza il filtro avanzato dimensione oggetto.

Codice	Campo	Descrizione
BUID (BUID)	Testata benna	Campo ID bucket. Utilizzato per operazioni interne. Viene visualizzato solo se STAT è PRGD.
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.

Codice	Campo	Descrizione
LOCS	Posizioni	La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato). CLEC: Per gli oggetti sottoposti a erasure coding, l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding applicati ai dati dell'oggetto. CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.
PERCORSO	ID bucket/chiave S3 o container/oggetto Swift	Il nome del bucket S3 e il nome della chiave S3 oppure il nome del container Swift e l'identificatore dell'oggetto Swift.
RSLT	Risultato	Risultato dell'operazione ILM. SUCS: Operazione ILM riuscita.
REGOLA	Etichetta regole	Etichetta leggibile assegnata alla regola ILM applicata a questo oggetto.
SGC	UUID container	UUID del container per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
SGCB	CBID contenitore	CBID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo per gli oggetti segmentati e multiparte.
URGENZA	Stato	Lo stato del funzionamento di ILM. FATTO: Operazioni ILM rispetto all'oggetto completate. DFER: L'oggetto è stato contrassegnato per la futura rivalutazione ILM. PRGD: L'oggetto è stato cancellato dal sistema StorageGRID. NLOC: I dati dell'oggetto non possono più essere trovati nel sistema StorageGRID. Questo stato potrebbe indicare che tutte le copie dei dati dell'oggetto sono mancanti o danneggiate.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Il messaggio di audit ORLM può essere emesso più di una volta per un singolo oggetto. Ad esempio, viene emesso ogni volta che si verifica uno dei seguenti eventi:

- Le regole ILM per l'oggetto sono soddisfatte per sempre.
- Le regole ILM per l'oggetto sono soddisfatte per questa epoca.
- Le regole ILM hanno eliminato l'oggetto.
- Il processo di verifica in background rileva che una copia dei dati degli oggetti replicati è danneggiata. Il sistema StorageGRID esegue una valutazione ILM per sostituire l'oggetto corrotto.

Informazioni correlate

- "Transazioni di acquisizione degli oggetti"
- "Transazioni di eliminazione degli oggetti"

OVWR: Sovrascrittura degli oggetti

Questo messaggio viene generato quando un'operazione esterna (richiesta dal client) causa la sovrascrittura di un oggetto da parte di un altro oggetto.

Codice	Campo	Descrizione
CBID	Content Block Identifier (nuovo)	Il CBID per il nuovo oggetto.
CSIZ	Dimensione oggetto precedente	La dimensione, in byte, dell'oggetto da sovrascrivere.
OCBD	Content Block Identifier (precedente)	Il CBID dell'oggetto precedente.
UUID	ID universally Unique (nuovo)	L'identificativo del nuovo oggetto all'interno del sistema StorageGRID.
ID OUID	ID universally Unique (precedente)	L'identificativo dell'oggetto precedente all'interno del sistema StorageGRID.
PERCORSO	S3 o Swift Object Path	Il percorso di oggetti S3 o Swift utilizzato sia per l'oggetto precedente che per quello nuovo
RSLT	Codice risultato	Risultato della transazione Object Overwrite. Il risultato è sempre: SUC: Riuscito
SGRP	Sito (gruppo)	Se presente, l'oggetto sovrascritto è stato cancellato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto sovrascritto.

S3SL: Richiesta S3 Select

Questo messaggio registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere messaggi di errore e dettagli del codice di errore. La richiesta potrebbe non essere riuscita.

Codice	Campo	Descrizione
BYSC	Byte sottoposti a scansione	Numero di byte sottoposti a scansione (ricevuti) dai nodi di storage. BYSC e BYPR potrebbero essere diversi se l'oggetto viene compresso. Se l'oggetto è compresso, BYSC avrebbe il conteggio dei byte compressi e BYPR i byte dopo la decompressione.
BYPR	Byte elaborati	Numero di byte elaborati. Indica quanti byte di "byte sottoposti a scansione" sono stati effettivamente elaborati o utilizzati da un lavoro S3 Select.
BYRT	Byte restituiti	Numero di byte restituiti al client da un lavoro S3 Select.
RPR	Record elaborati	Numero di record o righe ricevuti da un processo S3 Select dai nodi di storage.
RERT	Record restituiti	Numero di record o righe di un lavoro S3 Select restituito al client.
JOFI	Lavoro terminato	Indica se il lavoro S3 Select ha terminato o meno l'elaborazione. Se questo è falso, il lavoro non è stato completato e i campi di errore probabilmente contengono dei dati. Il client potrebbe aver ricevuto risultati parziali o non avere alcun risultato.
RID	ID richiesta	Identificatore della richiesta S3 Select.
ETM	Tempo di esecuzione	Il tempo, in secondi, impiegato per il completamento del processo S3 Select.
ERMG	Messaggio di errore	Messaggio di errore generato dal lavoro S3 Select.
EROSO	Tipo di errore	Tipo di errore generato dal lavoro S3 Select.
ERST	Errore StackTrace	Errore StackTrace generato dal lavoro S3 Select.
S3BK	Bucket S3	Il nome del bucket S3.

Codice	Campo	Descrizione
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 per l'utente che ha inviato la richiesta.
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket.

SADD: Disattivazione dell'audit di sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha disattivato la registrazione dei messaggi di audit; i messaggi di audit non vengono più raccolti o consegnati.

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Metodo utilizzato per disattivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per disattivare la registrazione dell'audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione era stata precedentemente attivata, ma ora è stata disattivata. Questo viene generalmente utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato (SADE) e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

SADE: Abilitazione controllo di sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha ripristinato la registrazione del messaggio di audit; i messaggi di audit vengono nuovamente raccolti e consegnati.

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Il metodo utilizzato per attivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per attivare la registrazione dell'audit.

Codice	Campo	Descrizione
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione è stata precedentemente disattivata (SADD), ma ora è stata ripristinata. In genere viene utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

SCMT: Commit dell'archivio di oggetti

Il contenuto della griglia non viene reso disponibile o riconosciuto come memorizzato fino a quando non viene assegnato (ovvero viene memorizzato in modo persistente). Il contenuto memorizzato in maniera persistente è stato completamente scritto su disco e ha superato i relativi controlli di integrità. Questo messaggio viene emesso quando un blocco di contenuto viene assegnato allo storage.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto impegnato nello storage permanente.
RSLT	Codice risultato	Stato al momento in cui l'oggetto è stato memorizzato sul disco: SUCS: Oggetto memorizzato correttamente.

Questo messaggio indica che un dato blocco di contenuto è stato completamente memorizzato e verificato e può essere richiesto. Può essere utilizzato per tenere traccia del flusso di dati all'interno del sistema.

SDEL: ELIMINAZIONE S3

Quando un client S3 esegue una transazione DI ELIMINAZIONE, viene effettuata una richiesta per rimuovere l'oggetto o il bucket specificato o per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto cancellato in byte. Le operazioni sui bucket non includono questo campo.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
GFID	ID connessione Grid Federation	L'ID di connessione della connessione a federazione di griglie associato a una richiesta di eliminazione della replica a griglia incrociata. Incluso solo nei registri di controllo nella griglia di destinazione.
GFSA	ID account di origine Grid Federation	L'ID account del tenant sulla griglia di origine per una richiesta di eliminazione della replica cross-grid. Incluso solo nei registri di controllo nella griglia di destinazione.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `` `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP). `` `x-amz-bypass-governance-retention` viene automaticamente incluso se è presente nella richiesta.
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione DI ELIMINAZIONE. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.

Codice	Campo	Descrizione
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.

Codice	Campo	Descrizione
UDM	Identificatore univoco universale per un marcatore di cancellazione	L'identificatore di un marcatore di eliminazione. I messaggi del registro di controllo specificano UUDM o UUID, dove UUDM indica un marcatore di eliminazione creato come risultato di una richiesta di eliminazione dell'oggetto e UUID indica un oggetto.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SGET: S3 GET

Quando un client S3 esegue una transazione GET, viene effettuata una richiesta per recuperare un oggetto o elencare gli oggetti in un bucket o per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).

Codice	Campo	Descrizione
LITY	ListObjectsV2	È stata richiesta una risposta *formato v2*. Per ulteriori informazioni, vedere "AWS ListObjectsV2". Solo per operazioni CON benna GET.
NCHD	Numero di bambini	Include tasti e prefissi comuni. Solo per operazioni CON benna GET.
RANG	Range Read (lettura intervallo)	Solo per operazioni di lettura dell'intervallo. Indica l'intervallo di byte letti da questa richiesta. Il valore dopo la barra (/) mostra la dimensione dell'intero oggetto.
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
TRNC	Troncato o non troncato	Impostare su false se sono stati restituiti tutti i risultati. Impostare su true se sono disponibili ulteriori risultati da restituire. Solo per operazioni CON benna GET.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SHEA: TESTA S3

Quando un client S3 esegue una transazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un oggetto o bucket e recuperare i metadati relativi a un oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto controllato in byte. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SPOS: POST S3

Quando un client S3 invia una richiesta di oggetto POST, questo messaggio viene inviato dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP). (Non previsto per SPOS).
RSLT	Codice risultato	Risultato della richiesta RestoreObject. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile. Impostare su "SELECT" per un'operazione di selezione S3.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.

Codice	Campo	Descrizione
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	Ripristinare le informazioni.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SPUT: S3 PUT

Quando un client S3 esegue una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o bucket o per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CMPS	Impostazioni di compliance	Le impostazioni di conformità utilizzate durante la creazione del bucket, se presenti nella richiesta (troncate ai primi 1024 caratteri).

Codice	Campo	Descrizione
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
GFID	ID connessione Grid Federation	L'ID di connessione della connessione a federazione di griglie associato a una richiesta DI PUT di replica a griglia incrociata. Incluso solo nei registri di controllo nella griglia di destinazione.
GFSA	ID account di origine Grid Federation	L'ID account del tenant sulla griglia di origine per una richiesta DI PUT di replica cross-grid. Incluso solo nei registri di controllo nella griglia di destinazione.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `` `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP). `` `x-amz-bypass-governance-retention` viene automaticamente incluso se è presente nella richiesta.
LKEN	Blocco oggetto attivato	Valore dell'intestazione della richiesta `x-amz-bucket-object-lock-enabled`, se presente nella richiesta.
LKSX	Blocco oggetto Legal Hold	Valore dell'intestazione della richiesta `x-amz-object-lock-legal-hold`, Se presente nella richiesta PutObject.
LKMD	Modalità di conservazione del blocco degli oggetti	Valore dell'intestazione della richiesta `x-amz-object-lock-mode`, Se presente nella richiesta PutObject.
LKRU	Blocco oggetto conserva fino alla data	Valore dell'intestazione della richiesta `x-amz-object-lock-retain-until-date`, Se presente nella richiesta PutObject.

Codice	Campo	Descrizione
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	La nuova configurazione delle sottorisorse (troncata ai primi 1024 caratteri).

Codice	Campo	Descrizione
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
ULID	ID upload	Incluso solo nei messaggi SPUT per le operazioni CompleteMultipartUpload. Indica che tutte le parti sono state caricate e assemblate.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.
VSST	Stato di versione	Il nuovo stato di versione di un bucket. Vengono utilizzati due stati: "Enabled" (attivato) o "Suspended" (sospeso). Le operazioni sugli oggetti non includono questo campo.

SREM: Rimozione dell'archivio di oggetti

Questo messaggio viene inviato quando il contenuto viene rimosso dallo storage persistente e non è più accessibile tramite API regolari.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto cancellato dallo storage permanente.
RSLT	Codice risultato	Indica il risultato delle operazioni di rimozione del contenuto. L'unico valore definito è: SUC: Contenuto rimosso dallo storage persistente

Questo messaggio di audit indica che un dato blocco di contenuto è stato cancellato da un nodo e non può più essere richiesto direttamente. Il messaggio può essere utilizzato per tenere traccia del flusso di contenuti cancellati all'interno del sistema.

SUPD: Metadati S3 aggiornati

Questo messaggio viene generato dall'API S3 quando un client S3 aggiorna i metadati per un oggetto acquisito. Il messaggio viene emesso dal server se l'aggiornamento dei metadati ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta, quando si aggiornano le impostazioni di conformità di un bucket.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

Codice	Campo	Descrizione
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto i cui metadati sono stati aggiornati. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SVRF: Verifica archivio oggetti non riuscita

Questo messaggio viene emesso ogni volta che un blocco di contenuto non supera il processo di verifica. Ogni volta che i dati degli oggetti replicati vengono letti o scritti su disco, vengono eseguiti diversi controlli di verifica e integrità per garantire che i dati inviati

all’utente richiedente siano identici ai dati originariamente acquisiti nel sistema. Se uno di questi controlli non riesce, il sistema mette automaticamente in quarantena i dati dell’oggetto replicato corrotto per impedirne il recupero.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto che non ha superato la verifica.
RSLT	Codice risultato	Tipo di errore di verifica: CRCF: Controllo di ridondanza ciclico (CRC) non riuscito. HMAC: Controllo HMAC (hash-based message Authentication code) non riuscito. EHSH: Hash di contenuto crittografato inatteso. PHSH: Hash di contenuto originale inaspettato. SEQC: Sequenza di dati errata sul disco. PERR: Struttura del file di disco non valida. DERR: Errore del disco. FNAM: Nome file non valido.

Questo messaggio deve essere monitorato attentamente. Gli errori di verifica del contenuto possono indicare guasti hardware imminenti.

Per determinare quale operazione ha attivato il messaggio, vedere il valore del campo AMID (Module ID) (ID modulo). Ad esempio, un valore SVFY indica che il messaggio è stato generato dal modulo Storage Verifier, ovvero la verifica in background e STOR indica che il messaggio è stato attivato dal recupero del contenuto.

SVRU: Verifica archivio oggetti sconosciuta

Il componente Storage del servizio LDR esegue una scansione continua di tutte le copie dei dati degli oggetti replicati nell’archivio di oggetti. Questo messaggio viene visualizzato quando viene rilevata una copia sconosciuta o imprevista dei dati degli oggetti replicati nell’archivio di oggetti e spostata nella directory di quarantena.

Codice	Campo	Descrizione
FPTH	Percorso del file	Il percorso del file della copia imprevista dell’oggetto.

Codice	Campo	Descrizione
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

Il messaggio di audit SVRU: Object Store Verify Unknown deve essere monitorato attentamente. Significa che sono state rilevate copie impreviste dei dati dell'oggetto nell'archivio di oggetti. Questa situazione deve essere esaminata immediatamente per determinare come sono state create queste copie, perché può indicare guasti hardware imminenti.

SYSD: Interruzione nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto lo shutdown. In genere, questo messaggio viene inviato solo dopo un riavvio successivo, in quanto la coda dei messaggi di controllo non viene cancellata prima dell'arresto. Se il servizio non è stato riavviato, cercare il messaggio SYST inviato all'inizio della sequenza di arresto.

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. L'RSLT di un SYSD non può indicare uno shutdown "anomalo", perché il messaggio viene generato solo dagli shutdown "puliti".

SYST: Interruzione del nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto lo shutdown e che il servizio ha avviato la sequenza di shutdown. SYST può essere utilizzato per determinare se è stato richiesto lo shutdown, prima che il servizio venga riavviato (a differenza di SYSD, che in genere viene inviato dopo il riavvio del servizio).

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. Il codice RSLT di un messaggio SYST non può indicare uno shutdown "dirty", perché il messaggio viene generato solo dagli shutdown "clean".

SYSU: Avvio nodo

Quando un servizio viene riavviato, questo messaggio viene generato per indicare se l'arresto precedente era pulito (comandato) o disordinato (imprevisto).

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito. DSDN: Il sistema non è stato spento correttamente. VRGN: Il sistema è stato avviato per la prima volta dopo l'installazione (o la reinstallazione) del server.

Il messaggio non indica se il server host è stato avviato, ma solo il servizio di reporting. Questo messaggio può essere utilizzato per:

- Rilevare la discontinuità nel registro di controllo.
- Determinare se un servizio si guasta durante il funzionamento (poiché la natura distribuita del sistema StorageGRID può mascherare questi guasti). Server Manager riavvia automaticamente un servizio guasto.

WDEL: ELIMINAZIONE rapida

Quando un client Swift esegue una transazione DI ELIMINAZIONE, viene inviata una richiesta per rimuovere l'oggetto o il container specificato. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto cancellato in byte. Le operazioni sui container non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).

Codice	Campo	Descrizione
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione DI ELIMINAZIONE. Il risultato è sempre: SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni sui container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

WGET: Swift GET

Quando un client Swift esegue una transazione GET, viene effettuata una richiesta per recuperare un oggetto, elencare gli oggetti in un container o elencare i container in un account. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni su account e container non includono questo campo.

Codice	Campo	Descrizione
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e container non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni su account e container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

WHEA: TESTA veloce

Quando un client Swift esegue una transazione HEAD, viene inviata una richiesta per verificare l'esistenza di un account, un container o un oggetto e recuperare eventuali

metadati pertinenti. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni su account e container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e container non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	Codice risultato	Risultato dell'operazione PRINCIPALE. Il risultato è sempre: SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni su account e container non includono questo campo.

Codice	Campo	Descrizione
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

WPUT: MESSA rapida

Quando un client Swift esegue una transazione PUT, viene inviata una richiesta per creare un nuovo oggetto o container. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui container non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.

Codice	Campo	Descrizione
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni sui container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

Espandere una griglia

Espandere una griglia: Panoramica

Puoi espandere la capacità o le funzionalità del tuo sistema StorageGRID senza interrompere le operazioni di sistema.

Un'espansione StorageGRID consente di aggiungere:

- Volumi storage sui nodi storage
- Nuovi nodi di griglia in un sito esistente
- Un intero nuovo sito

Il motivo dell'espansione determina il numero di nuovi nodi di ciascun tipo da aggiungere e la posizione dei nuovi nodi. Ad esempio, se si esegue un'espansione per aumentare la capacità dello storage, aggiungere la capacità dei metadati o aggiungere ridondanza o nuove funzionalità, esistono diversi requisiti dei nodi.

Seguire la procedura per il tipo di espansione che si sta eseguendo:

Aggiungere volumi di storage

Seguire la procedura per "Aggiunta di volumi di storage ai nodi di storage".

Aggiungere nodi griglia

1. Seguire la procedura per "aggiunta di nodi griglia a un sito esistente".
2. "Aggiornare le subnet".
3. Implementare nodi griglia:
   - "Appliance"
   - "VMware"
   - "Linux"

   > "Linux" si riferisce a una distribuzione Red Hat Enterprise Linux, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp (IMT)".

4. "Eseguire l'espansione".
5. "Configurare il sistema espanso".

Aggiungi nuovo sito

1. Seguire la procedura per "Aggiunta di un nuovo sito".
2. "Aggiornare le subnet".
3. Implementare nodi griglia:
   - "Appliance"
   - "VMware"
   - "Linux"

   > "Linux" si riferisce a una distribuzione Red Hat Enterprise Linux, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp (IMT)".

4. "Eseguire l'espansione".
5. "Configurare il sistema espanso".

Pianificare l'espansione di StorageGRID

Aggiungere capacità di storage

Linee guida per l'aggiunta della capacità degli oggetti

È possibile espandere la capacità dello storage a oggetti del sistema StorageGRID aggiungendo volumi di storage ai nodi di storage esistenti o aggiungendo nuovi nodi di storage ai siti esistenti. È necessario aggiungere capacità di storage in modo che soddisfi i requisiti della policy ILM (Information Lifecycle Management).

Linee guida per l'aggiunta di volumi di storage

Prima di aggiungere volumi di storage ai nodi di storage esistenti, consultare le seguenti linee guida e limitazioni:

- È necessario esaminare le regole ILM correnti per determinare dove e quando "aggiungere volumi di storage" per aumentare lo storage disponibile per "oggetti replicati" oppure "oggetti con codifica erasure".
- Non è possibile aumentare la capacità dei metadati del sistema aggiungendo volumi di storage perché i metadati degli oggetti vengono memorizzati solo sul volume 0.
- Ogni nodo di storage basato su software può supportare un massimo di 16 volumi di storage. Se è necessario aggiungere capacità oltre tale limite, è necessario aggiungere nuovi nodi di storage.
- È possibile aggiungere uno o due shelf di espansione a ciascuna appliance SG6060. Ogni shelf di espansione aggiunge 16 volumi di storage. Con entrambi gli shelf di espansione installati, SG6060 può supportare un totale di 48 volumi di storage.
- Puoi aggiungere uno o due shelf di espansione a ogni appliance SG6160. Ogni shelf di espansione aggiunge 60 volumi di storage. Con i due shelf di espansione installati, SG6160 supporta un totale di 180 volumi di storage.
- Non è possibile aggiungere volumi di storage ad altre appliance di storage.
- Non è possibile aumentare le dimensioni di un volume di storage esistente.
- Non è possibile aggiungere volumi di storage a un nodo di storage contemporaneamente all'aggiornamento del sistema, all'operazione di recovery o a un'altra espansione.

Dopo aver deciso di aggiungere volumi di storage e aver determinato i nodi di storage da espandere per soddisfare la policy ILM, seguire le istruzioni relative al tipo di nodo di storage:

- Per aggiungere uno o due shelf di espansione a un'appliance di storage SG6060, visitare il sito Web all'indirizzo "Aggiunta di shelf di espansione a SG6060 implementato".
- Per aggiungere uno o due shelf di espansione a un'appliance di storage SG6160, passare al "Aggiungi shelf di espansione alla piattaforma SG6160 implementata"
- Per un nodo basato su software, seguire le istruzioni per "Aggiunta di volumi di storage ai nodi di storage".

Linee guida per l'aggiunta di nodi di storage

Prima di aggiungere nodi di storage ai siti esistenti, consultare le seguenti linee guida e limitazioni:

- È necessario esaminare le regole ILM correnti per determinare dove e quando aggiungere nodi di storage per aumentare lo storage disponibile "oggetti replicati" oppure "oggetti con codifica erasure".
- Non aggiungere più di 10 nodi di storage in una singola procedura di espansione.
- È possibile aggiungere nodi di storage a più siti in una singola procedura di espansione.
- È possibile aggiungere nodi di storage e altri tipi di nodi in una singola procedura di espansione.
- Prima di avviare la procedura di espansione, è necessario confermare che tutte le operazioni di riparazione dei dati eseguite nell'ambito di un ripristino sono state completate. Vedere "Controllare i lavori di riparazione dei dati".
- Se è necessario rimuovere i nodi di storage prima o dopo l'esecuzione di un'espansione, non è necessario decommissionare più di 10 nodi di storage in una singola procedura Decommission Node.

Linee guida per il servizio ADC sui nodi di storage

Quando si configura l'espansione, è necessario scegliere se includere il servizio ADC (Administrative Domain Controller) in ogni nuovo nodo di storage. Il servizio ADC tiene traccia della posizione e della disponibilità dei servizi grid.

- Il sistema StorageGRID richiede un "Quorum dei servizi ADC" essere disponibile in ogni sito e in qualsiasi momento.
- Almeno tre nodi di storage in ogni sito devono includere il servizio ADC.
- Si sconsiglia di aggiungere il servizio ADC a ogni nodo di storage. L'inclusione di un numero eccessivo di servizi ADC può causare rallentamenti dovuti all'aumento della comunicazione tra i nodi.
- Un singolo grid non deve avere più di 48 nodi di storage con il servizio ADC. Ciò equivale a 16 siti con tre servizi ADC in ogni sito.
- In generale, quando si seleziona l'impostazione **Servizio ADC** per un nuovo nodo, selezionare **automatico**. Selezionare **Sì** solo se il nuovo nodo sostituirà un altro nodo di storage che include il servizio ADC. Poiché non è possibile decommissionare un nodo di storage se rimangono pochi servizi ADC, questo garantisce che sia disponibile un nuovo servizio ADC prima che il vecchio servizio venga rimosso.
- Non è possibile aggiungere il servizio ADC a un nodo dopo averlo implementato.

Aggiungere capacità di storage per gli oggetti replicati

Se il criterio ILM (Information Lifecycle Management) per l'implementazione include una regola che crea copie replicate di oggetti, è necessario considerare la quantità di storage da aggiungere e la posizione in cui aggiungere i nuovi volumi di storage o i nuovi nodi di storage.

Per informazioni su dove aggiungere storage aggiuntivo, esaminare le regole ILM che creano copie replicate. Se le regole ILM creano due o più copie di oggetti, pianificare di aggiungere storage in ogni posizione in cui vengono eseguite le copie di oggetti. Ad esempio, se si dispone di una griglia a due siti e di una regola ILM che crea una copia dell'oggetto in ogni sito, è necessario "aggiungere storage" per ogni sito per aumentare la capacità complessiva degli oggetti della griglia. Per informazioni sulla replica degli oggetti, vedere "Cos'è la replica".

Per motivi di performance, dovresti cercare di mantenere la capacità dello storage e la potenza di calcolo bilanciati tra i siti. Pertanto, per questo esempio, è necessario aggiungere lo stesso numero di nodi di storage a ciascun sito o volumi di storage aggiuntivi in ciascun sito.

Se si dispone di una policy ILM più complessa che include regole che posizionano oggetti in posizioni diverse in base a criteri come il nome del bucket o regole che cambiano le posizioni degli oggetti nel tempo, l'analisi dei punti in cui è richiesto lo storage per l'espansione sarà simile, ma più complessa.

La creazione di grafici sulla velocità di consumo della capacità di storage complessiva può aiutare a comprendere la quantità di storage da aggiungere all'espansione e quando sarà necessario lo spazio di storage aggiuntivo. È possibile utilizzare Grid Manager per "monitorare e tracciare la capacità di storage".

Quando si pianifica la tempistica di un'espansione, ricordarsi di considerare quanto tempo potrebbe essere necessario per procurarsi e installare storage aggiuntivo.

Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione

Se il criterio ILM include una regola che crea copie con codifica di cancellazione, è

necessario pianificare dove aggiungere nuovo storage e quando aggiungere nuovo storage. La quantità di storage aggiunta e la tempistica dell'aggiunta possono influire sulla capacità di storage utilizzabile del grid.

Il primo passo nella pianificazione di un'espansione dello storage consiste nell'esaminare le regole dei criteri ILM che creano oggetti con codifica in cancellazione. Poiché StorageGRID crea *k+m* frammenti per ogni oggetto con codifica di cancellazione e memorizza ciascun frammento su un nodo di storage diverso, è necessario assicurarsi che almeno *k+m* nodi di storage abbiano spazio per i nuovi dati con codifica di cancellazione dopo l'espansione. Se il profilo di erasure coding fornisce la protezione dalla perdita di sito, è necessario aggiungere storage a ciascun sito. Vedere "Cosa sono gli schemi di erasure coding" per informazioni sui profili di erasure coding.

Il numero di nodi da aggiungere dipende anche dal livello di riempimento dei nodi esistenti quando si esegue l'espansione.

Raccomandazioni generali per l'aggiunta di capacità di storage per gli oggetti con codifica di cancellazione

Se si desidera evitare calcoli dettagliati, è possibile aggiungere due nodi di storage per sito quando i nodi di storage esistenti raggiungono il 70% della capacità.

Questa raccomandazione generale fornisce risultati ragionevoli in un'ampia gamma di schemi di erasure coding sia per le griglie a sito singolo che per le griglie in cui la codifica erasure fornisce protezione dalle perdite di sito.

Per comprendere meglio i fattori che hanno portato a questo suggerimento o per sviluppare un piano più preciso per il tuo sito, consulta "Considerazioni per il ribilanciamento dei dati con codifica erasure". Per un consiglio personalizzato ottimizzato per la tua situazione, contatta il tuo consulente NetApp Professional Services.

Considerazioni per il ribilanciamento dei dati con codifica erasure

Se si esegue un'espansione per aggiungere nodi di storage e si utilizzano le regole ILM per erasure dei dati del codice, potrebbe essere necessario eseguire la procedura di ribilanciamento EC se non è possibile aggiungere un numero sufficiente di nodi di storage per lo schema di erasure coding in uso.

Dopo aver esaminato queste considerazioni, eseguire l'espansione, quindi passare a. "Ribilanciare i dati con codifica di cancellazione dopo l'aggiunta di nodi di storage" per eseguire la procedura.

Cos'è il ribilanciamento EC?

Il ribilanciamento EC è una procedura StorageGRID che potrebbe essere necessaria dopo l'espansione di un nodo di storage. La procedura viene eseguita come script della riga di comando dal nodo di amministrazione primario. Quando si esegue la procedura di ribilanciamento EC, StorageGRID ridistribuisce i frammenti con codifica erasure tra i nodi di storage esistenti e quelli appena aggiunti in un sito.

Procedura di ribilanciamento CE:

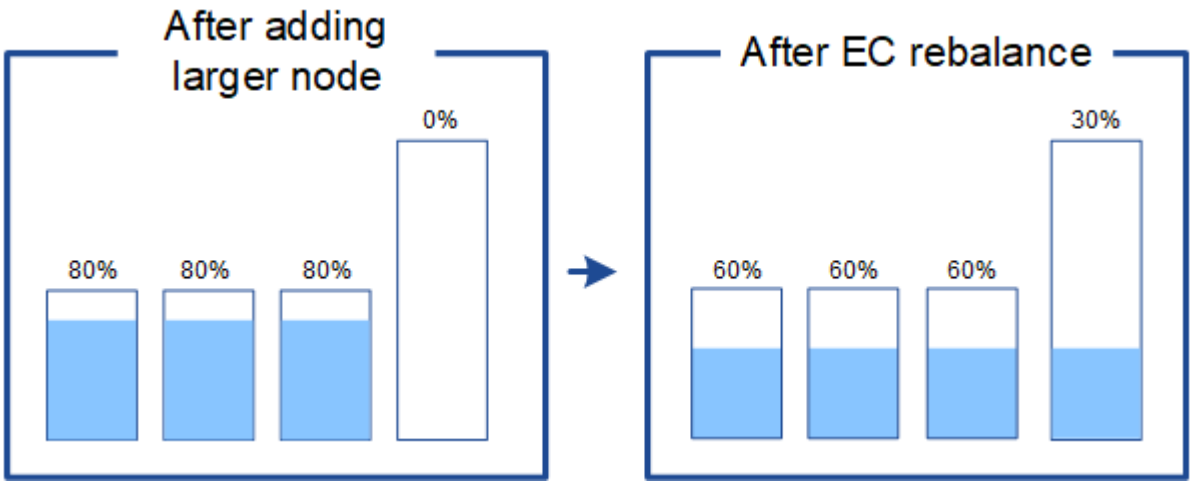
- Sposta solo i dati degli oggetti con codifica erasure. Non sposta i dati degli oggetti replicati.
- Ridistribuisce i dati all'interno di un sito. Non sposta i dati tra siti.
- Ridistribuisce i dati tra tutti i nodi di storage di un sito. Non ridistribuisce i dati all'interno dei volumi di storage.

- Non prende in considerazione l'utilizzo dei dati replicati su ciascun nodo di storage quando determina dove spostare i dati con codifica di cancellazione.
- Ridistribuisce in modo uniforme i dati con codifica di cancellazione tra i nodi di storage senza considerare le capacità relative di ciascun nodo.
- Non distribuirà i dati sottoposti a erasure coding ai nodi storage che sono pieni oltre il 80%.
- Potrebbe ridurre le performance delle operazioni ILM e delle operazioni dei client S3 e Swift quando viene eseguito. 8212; sono necessarie risorse aggiuntive per ridistribuire i frammenti di erasure coding.

Al termine della procedura di ribilanciamento EC:

- I dati con codifica erasure saranno stati spostati dai nodi di storage con meno spazio disponibile ai nodi di storage con più spazio disponibile.
- La protezione dei dati degli oggetti con codifica erasure rimane invariata.
- I valori utilizzati (%) potrebbero essere diversi tra i nodi di storage per due motivi:
  - Le copie replicate degli oggetti continueranno a consumare spazio sui nodi esistenti& 8212;la procedura di ribilanciamento EC non sposta i dati replicati.
  - I nodi con capacità maggiore saranno relativamente meno pieni dei nodi con capacità inferiore, anche se tutti i nodi finiranno con una quantità approssimativamente uguale di dati con codifica di cancellazione.

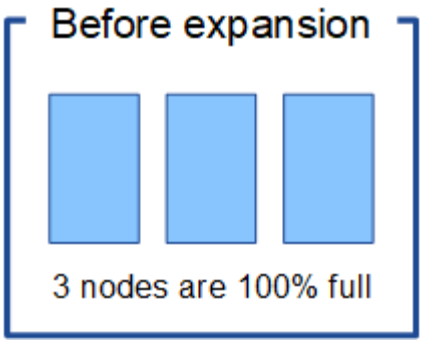
    Si supponga, ad esempio, che tre nodi da 200 TB siano riempiti al 80% ciascuno (200 e 215; 0.8 = 160 TB per ogni nodo o 480 TB per il sito). Se si aggiunge un nodo da 400 TB ed si esegue la procedura di ribilanciamento, tutti i nodi avranno ora circa la stessa quantità di dati di erasure-code (480/4 = 120 TB). Tuttavia, il valore utilizzato (%) per il nodo più grande sarà inferiore a quello utilizzato (%) per i nodi più piccoli.



Quando ribilanciare i dati con codifica di cancellazione

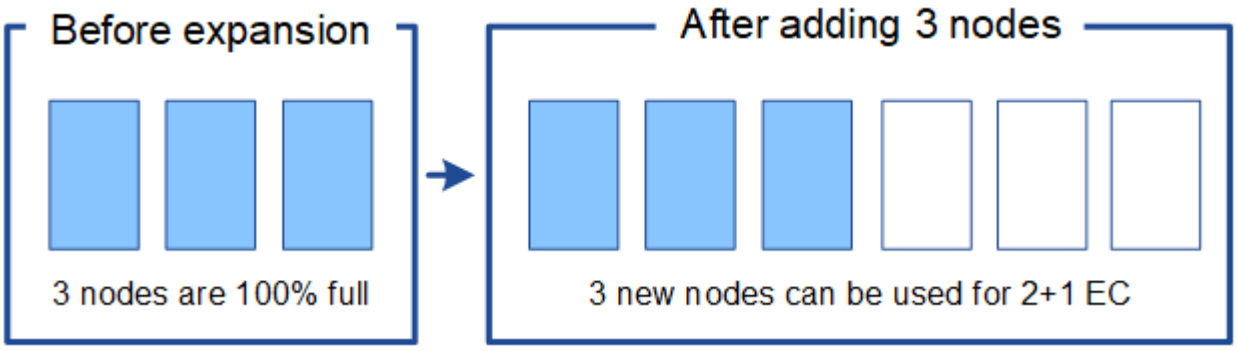
Considerare il seguente scenario:

- StorageGRID viene eseguito in un singolo sito, che contiene tre nodi di storage.
- Il criterio ILM utilizza una regola di erasure coding 2+1 per tutti gli oggetti più grandi di 1.0 MB e una regola di replica a 2 copie per gli oggetti più piccoli.
- Tutti i nodi di storage sono completamente pieni. L'avviso **Low Object Storage** è stato attivato al livello di gravità maggiore.



Il ribilanciamento non è necessario se si aggiungono nodi sufficienti

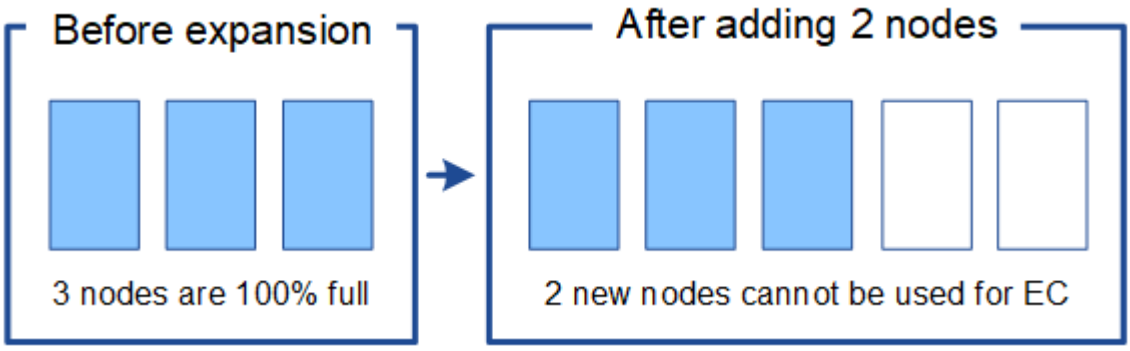
Per capire quando non è richiesto il ribilanciamento EC, supponiamo di aver aggiunto tre (o più) nuovi nodi di storage. In questo caso, non è necessario eseguire il ribilanciamento EC. I nodi di storage originali rimarranno pieni, ma i nuovi oggetti ora utilizzeranno i tre nuovi nodi per la codifica di cancellazione 2+1& 8212; i due frammenti di dati e un frammento di parità possono essere memorizzati su un nodo diverso.



Anche se in questo caso è possibile eseguire la procedura di ribilanciamento EC, lo spostamento dei dati con codifica di cancellazione esistenti ridurrà temporaneamente le prestazioni della griglia, con un impatto sulle operazioni del client.

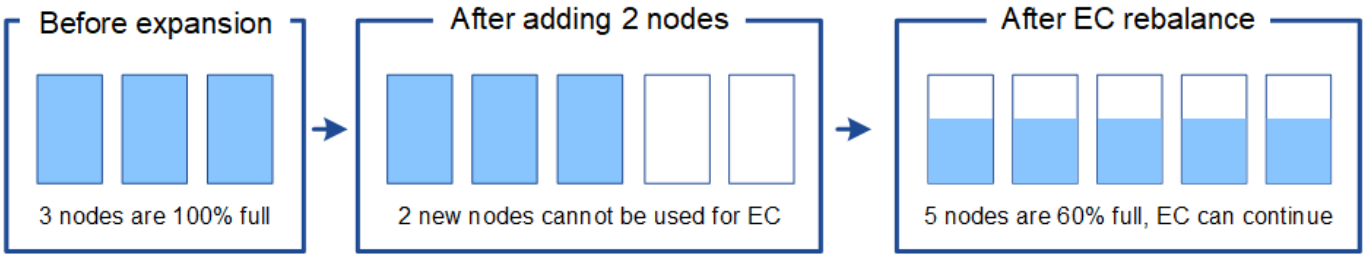
Il ribilanciamento è necessario se non è possibile aggiungere un numero sufficiente di nodi

Per capire quando è necessario ribilanciare EC, supponiamo di poter aggiungere solo due nodi storage, invece di tre. Poiché lo schema 2+1 richiede almeno tre nodi di storage per avere spazio disponibile, i nodi vuoti non possono essere utilizzati per i nuovi dati con codifica di cancellazione.



Per utilizzare i nuovi nodi di storage, è necessario eseguire la procedura di ribilanciamento EC. Quando viene

eseguita questa procedura, StorageGRID ridistribuisce i dati con codifica di cancellazione e i frammenti di parità esistenti tra tutti i nodi di storage del sito. In questo esempio, quando la procedura di ribilanciamento EC è completa, tutti e cinque i nodi sono ora pieni solo al 60% e gli oggetti possono continuare ad essere acquisiti nello schema di erasure coding 2+1 su tutti i nodi Storage.



Raccomandazioni per il ribilanciamento CE

NetApp richiede il ribilanciamento EC se *tutte* le seguenti affermazioni sono vere:

- Si utilizza la codifica di cancellazione per i dati dell'oggetto.
- L'avviso **Low Object Storage** è stato attivato per uno o più nodi di storage in un sito, a indicare che i nodi sono pieni al 80% o più.
- Non è possibile aggiungere un numero sufficiente di nuovi nodi di storage per lo schema di erasure coding in uso. Vedere "Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione".
- I client S3 e Swift possono tollerare prestazioni inferiori per le operazioni di scrittura e lettura durante l'esecuzione della procedura di ribilanciamento EC.

È possibile eseguire la procedura di ribilanciamento EC se si preferisce che i nodi di storage siano riempiti a livelli simili e i client S3 e Swift possono tollerare prestazioni inferiori per le operazioni di scrittura e lettura mentre la procedura di ribilanciamento EC è in esecuzione.

Come la procedura di ribilanciamento EC interagisce con altre attività di manutenzione

Non è possibile eseguire alcune procedure di manutenzione contemporaneamente all'esecuzione della procedura di ribilanciamento EC.

Procedura	Consentito durante la procedura di ribilanciamento EC?
Ulteriori procedure di ribilanciamento EC	No È possibile eseguire una sola procedura di ribilanciamento EC alla volta.
Procedura di decommissionamento Lavoro di riparazione dei dati EC	No • Non è possibile avviare una procedura di decommissionamento o una riparazione dei dati EC mentre è in esecuzione la procedura di ribilanciamento EC. • Non è possibile avviare la procedura di ribilanciamento EC mentre è in esecuzione una procedura di decommissionamento del nodo di storage o una riparazione dei dati EC.

Procedura	Consentito durante la procedura di ribilanciamento EC?
Procedura di espansione	No Se è necessario aggiungere nuovi nodi di storage in un'espansione, eseguire la procedura di ribilanciamento EC dopo aver aggiunto tutti i nuovi nodi.
Procedura di aggiornamento	No Se è necessario aggiornare il software StorageGRID, eseguire la procedura di aggiornamento prima o dopo l'esecuzione della procedura di ribilanciamento EC. Se necessario, è possibile terminare la procedura di ribilanciamento EC per eseguire un aggiornamento del software.
Procedura di clone del nodo dell'appliance	No Se è necessario clonare un nodo di storage dell'appliance, eseguire la procedura di ribilanciamento EC dopo aver aggiunto il nuovo nodo.
Procedura di hotfix	Sì. È possibile applicare una correzione rapida StorageGRID mentre è in esecuzione la procedura di ribilanciamento EC.
Altre procedure di manutenzione	No È necessario terminare la procedura di ribilanciamento EC prima di eseguire altre procedure di manutenzione.

Come la procedura di ribilanciamento EC interagisce con ILM

Durante l'esecuzione della procedura di ribilanciamento EC, evitare di apportare modifiche ILM che potrebbero modificare la posizione degli oggetti con codifica di cancellazione esistenti. Ad esempio, non iniziare a utilizzare una regola ILM con un profilo di erasure coding diverso. Se è necessario apportare tali modifiche ILM, interrompere la procedura di ribilanciamento EC.

Aggiungere capacità di metadati

Per garantire che sia disponibile spazio adeguato per i metadati degli oggetti, potrebbe essere necessario eseguire una procedura di espansione per aggiungere nuovi nodi di storage in ogni sito.

StorageGRID riserva spazio per i metadati degli oggetti sul volume 0 di ciascun nodo di storage. In ogni sito vengono conservate tre copie di tutti i metadati degli oggetti, distribuite uniformemente in tutti i nodi di storage.

È possibile utilizzare Grid Manager per monitorare la capacità dei metadati dei nodi di storage e stimare la velocità di utilizzo della capacità dei metadati. Inoltre, l'avviso **Low metadata storage** viene attivato per un nodo di storage quando lo spazio di metadati utilizzato raggiunge determinate soglie.

Si noti che la capacità dei metadati degli oggetti di una griglia potrebbe essere consumata più rapidamente rispetto alla capacità dello storage a oggetti, a seconda di come si utilizza la griglia. Ad esempio, se in genere

si acquisiscono grandi quantità di oggetti di piccole dimensioni o si aggiungono grandi quantità di metadati o tag utente agli oggetti, potrebbe essere necessario aggiungere nodi di storage per aumentare la capacità dei metadati anche se rimane sufficiente capacità di storage a oggetti.

Per ulteriori informazioni, vedere quanto segue:

- "Gestire lo storage dei metadati degli oggetti"
- "Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage"

Linee guida per aumentare la capacità dei metadati

Prima di aggiungere nodi di storage per aumentare la capacità dei metadati, consultare le seguenti linee guida e limitazioni:

- Supponendo che sia disponibile una capacità di storage a oggetti sufficiente, avere più spazio disponibile per i metadati a oggetti aumenta il numero di oggetti che è possibile memorizzare nel sistema StorageGRID.
- È possibile aumentare la capacità dei metadati di un grid aggiungendo uno o più nodi di storage a ciascun sito.
- Lo spazio effettivo riservato ai metadati dell'oggetto su qualsiasi nodo di storage specifico dipende dall'opzione di storage Metadata Reserved Space (impostazione a livello di sistema), dalla quantità di RAM allocata al nodo e dalla dimensione del volume 0 del nodo.
- Non è possibile aumentare la capacità dei metadati aggiungendo volumi di storage ai nodi di storage esistenti, perché i metadati vengono memorizzati solo sul volume 0.
- Non è possibile aumentare la capacità dei metadati aggiungendo un nuovo sito.
- StorageGRID conserva tre copie di tutti i metadati degli oggetti in ogni sito. Per questo motivo, la capacità dei metadati del sistema è limitata dalla capacità dei metadati del sito più piccolo.
- Quando si aggiunge la capacità dei metadati, è necessario aggiungere lo stesso numero di nodi di storage a ciascun sito.

Le risorse dei nodi di solo metadati basate su software devono corrispondere alle risorse dei nodi di storage esistenti. Ad esempio:

- Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:
  - 128 GB DI RAM
  - CPU a 8 core
  - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)
- Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuale con 24 GB di RAM, 8 core CPU e 3 TB o 4TB di memorizzazione di metadati, i nodi basati solo sui metadati del software devono utilizzare risorse simili (24 GB di RAM, 8 core CPU e 4TB di memorizzazione di metadati (rangedb/0).

Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve almeno StorageGRID corrispondere ai nodi storage dei siti StorageGRID esistenti e alle nuove risorse del sito.

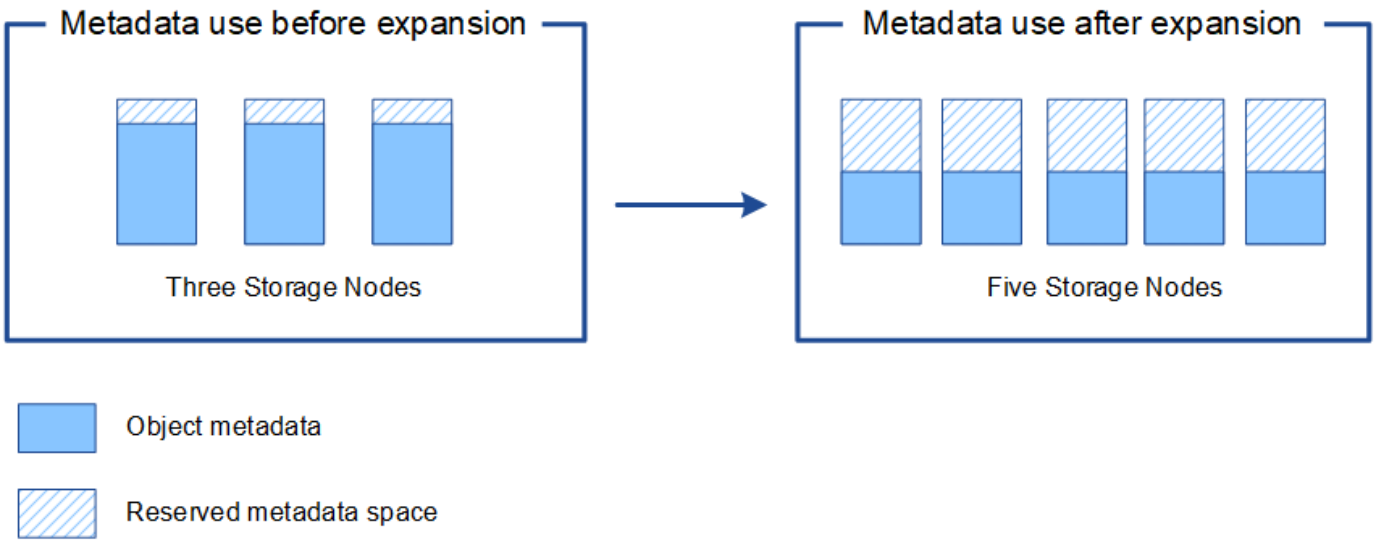
Vedere "Descrizione di Metadata Reserved Space".

Come vengono ridistribuiti i metadati quando si aggiungono nodi di storage

Quando si aggiungono nodi di storage in un'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti nei nuovi nodi di ciascun sito, aumentando così la capacità complessiva dei metadati del grid. Non è richiesta alcuna azione da parte dell'utente.

La figura seguente mostra come StorageGRID ridistribuisce i metadati degli oggetti quando si aggiungono nodi di storage in un'espansione. Il lato sinistro della figura rappresenta il volume 0 di tre nodi di storage prima di un'espansione. I metadati consumano una porzione relativamente grande dello spazio di metadati disponibile di ciascun nodo ed è stato attivato l'avviso **Low metadata storage**.

Il lato destro della figura mostra come vengono ridistribuiti i metadati esistenti dopo l'aggiunta di due nodi di storage al sito. La quantità di metadati su ciascun nodo è diminuita, l'avviso **Low metadata storage** non viene più attivato e lo spazio disponibile per i metadati è aumentato.



Aggiungi nodi grid per aggiungere funzionalità al tuo sistema

È possibile aggiungere ridondanza o funzionalità aggiuntive a un sistema StorageGRID aggiungendo nuovi nodi grid ai siti esistenti.

Ad esempio, è possibile scegliere di aggiungere nodi gateway da utilizzare in un gruppo ad alta disponibilità (ha) oppure aggiungere un nodo amministratore in un sito remoto per consentire il monitoraggio utilizzando un nodo locale.

È possibile aggiungere uno o più dei seguenti tipi di nodi a uno o più siti esistenti in una singola operazione di espansione:

- Nodi amministrativi non primari
- Nodi di storage
- Nodi gateway

Durante la preparazione all'aggiunta di nodi di rete, tenere presente le seguenti limitazioni:

- Il nodo di amministrazione primario viene implementato durante l'installazione iniziale. Non è possibile aggiungere un nodo amministratore primario durante un'espansione.
- È possibile aggiungere nodi di storage e altri tipi di nodi nella stessa espansione.

- Quando si aggiungono nodi di storage, è necessario pianificare attentamente il numero e la posizione dei nuovi nodi. Vedere "Linee guida per l'aggiunta della capacità degli oggetti".
- Se l'opzione **Imposta nuovo nodo predefinito** è **non attendibile** nella scheda reti client non attendibili della pagina di controllo Firewall, le applicazioni client che si connettono ai nodi di espansione utilizzando la rete client devono connettersi utilizzando una porta endpoint del bilanciamento del carico (**CONFIGURAZIONE** > **sicurezza** > **controllo firewall**). Consultare le istruzioni a. "modificare l'impostazione di sicurezza per il nuovo nodo" e a. "configurare gli endpoint del bilanciamento del carico".

Aggiungere un nuovo sito

È possibile espandere il sistema StorageGRID aggiungendo un nuovo sito.

Linee guida per l'aggiunta di un sito

Prima di aggiungere un sito, esaminare i seguenti requisiti e limitazioni:

- È possibile aggiungere un solo sito per ciascuna operazione di espansione.
- Non è possibile aggiungere nodi grid a un sito esistente come parte della stessa espansione.
- Tutti i siti devono includere almeno tre nodi di storage.
- L'aggiunta di un nuovo sito non aumenta automaticamente il numero di oggetti che è possibile memorizzare. La capacità totale degli oggetti di un grid dipende dalla quantità di storage disponibile, dal criterio ILM e dalla capacità dei metadati di ciascun sito.
- Quando si ridimensiona un nuovo sito, è necessario assicurarsi che includa una capacità di metadati sufficiente.

  StorageGRID conserva una copia di tutti i metadati degli oggetti in ogni sito. Quando si aggiunge un nuovo sito, è necessario assicurarsi che includa una capacità di metadati sufficiente per i metadati degli oggetti esistenti e una capacità di metadati sufficiente per la crescita.

  Per ulteriori informazioni, vedere quanto segue:

  - "Gestire lo storage dei metadati degli oggetti"
  - "Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage"
- È necessario considerare la larghezza di banda della rete disponibile tra i siti e il livello di latenza della rete. Gli aggiornamenti dei metadati vengono continuamente replicati tra i siti anche se tutti gli oggetti vengono memorizzati solo nel sito in cui vengono acquisiti.
- Poiché il sistema StorageGRID rimane operativo durante l'espansione, è necessario rivedere le regole ILM prima di avviare la procedura di espansione. È necessario assicurarsi che le copie a oggetti non vengano memorizzate nel nuovo sito fino al completamento della procedura di espansione.

  Ad esempio, prima di iniziare l'espansione, determinare se alcune regole utilizzano il pool di storage predefinito (tutti i nodi di storage). In tal caso, è necessario creare un nuovo pool di storage contenente i nodi di storage esistenti e aggiornare le regole ILM per utilizzare il nuovo pool di storage. In caso contrario, gli oggetti verranno copiati nel nuovo sito non appena il primo nodo del sito diventa attivo.

  Per ulteriori informazioni sulla modifica di ILM durante l'aggiunta di un nuovo sito, consultare "Esempio di modifica di un criterio ILM".

Raccogliere il materiale necessario

Prima di eseguire un'operazione di espansione, raccogliere i materiali e installare e configurare eventuali nuovi hardware e reti.

Elemento	Note
Archivio di installazione di StorageGRID	Se si aggiungono nuovi nodi di griglia o un nuovo sito, è necessario scaricare ed estrarre l'archivio di installazione di StorageGRID. È necessario utilizzare la stessa versione attualmente in esecuzione sulla griglia. Per ulteriori informazioni, consultare le istruzioni di Download ed estrazione dei file di installazione di StorageGRID. **Nota:** non è necessario scaricare i file se si aggiungono nuovi volumi di storage ai nodi di storage esistenti o si installa una nuova appliance StorageGRID.
Laptop di assistenza	Il laptop di assistenza dispone di quanto segue: • Porta di rete • Client SSH (ad esempio, putty) • "Browser Web supportato"
`Passwords.txt` file	Contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando. Incluso nel pacchetto di ripristino.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non si trova in `Passwords.txt` file.
Documentazione StorageGRID	• "Amministrare StorageGRID" • "Note di rilascio" • Istruzioni per l'installazione della piattaforma ◦ "Installare StorageGRID su Red Hat Enterprise Linux" ◦ "Installare StorageGRID su Ubuntu o Debian" ◦ "Installare StorageGRID su VMware"
Documentazione aggiornata per la piattaforma	Per le versioni supportate, vedere "Tool di matrice di interoperabilità (IMT)".

Scaricare ed estrarre i file di installazione di StorageGRID

Prima di poter aggiungere nuovi nodi grid o un nuovo sito, è necessario scaricare l'archivio di installazione StorageGRID appropriato ed estrarre i file.

A proposito di questa attività

È necessario eseguire operazioni di espansione utilizzando la versione di StorageGRID attualmente in esecuzione sulla griglia.

Fasi

1. Passare a. "Download NetApp: StorageGRID".
2. Selezionare la versione di StorageGRID attualmente in esecuzione nella griglia.
3. Accedi con il nome utente e la password del tuo account NetApp.
4. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).
5. Nella colonna **Installa StorageGRID** della pagina di download, selezionare `.tgz` oppure `.zip` file per la tua piattaforma.

   La versione mostrata nel file di archivio dell'installazione deve corrispondere alla versione del software attualmente installato.

   Utilizzare `.zip` File se si esegue Windows sul laptop di assistenza.

Piattaforma	Archivio di installazione

Red Hat Enterprise Linux	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`

Ubuntu o Debian o appliance	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

OpenStack/Altro hypervisor	Per espandere una distribuzione esistente su OpenStack, è necessario implementare una macchina virtuale che esegue una delle distribuzioni Linux supportate elencate sopra e seguire le istruzioni appropriate per Linux.

6. Scaricare ed estrarre il file di archivio.
7. Seguire la fase appropriata per la piattaforma per scegliere i file necessari, in base alla piattaforma, alla topologia della griglia pianificata e al modo in cui si espanderà il sistema StorageGRID.

   I percorsi elencati nella fase per ciascuna piattaforma sono relativi alla directory di primo livello installata dal file di archivio.

8. Se state espandendo un sistema Red Hat Enterprise Linux, selezionate i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Pacchetto RPM per l'installazione delle immagini del nodo StorageGRID sui vostri host RHEL.
	Pacchetto RPM per l'installazione del servizio host StorageGRID sugli host RHEL.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per il ping federate.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di ruolo e playbook Ansible per la configurazione degli host RHEL per l'implementazione dei container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Script di supporto chiamato dal compagno `storagegrid-ssoauth-azure.py` Script Python per eseguire interazioni SSO con Azure.

Percorso e nome del file	Descrizione
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta espandendo un sistema Ubuntu o Debian, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Un file di licenza NetApp non in produzione che è possibile utilizzare per le implementazioni di test e proof of concept.
	PACCHETTO DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.
	Checksum MD5 per il file `/debs/storagegrid-webscale-images-version-SHA.deb`.
	PACCHETTO DEB per l'installazione del servizio host StorageGRID su host Ubuntu o Debian.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per il ping federate.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.

Percorso e nome del file	Descrizione
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di manuale e ruolo Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Script di supporto chiamato dal compagno `storagegrid-ssoauth-azure.py` Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta espandendo un sistema VMware, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid.
	Il file di modello Open Virtualization Format (`.ovf`) e il file manifest (`.mf`) Per l'implementazione del nodo di amministrazione primario.

Percorso e nome del file	Descrizione
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi amministrativi non primari.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi di archiviazione.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi gateway.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi di storage basati su macchine virtuali.
Tool di scripting per la distribuzione	Descrizione
	Uno script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.
	Un file di configurazione di esempio da utilizzare con `deploy-vsphere-ovftool.sh` script.
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando è attivato il Single Sign-on (SSO). È anche possibile utilizzare questo script per il ping federate.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Script di supporto chiamato dal compagno `storagegrid-ssoauth-azure.py` Script Python per eseguire interazioni SSO con Azure.

Percorso e nome del file	Descrizione
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta espandendo un sistema basato su appliance StorageGRID, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	PACCHETTO DEB per l'installazione delle immagini del nodo StorageGRID sulle appliance.
	Checksum MD5 per il file `/debs/storagegridwebscale-images-version-SHA.deb`.

Per l'installazione dell'appliance, questi file sono necessari solo se è necessario evitare il traffico di rete. L'appliance può scaricare i file richiesti dal nodo di amministrazione principale.

Verificare l'hardware e il collegamento in rete

Prima di iniziare l'espansione del sistema StorageGRID, verificare quanto segue:

- L'hardware necessario per supportare i nuovi nodi di rete o il nuovo sito è stato installato e configurato.
- Tutti i nuovi nodi dispongono di percorsi di comunicazione bidirezionali per tutti i nodi esistenti e nuovi (un requisito per la Grid Network). In particolare, verificare che le seguenti porte TCP siano aperte tra i nuovi nodi che si stanno aggiungendo nell'espansione e il nodo di amministrazione primario:
  - 1055
  - 7443
  - 8011
  - 10342

  Vedere "Comunicazioni interne al nodo di rete".
- Il nodo di amministrazione primario può comunicare con tutti i server di espansione destinati a ospitare il sistema StorageGRID.
- Se uno dei nuovi nodi ha un indirizzo IP Grid Network su una subnet non utilizzata in precedenza, l'operazione è già stata effettuata "aggiunta della nuova subnet" Nell'elenco Grid Network Subnet (subnet rete griglia). In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e avviare nuovamente la procedura.
- Non stai utilizzando la conversione degli indirizzi di rete (NAT) 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. L'utilizzo di NAT per il bridge della rete Grid attraverso un segmento di rete pubblico è supportato solo se si utilizza un'applicazione di tunneling trasparente a tutti
Nodi nella griglia, ovvero i nodi della griglia non richiedono alcuna conoscenza degli indirizzi IP pubblici.

Questa restrizione NAT è specifica per i nodi di griglia e la rete di griglia. 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.

Aggiungere volumi di storage

Aggiungere volumi di storage ai nodi di storage

È possibile espandere la capacità di storage dei nodi di storage con un numero di volumi di storage inferiore o uguale a 16 aggiungendo ulteriori volumi di storage. Potrebbe essere necessario aggiungere volumi di storage a più di un nodo di storage per soddisfare i requisiti ILM per le copie replicate o con codifica di cancellazione.

Prima di iniziare

Prima di aggiungere volumi di storage, consultare "linee guida per l'aggiunta della capacità degli oggetti" Per assicurarsi di sapere dove aggiungere volumi per soddisfare i requisiti della policy ILM.

> Queste istruzioni sono valide solo per i nodi storage basati su software. Vedere "Aggiunta di shelf di espansione a SG6060 implementato" oppure "Aggiungi shelf di espansione alla piattaforma SG6160 implementata" Per scoprire come aggiungere volumi di storage a SG6060 o SG6160 installando shelf di espansione. Impossibile espandere altri nodi storage dell'appliance.

A proposito di questa attività

Lo storage sottostante di un nodo di storage è suddiviso in volumi di storage. I volumi di storage sono dispositivi di storage basati su blocchi formattati dal sistema StorageGRID e montati per memorizzare oggetti. Ciascun nodo di storage può supportare fino a 16 volumi di storage, denominati *archivi di oggetti* in Grid Manager.

> I metadati degli oggetti sono sempre memorizzati nell'archivio di oggetti 0.

Ogni archivio di oggetti viene montato su un volume che corrisponde al relativo ID. Ad esempio, l'archivio di oggetti con un ID di 0000 corrisponde a. `/var/local/rangedb/0` punto di montaggio.

Prima di aggiungere nuovi volumi di storage, utilizzare Grid Manager per visualizzare gli archivi di oggetti correnti per ciascun nodo di storage e i punti di montaggio corrispondenti. È possibile utilizzare queste informazioni quando si aggiungono volumi di storage.

Fasi

1. Selezionare **NODES** > ***Site*** > ***Storage Node*** > **Storage**.
2. Scorrere verso il basso per visualizzare le quantità di storage disponibili per ciascun volume e archivio di oggetti.

   Per i nodi di storage dell'appliance, il nome globale di ciascun disco corrisponde all'identificativo mondiale

del volume (WWID) visualizzato quando si visualizzano le proprietà dei volumi standard in SANtricity OS (il software di gestione collegato al controller di storage dell'appliance).

Per semplificare l'interpretazione delle statistiche di lettura e scrittura dei dischi relative ai punti di montaggio del volume, la prima parte del nome visualizzato nella colonna **Name** della tabella Disk Devices (periferiche disco) (ovvero *sdc*, *sdd*, *sde* e così via) corrisponde al valore visualizzato nella colonna **Device** della tabella Volumes (volumi).

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

3. Seguire le istruzioni della piattaforma per aggiungere nuovi volumi di storage al nodo di storage.
   - "VMware: Aggiunta di volumi di storage a Storage Node"
   - "Linux: Aggiunta di volumi direct-attached o SAN al nodo di storage"

VMware: Aggiunta di volumi di storage a Storage Node

Se un nodo di storage include meno di 16 volumi di storage, è possibile aumentarne la capacità utilizzando VMware vSphere per aggiungere volumi.

Prima di iniziare

- È possibile accedere alle istruzioni per l'installazione di StorageGRID per le implementazioni VMware.
  - "Installare StorageGRID su VMware"
- Hai il `Passwords.txt` file.
- Lo hai fatto "autorizzazioni di accesso specifiche".

> Non tentare di aggiungere volumi di storage a un nodo di storage mentre è attiva una procedura di aggiornamento del software, di ripristino o un'altra procedura di espansione.

A proposito di questa attività

Il nodo di storage non è disponibile per un breve periodo di tempo quando si aggiungono volumi di storage. È necessario eseguire questa procedura su un nodo di storage alla volta per evitare impatti sui servizi grid rivolti al client.

Fasi

1. Se necessario, installare nuovo hardware per lo storage e creare nuovi datastore VMware.
2. Aggiungere uno o più dischi rigidi alla macchina virtuale per utilizzarli come storage (archivi di oggetti).
   a. Aprire VMware vSphere Client.
   b. Modificare le impostazioni della macchina virtuale per aggiungere uno o più dischi rigidi aggiuntivi.

   I dischi rigidi sono in genere configurati come Virtual Machine Disk (VMDK). I VMDK sono più comunemente utilizzati e sono più facili da gestire, mentre i RDM potrebbero fornire performance migliori per i carichi di lavoro che utilizzano oggetti di dimensioni maggiori (ad esempio, superiori a 100 MB). Per ulteriori informazioni sull'aggiunta di dischi rigidi alle macchine virtuali, consultare la documentazione di VMware vSphere.
3. Riavviare la macchina virtuale utilizzando l'opzione **Restart Guest OS** (Riavvia sistema operativo guest) in VMware vSphere Client o immettendo il seguente comando in una sessione ssh sulla macchina virtuale:`sudo reboot`

   > Non utilizzare **Power Off** o **Reset** per riavviare la macchina virtuale.
4. Configurare il nuovo storage per l'utilizzo da parte del nodo di storage:
   a. Accedere al nodo Grid:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.

iii. Immettere il seguente comando per passare a root: `su -`

iv. Immettere la password elencata in `Passwords.txt` file.
Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

b. Configurare i nuovi volumi di storage:

```
sudo add_rangedbs.rb
```

Questo script trova i nuovi volumi di storage e richiede di formattarli.

c. Immettere **y** per accettare la formattazione.

d. Se uno dei volumi è stato precedentemente formattato, decidere se si desidera riformattarlo.

- Immettere **y** per riformattare.
- Inserire **n** per saltare la riformattazione.

Il `setup_rangedbs.sh` lo script viene eseguito automaticamente.

5. Verificare che i servizi vengano avviati correttamente:

a. Visualizzare un elenco dello stato di tutti i servizi sul server:

```
sudo storagegrid-status
```

Lo stato viene aggiornato automaticamente.

a. Attendere che tutti i servizi siano in esecuzione o verificati.

b. Uscire dalla schermata di stato:

```
Ctrl+C
```

6. Verificare che il nodo di storage sia in linea:

a. Accedere a Grid Manager utilizzando un "browser web supportato".

b. Selezionare **SUPPORT** > **Tools** > **Grid topology**.

c. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Storage**.

d. Selezionare la scheda **Configurazione**, quindi la scheda **principale**.

e. Se l'elenco a discesa **Storage state - Desired** (Stato di storage - desiderato) è impostato su Read-only (sola lettura) o Offline (non in linea), selezionare **Online**.

f. Selezionare **Applica modifiche**.

7. Per visualizzare i nuovi archivi di oggetti:

a. Selezionare **NODES** > ***Site*** > ***Storage Node*** > **Storage**.

b. Visualizzare i dettagli nella tabella **Object Stores**.

Risultato

È possibile utilizzare la capacità estesa dei nodi di storage per salvare i dati degli oggetti.

Linux: Aggiunta di volumi direct-attached o SAN al nodo di storage

Se un nodo di storage include meno di 16 volumi di storage, è possibile aumentarne la

capacità aggiungendo nuovi dispositivi di storage a blocchi, rendendoli visibili agli host Linux e aggiungendo i nuovi mapping dei dispositivi a blocchi al file di configurazione StorageGRID utilizzato per il nodo di storage.

Prima di iniziare

- Hai accesso alle istruzioni per l'installazione di StorageGRID per la tua piattaforma Linux.
  - "Installare StorageGRID su Red Hat Enterprise Linux"
  - "Installare StorageGRID su Ubuntu o Debian"
- Hai il `Passwords.txt` file.
- Lo hai fatto "autorizzazioni di accesso specifiche".

> Non tentare di aggiungere volumi di storage a un nodo di storage mentre è attiva una procedura di aggiornamento del software, di ripristino o un'altra procedura di espansione.

A proposito di questa attività

Il nodo di storage non è disponibile per un breve periodo di tempo quando si aggiungono volumi di storage. È necessario eseguire questa procedura su un nodo di storage alla volta per evitare impatti sui servizi grid rivolti al client.

Fasi

1. Installare il nuovo hardware di storage.

   Per ulteriori informazioni, consultare la documentazione fornita dal fornitore dell'hardware.

2. Creare nuovi volumi di storage a blocchi delle dimensioni desiderate.
   - Collegare le nuove unità e aggiornare la configurazione del controller RAID secondo necessità, oppure allocare le nuove LUN SAN sugli array di storage condivisi e consentire all'host Linux di accedervi.
   - Utilizzare lo stesso schema di denominazione persistente utilizzato per i volumi di storage sul nodo di storage esistente.
   - Se si utilizza la funzionalità di migrazione dei nodi StorageGRID, rendere visibili i nuovi volumi agli altri host Linux che sono destinazioni di migrazione per questo nodo di storage.
     Per ulteriori informazioni, consulta le istruzioni per l'installazione di StorageGRID per la tua piattaforma Linux.
3. Accedere all'host Linux che supporta il nodo di storage come root o con un account che dispone dell'autorizzazione sudo.
4. Verificare che i nuovi volumi di storage siano visibili sull'host Linux.

   Potrebbe essere necessario eseguire una nuova scansione per le periferiche.

5. Eseguire il seguente comando per disattivare temporaneamente il nodo di storage:

   ```
   sudo storagegrid node stop <node-name>
   ```

6. Utilizzando un editor di testo come vim o pico, modificare il file di configurazione del nodo per il nodo di storage, disponibile all'indirizzo `/etc/storagegrid/nodes/<node-name>.conf`.
7. Individuare la sezione del file di configurazione del nodo che contiene le mappature dei dispositivi di blocco dello storage a oggetti esistenti.

Nell'esempio, `BLOCK_DEVICE_RANGEDB_00` a. `BLOCK_DEVICE_RANGEDB_03` sono le mappature esistenti dei dispositivi a blocchi di storage a oggetti.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. Aggiungere nuove mappature dei dispositivi a blocchi di storage a oggetti corrispondenti ai volumi di storage a blocchi aggiunti per questo nodo di storage.

   Assicurarsi di iniziare dal successivo `BLOCK_DEVICE_RANGEDB_nn`. Non lasciare un gap.

   - In base all'esempio precedente, iniziare da `BLOCK_DEVICE_RANGEDB_04`.
   - Nell'esempio riportato di seguito, sono stati aggiunti quattro nuovi volumi di storage a blocchi al nodo: `BLOCK_DEVICE_RANGEDB_04` a. `BLOCK_DEVICE_RANGEDB_07`.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. Eseguire il seguente comando per convalidare le modifiche apportate al file di configurazione del nodo per il nodo di storage:

```
sudo storagegrid node validate <node-name>
```

Risolvere eventuali errori o avvisi prima di passare alla fase successiva.

> Se si osserva un errore simile a quanto segue, significa che il file di configurazione del nodo sta tentando di mappare il dispositivo a blocchi utilizzato da `<node-name>` per `<PURPOSE>` al dato `<path-name>` Nel file system Linux, ma non esiste un file speciale valido per il dispositivo a blocchi (o un softlink a un file speciale per il dispositivo a blocchi) in tale posizione.
>
> ```
> Checking configuration file for node <node-name>…
> ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
> <path-name> is not a valid block device
> ```
>
> Verificare di aver inserito il corretto `<path-name>`.

10. Eseguire il seguente comando per riavviare il nodo con le nuove mappature del dispositivo a blocchi in posizione:

    ```
    sudo storagegrid node start <node-name>
    ```

11. Accedere al nodo di storage come amministratore utilizzando la password elencata in `Passwords.txt` file.
12. Verificare che i servizi vengano avviati correttamente:
    a. Visualizzare un elenco dello stato di tutti i servizi sul server:

       ```
       sudo storagegrid-status
       ```

       Lo stato viene aggiornato automaticamente.

    b. Attendere che tutti i servizi siano in esecuzione o verificati.
    c. Uscire dalla schermata di stato:

       ```
       Ctrl+C
       ```

13. Configurare il nuovo storage per l'utilizzo da parte del nodo di storage:
    a. Configurare i nuovi volumi di storage:

       ```
       sudo add_rangedbs.rb
       ```

       Questo script trova i nuovi volumi di storage e richiede di formattarli.

    b. Inserire **y** per formattare i volumi di storage.
    c. Se uno dei volumi è stato precedentemente formattato, decidere se si desidera riformattarlo.
       - Immettere **y** per riformattare.
       - Inserire **n** per saltare la riformattazione.

Il `setup_rangedbs.sh` lo script viene eseguito automaticamente.

14. Verificare che il nodo di storage sia in linea:
    a. Accedere a Grid Manager utilizzando un "browser web supportato".
    b. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
    c. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Storage**.
    d. Selezionare la scheda **Configurazione**, quindi la scheda **principale**.
    e. Se l'elenco a discesa **Storage state - Desired** (Stato di storage - desiderato) è impostato su Read-only (sola lettura) o Offline (non in linea), selezionare **Online**.
    f. Fare clic su **Applica modifiche**.
15. Per visualizzare i nuovi archivi di oggetti:
    a. Selezionare **NODES** > ***Site*** > ***Storage Node*** > **Storage**.
    b. Visualizzare i dettagli nella tabella **Object Stores**.

Risultato

È ora possibile utilizzare la capacità estesa dei nodi di storage per salvare i dati degli oggetti.

Aggiunta di nodi o siti grid

Aggiunta di nodi di griglia al sito esistente o aggiunta di un nuovo sito

Seguire questa procedura per aggiungere nodi di griglia a siti esistenti o per aggiungere un nuovo sito. È possibile eseguire un solo tipo di espansione alla volta.

Prima di iniziare

- Hai il "Autorizzazione di accesso root o di manutenzione".
- Tutti i nodi esistenti nel grid sono attivi e in esecuzione in tutti i siti.
- Tutte le precedenti procedure di espansione, aggiornamento, disattivazione o ripristino sono state completate.

> Non è possibile avviare un'espansione mentre è in corso un'altra procedura di espansione, aggiornamento, ripristino o decommissionamento attivo. Tuttavia, se necessario, è possibile sospendere una procedura di decommissionamento per avviare un'espansione.

Fasi

1. "Aggiornare le subnet per Grid Network".
2. "Implementare nuovi nodi grid".
3. "Eseguire l'espansione".

Aggiornare le subnet per Grid Network

Quando si aggiungono nodi griglia o un nuovo sito in un'espansione, potrebbe essere necessario aggiornare o aggiungere sottoreti alla rete Grid.

StorageGRID mantiene un elenco delle subnet di rete utilizzate per comunicare tra i nodi della griglia sulla rete (eth0). Queste voci includono le subnet utilizzate per la rete griglia da ciascun sito nel sistema StorageGRID, nonché le subnet utilizzate per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway della

rete griglia.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.
- Si dispone degli indirizzi di rete, in notazione CIDR, delle subnet che si desidera configurare.

A proposito di questa attività

Se uno dei nuovi nodi ha un indirizzo IP Grid Network su una subnet non utilizzata in precedenza, è necessario aggiungere la nuova subnet all'elenco Grid Network subnet prima di avviare l'espansione. In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e avviare nuovamente la procedura.

Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete di amministrazione o la rete client di alcun nodo:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Ad esempio, non utilizzare i seguenti intervalli di subnet per la rete Grid, la rete amministrativa o la rete client di alcun nodo:

- 192.168.130.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 198.51.100.2 e 198.51.100.4

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **rete griglia**.
2. Selezionare **Aggiungi un'altra subnet** per aggiungere una nuova subnet nella notazione CIDR.

   Ad esempio, immettere `10.96.104.0/22`.

3. Inserire la passphrase di provisioning e selezionare **Save** (Salva).
4. Attendere che le modifiche vengano applicate, quindi scaricare un nuovo pacchetto di ripristino.
   a. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.
   b. Immettere la **Provisioning Passphrase**.

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. Viene inoltre utilizzato per ripristinare il nodo di amministrazione primario.

Le subnet specificate vengono configurate automaticamente per il sistema StorageGRID.

Implementare nuovi nodi grid

I passaggi per l'implementazione di nuovi nodi grid in un'espansione sono gli stessi utilizzati al momento dell'installazione della griglia. Prima di eseguire l'espansione, è necessario implementare tutti i nuovi nodi grid.

Quando si espande una griglia, i nodi aggiunti non devono corrispondere ai tipi di nodo esistenti. È possibile aggiungere nodi VMware, nodi Linux basati su container o nodi appliance.

VMware: Implementazione di nodi grid

È necessario implementare una macchina virtuale in VMware vSphere per ciascun nodo VMware che si desidera aggiungere all'espansione.

Fasi

1. "Implementare il nuovo nodo come macchina virtuale" E connetterlo a una o più reti StorageGRID.

   Quando si implementa il nodo, è possibile rimappare le porte del nodo o aumentare le impostazioni della CPU o della memoria.

2. Dopo aver implementato tutti i nuovi nodi VMware, "eseguire la procedura di espansione".

Linux: Implementazione di nodi grid

È possibile implementare nodi grid su nuovi host Linux o su host Linux esistenti. Se sono necessari altri host Linux per supportare i requisiti di CPU, RAM e storage dei nodi StorageGRID che si desidera aggiungere al grid, è necessario prepararli nello stesso modo in cui sono stati preparati gli host al momento dell'installazione. Quindi, i nodi di espansione vengono implementati nello stesso modo in cui vengono implementati i nodi di rete durante l'installazione.

Prima di iniziare

- Sono disponibili le istruzioni per l'installazione di StorageGRID per la versione di Linux in uso e i requisiti hardware e storage.
  - "Installare StorageGRID su Red Hat Enterprise Linux"
  - "Installare StorageGRID su Ubuntu o Debian"
- Se si prevede di implementare nuovi nodi grid su host esistenti, è stato confermato che gli host esistenti dispongono di CPU, RAM e capacità di storage sufficienti per i nodi aggiuntivi.
- Hai un piano per ridurre al minimo i domini di guasto. Ad esempio, non è necessario implementare tutti i nodi gateway su un singolo host fisico.

In un'implementazione in produzione, non eseguire più di un nodo di storage su un singolo host fisico o virtuale. L'utilizzo di un host dedicato per ciascun nodo di storage fornisce un dominio di errore isolato.

- Se il nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verifica che il volume non disponga di una policy di tiering FabricPool abilitata. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

Fasi

1. Se si aggiungono nuovi host, accedere alle istruzioni di installazione per l'implementazione dei nodi StorageGRID.
2. Per implementare i nuovi host, seguire le istruzioni per la preparazione degli host.
3. Per creare file di configurazione del nodo e convalidare la configurazione StorageGRID, seguire le istruzioni per l'implementazione dei nodi Grid.
4. Se si aggiungono nodi a un nuovo host Linux, avviare il servizio host StorageGRID.
5. Se si aggiungono nodi a un host Linux esistente, avviare i nuovi nodi utilizzando la CLI del servizio host StorageGRID:`sudo storagegrid node start [<node name\>]`

Al termine

Dopo aver implementato tutti i nuovi nodi grid, è possibile "eseguire l'espansione".

Appliance: Implementazione di storage, gateway o nodi di amministrazione non primari

Per installare il software StorageGRID su un nodo appliance, utilizzare il programma di installazione dell'appliance StorageGRID, incluso nell'appliance. In un'espansione, ogni appliance di storage funziona come un singolo nodo di storage e ogni appliance di servizi funziona come un singolo nodo di gateway o un nodo di amministrazione non primario. Qualsiasi appliance può connettersi a Grid Network, Admin Network e Client Network.

Prima di iniziare

- L'apparecchio è stato installato in un rack o in un cabinet, collegato alla rete e acceso.
- Hai completato il "Configurare l'hardware" fasi.

  La configurazione dell'hardware dell'appliance include i passaggi necessari per la configurazione delle connessioni StorageGRID (collegamenti di rete e indirizzi IP), nonché i passaggi facoltativi per abilitare la crittografia dei nodi, modificare la modalità RAID e rimappare le porte di rete.

- Tutte le subnet della rete griglia elencate nella pagina di configurazione IP del programma di installazione dell'appliance StorageGRID sono state definite nell'elenco delle subnet della rete griglia nel nodo di amministrazione principale.
- Il firmware del programma di installazione dell'appliance StorageGRID sull'appliance sostitutiva è compatibile con la versione del software StorageGRID attualmente in esecuzione sulla griglia. Se le versioni non sono compatibili, è necessario aggiornare il firmware del programma di installazione dell'appliance StorageGRID.
- Si dispone di un laptop di assistenza con un "browser web supportato".
- Conosci uno degli indirizzi IP assegnati al controller di calcolo dell'appliance. È possibile utilizzare l'indirizzo IP per qualsiasi rete StorageGRID collegata.

A proposito di questa attività

Il processo di installazione di StorageGRID su un nodo appliance prevede le seguenti fasi:

- Specificare o confermare l'indirizzo IP del nodo Admin primario e il nome del nodo appliance.
- Avviare l'installazione e attendere la configurazione dei volumi e l'installazione del software.

Durante le attività di installazione dell'appliance, l'installazione viene interrotta. Per riprendere l'installazione, accedi a Grid Manager, approva tutti i nodi della griglia e completa il processo di installazione di StorageGRID.

> Se è necessario implementare più nodi appliance contemporaneamente, è possibile automatizzare il processo di installazione utilizzando `configure-sga.py` Script di installazione dell'appliance.

Fasi

1. Aprire un browser e inserire uno degli indirizzi IP del controller di elaborazione dell'appliance.

   `https://Controller_IP:8443`

   Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.

2. Nella sezione connessione **Primary Admin Node**, determinare se è necessario specificare l'indirizzo IP per il nodo di amministrazione primario.

   Se in precedenza sono stati installati altri nodi in questo data center, il programma di installazione dell'appliance StorageGRID è in grado di rilevare automaticamente questo indirizzo IP, supponendo che il nodo di amministrazione primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente sulla stessa sottorete.

3. Se questo indirizzo IP non viene visualizzato o se è necessario modificarlo, specificare l'indirizzo:

Opzione	Descrizione
Immissione manuale dell'IP	a. Deselezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Inserire l'indirizzo IP manualmente. c. Fare clic su **Save** (Salva). d. Attendere che lo stato di connessione del nuovo indirizzo IP diventi pronto.
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Attendere che venga visualizzato l'elenco degli indirizzi IP rilevati. c. Selezionare il nodo di amministrazione principale per la griglia in cui verrà implementato il nodo di storage dell'appliance. d. Fare clic su **Save** (Salva). e. Attendere che lo stato di connessione del nuovo indirizzo IP diventi pronto.

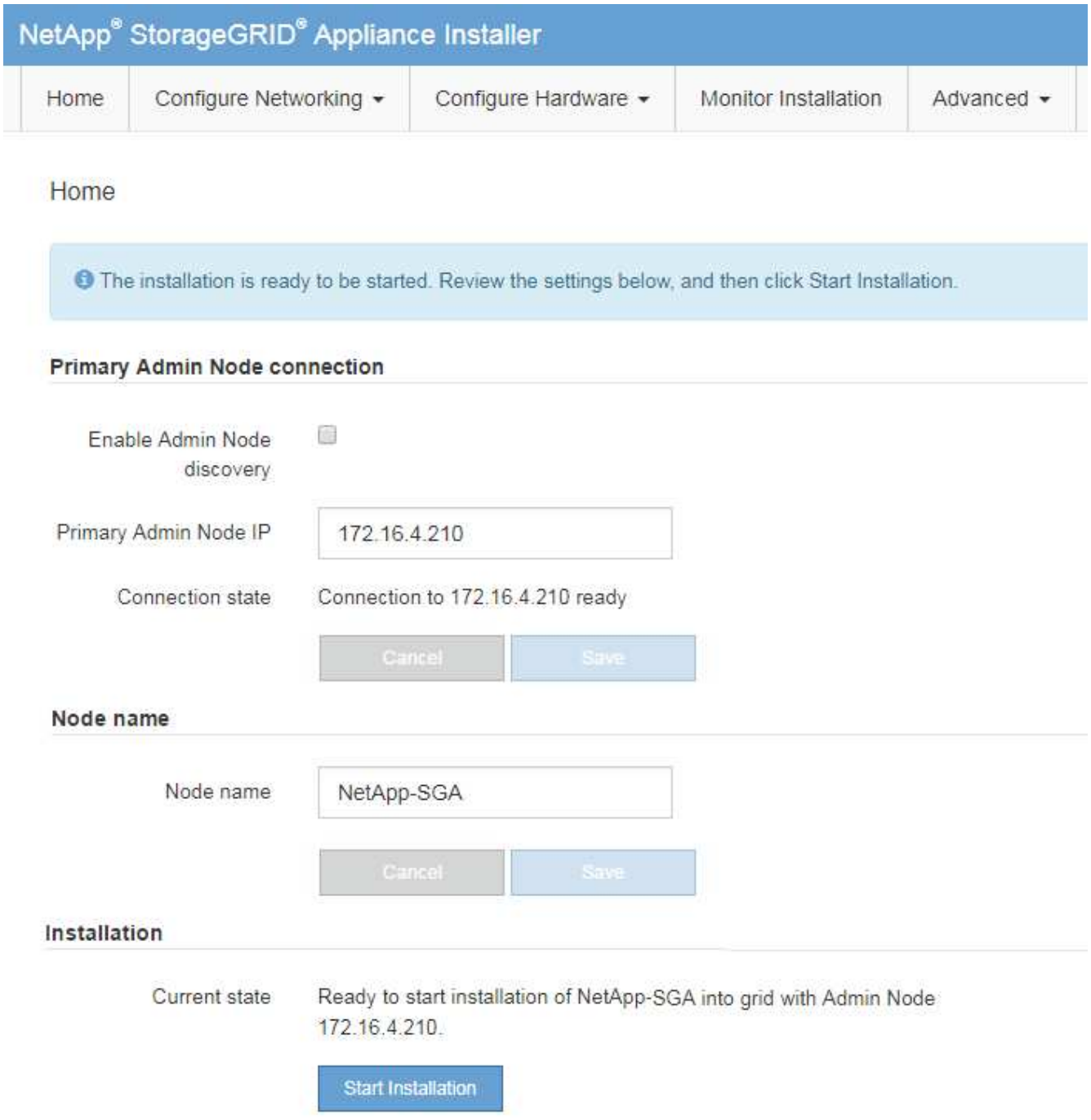
4. Nel campo **Node name** (Nome nodo), immettere il nome che si desidera utilizzare per il nodo dell'appliance e selezionare **Save** (Salva).

   Il nome del nodo viene assegnato al nodo dell'appliance nel sistema StorageGRID. Viene visualizzato nella pagina nodi (scheda Panoramica) di Grid Manager. Se necessario, è possibile modificare il nome quando si approva il nodo.

5. Nella sezione **Installazione**, verificare che lo stato corrente sia "Pronto per avviare l'installazione di *node name* nella griglia con nodo di amministrazione primario *admin_ip*" e che il pulsante **Avvia installazione** sia attivato.

   Se il pulsante **Avvia installazione** non è attivato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per istruzioni, consultare le istruzioni di manutenzione dell'apparecchio.

6. Dalla home page del programma di installazione dell'appliance StorageGRID, selezionare **Avvia installazione**.



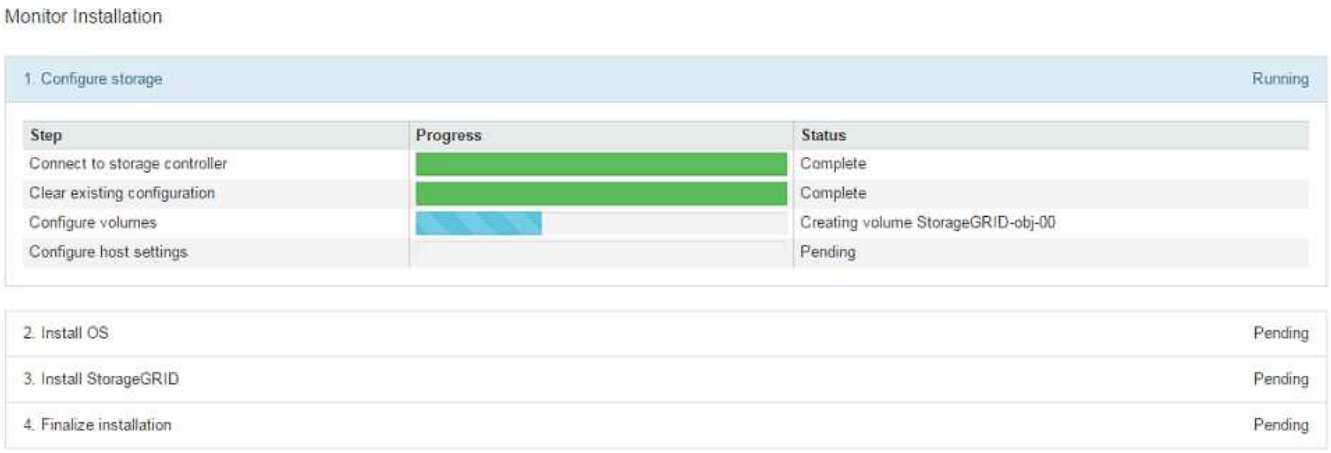
   Lo stato corrente cambia in "Installazione in corso" e viene visualizzata la pagina Installazione monitor.

7. Se l'espansione include più nodi appliance, ripetere i passaggi precedenti per ogni appliance.

Se è necessario implementare più nodi storage dell'appliance contemporaneamente, è possibile automatizzare il processo di installazione utilizzando lo script di installazione dell'appliance configure-sga.py.

8. Per accedere manualmente alla pagina Installazione monitor, selezionare **Installazione monitor** dalla barra dei menu.

   La pagina Monitor Installation (Installazione monitor) mostra lo stato di avanzamento dell'installazione.



   La barra di stato blu indica l'attività attualmente in corso. Le barre di stato verdi indicano le attività completate correttamente.

   Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si sta eseguendo nuovamente un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "saltato".

9. Esaminare i progressi delle prime due fasi dell'installazione.

   1. Configurare l'appliance

   In questa fase, si verifica uno dei seguenti processi:

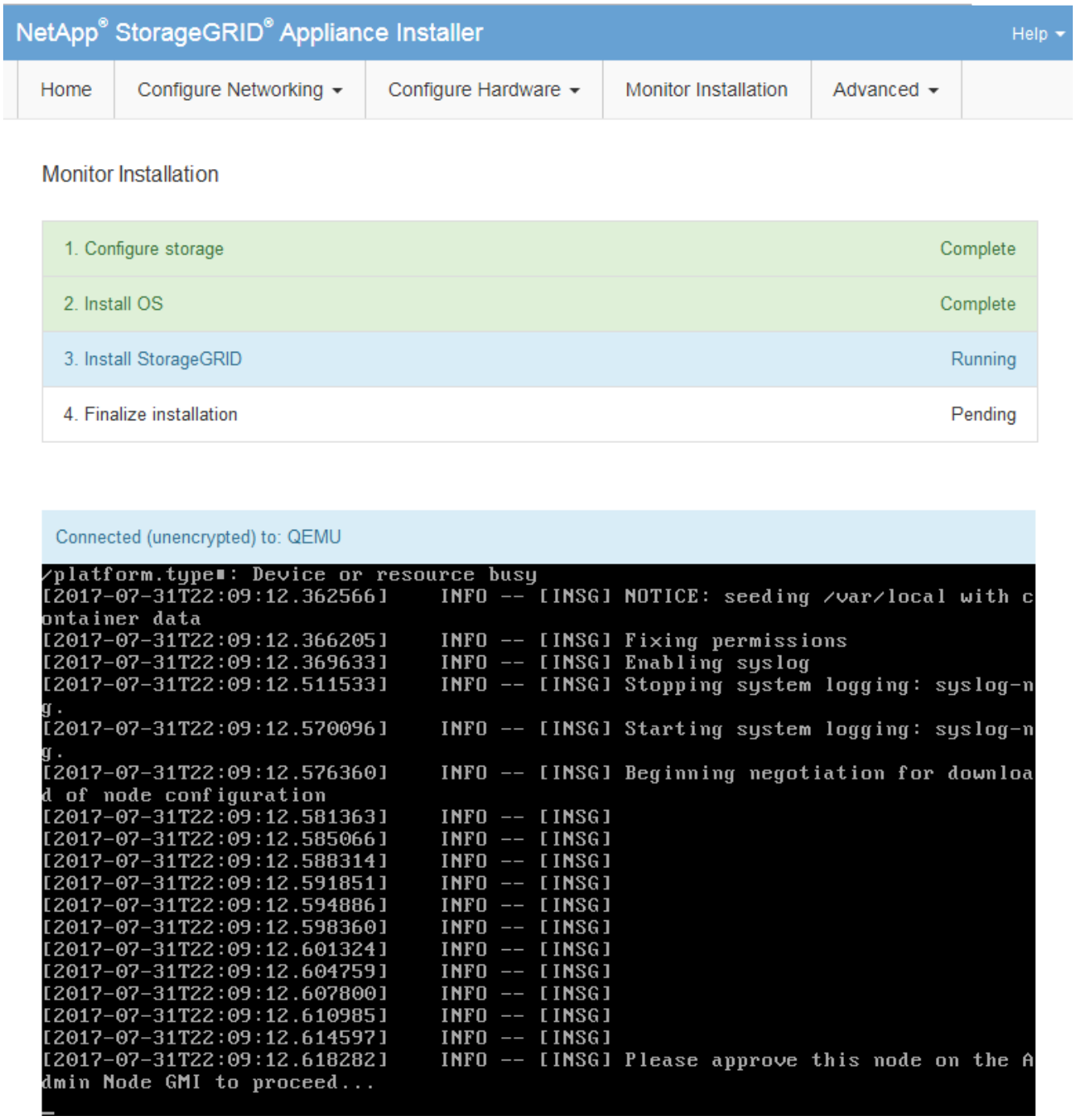
   - Per un'appliance di storage, il programma di installazione si connette al controller dello storage, cancella qualsiasi configurazione esistente, comunica con SANtricity OS per configurare i volumi e configura le impostazioni dell'host.
   - Per un'appliance di servizi, il programma di installazione cancella qualsiasi configurazione esistente dai dischi nel controller di calcolo e configura le impostazioni dell'host.

   2. Installare il sistema operativo

   In questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID nell'appliance.

10. Continuare a monitorare l'avanzamento dell'installazione fino a quando non viene visualizzato un messaggio nella finestra della console, che richiede di utilizzare Grid Manager per approvare il nodo.

    Attendere che tutti i nodi aggiunti a questa espansione siano pronti per l'approvazione prima di passare al Grid Manager per approvare i nodi.



Eseguire l'espansione

Quando si esegue l'espansione, i nuovi nodi grid vengono aggiunti all'implementazione StorageGRID esistente.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone della passphrase di provisioning.
- Sono stati implementati tutti i nodi grid che vengono aggiunti in questa espansione.
- Hai il "Autorizzazione di manutenzione o di accesso root".

- Se si aggiungono nodi di storage, si conferma che tutte le operazioni di riparazione dei dati eseguite come parte di un ripristino sono state completate. Vedere "Controllare i lavori di riparazione dei dati".
- Se si aggiungono nodi di storage e si desidera assegnare un livello di storage personalizzato a tali nodi, è già stato fatto "creato il livello di storage personalizzato". Si dispone anche dell'autorizzazione di accesso root o di entrambe le autorizzazioni Maintenance e ILM.
- Se si aggiunge un nuovo sito, sono state riviste e aggiornate le regole ILM. È necessario assicurarsi che le copie a oggetti non vengano memorizzate nel nuovo sito fino al completamento dell'espansione. Ad esempio, se una regola utilizza il pool di storage predefinito (**tutti i nodi di storage**), è necessario "creare un nuovo pool di storage" Che contiene solo i nodi di storage esistenti e. "Aggiornare le regole ILM" E il criterio ILM per utilizzare il nuovo pool di storage. In caso contrario, gli oggetti verranno copiati nel nuovo sito non appena il primo nodo del sito diventa attivo.

A proposito di questa attività

L'esecuzione dell'espansione include le seguenti attività principali dell'utente:

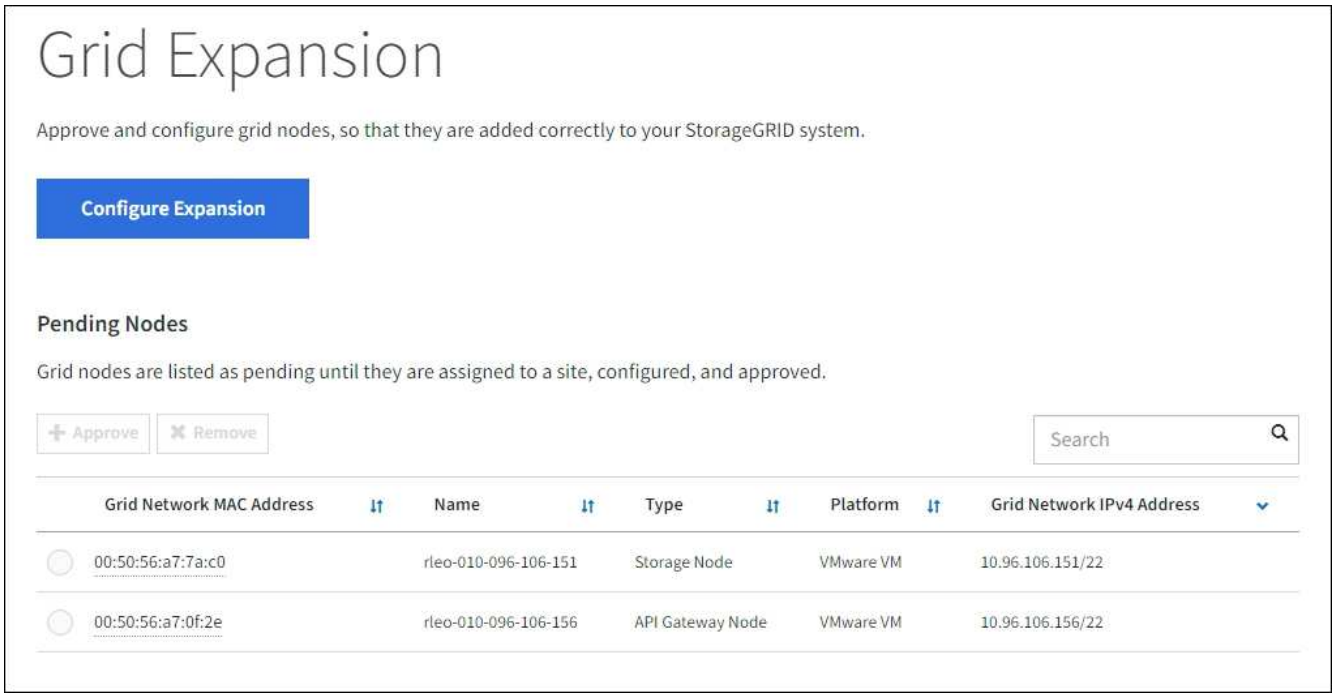
1. Configurare l'espansione.
2. Avviare l'espansione.
3. Scaricare un nuovo file di Recovery Package.
4. Monitorare le fasi e le fasi di espansione fino a quando tutti i nuovi nodi non vengono installati e configurati e tutti i servizi non vengono avviati.

> Alcune fasi e fasi di espansione potrebbero richiedere molto tempo per essere eseguite su un grande grid. Ad esempio, lo streaming di Cassandra su un nuovo nodo di storage potrebbe richiedere solo pochi minuti se il database Cassandra è vuoto. Tuttavia, se il database Cassandra include una grande quantità di metadati degli oggetti, questa fase potrebbe richiedere diverse ore o più. Non riavviare i nodi di storage durante le fasi "espansione del cluster Cassandra" o "Avvio di Cassandra e dati in streaming".

Fasi

1. Selezionare **MANUTENZIONE** > **attività** > **espansione**.

   Viene visualizzata la pagina Grid Expansion (espansione griglia). La sezione Pending Nodes (nodi in sospeso) elenca i nodi che sono pronti per essere aggiunti.

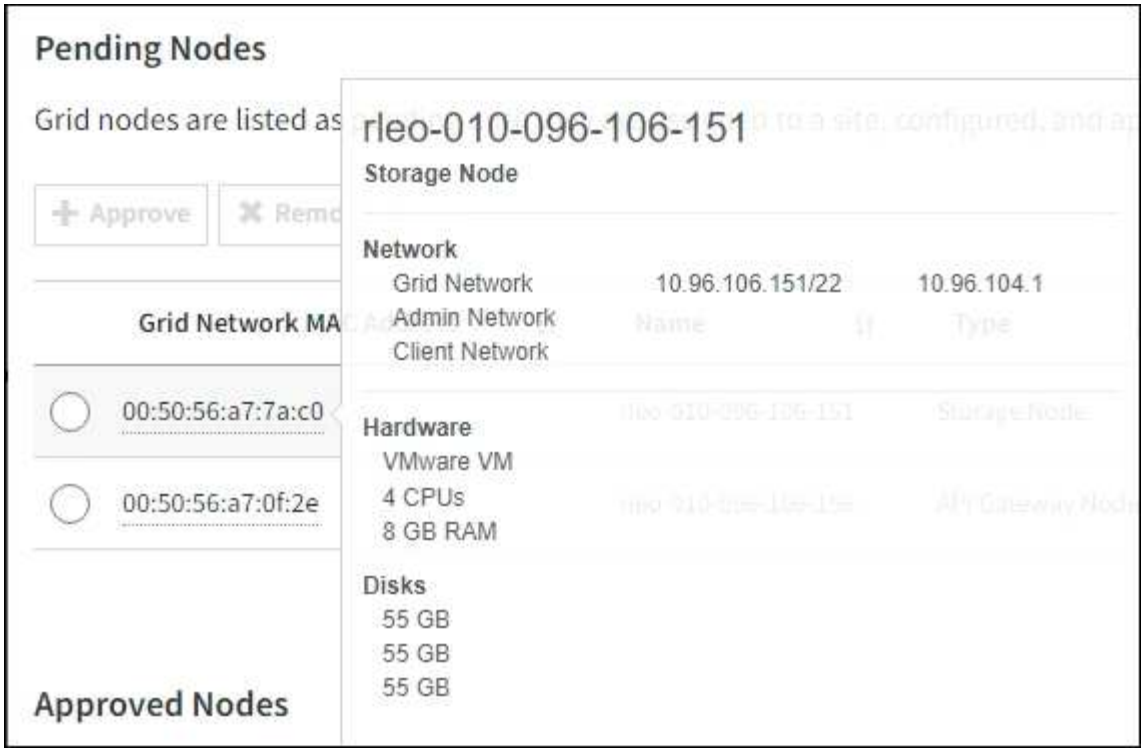


2. Selezionare **Configure Expansion** (Configura espansione).

   Viene visualizzata la finestra di dialogo Site Selection (selezione sito).

3. Selezionare il tipo di espansione che si desidera avviare:
   - Se si sta aggiungendo un nuovo sito, selezionare **nuovo** e immettere il nome del nuovo sito.
   - Se si aggiungono uno o più nodi a un sito esistente, selezionare **esistente**.
4. Selezionare **Salva**.
5. Esaminare l'elenco **Pending Nodes** (nodi in sospeso) e confermare che mostra tutti i nodi della griglia implementati.

   Se necessario, puoi posizionare il cursore su **Grid Network MAC Address** di un nodo per visualizzare i dettagli relativi a tale nodo.



Se manca un nodo, confermarne la corretta implementazione.

6. Dall'elenco dei nodi in sospeso, approvare i nodi che si desidera aggiungere a questa espansione.
   a. Selezionare il pulsante di opzione accanto al primo nodo della griglia in sospeso che si desidera approvare.
   b. Selezionare **approva**.

      Viene visualizzato il modulo di configurazione del nodo della griglia.

   c. Se necessario, modificare le impostazioni generali:

Campo	Descrizione
Sito	Il nome del sito a cui verrà associato il nodo della griglia. Se si aggiungono più nodi, assicurarsi di selezionare il sito corretto per ciascun nodo. Se si aggiunge un nuovo sito, tutti i nodi vengono aggiunti al nuovo sito.
Nome	Il nome di sistema del nodo. I nomi di sistema sono richiesti per le operazioni StorageGRID interne e non possono essere modificati.

Campo	Descrizione
Ruolo NTP	Il ruolo NTP (Network Time Protocol) del nodo Grid: • Selezionare **automatico** (impostazione predefinita) per assegnare automaticamente il ruolo NTP al nodo. Il ruolo primario verrà assegnato ai nodi di amministrazione, ai nodi di storage con servizi ADC, ai nodi gateway e a tutti i nodi grid che hanno indirizzi IP non statici. Il ruolo Client verrà assegnato a tutti gli altri nodi della griglia. • Selezionare **Primary** per assegnare manualmente il ruolo Primary NTP al nodo. Almeno due nodi in ogni sito devono avere il ruolo primario per fornire un accesso ridondante al sistema a fonti di tempistica esterne. • Selezionare **Client** per assegnare manualmente il ruolo NTP client al nodo.
Servizio ADC (solo nodi di storage)	Se questo nodo di storage eseguirà il servizio ADC (Administrative Domain Controller). Il servizio ADC tiene traccia della posizione e della disponibilità dei servizi grid. Almeno tre nodi di storage in ogni sito devono includere il servizio ADC. Non è possibile aggiungere il servizio ADC a un nodo dopo averlo implementato. • Selezionare **Sì** se il nodo di storage che si sta sostituendo include il servizio ADC. Poiché non è possibile decommissionare un nodo di storage se rimangono pochi servizi ADC, questo garantisce che sia disponibile un nuovo servizio ADC prima che il vecchio servizio venga rimosso. • Selezionare **automatico** per consentire al sistema di determinare se questo nodo richiede il servizio ADC. Ulteriori informazioni su "Quorum ADC".
Storage grade (solo nodi storage)	Utilizzare il livello di storage **Default** o selezionare il livello di storage personalizzato che si desidera assegnare al nuovo nodo. I livelli di storage vengono utilizzati dai pool di storage ILM, in modo che la selezione possa influire sugli oggetti da posizionare nel nodo di storage.

d. Se necessario, modificare le impostazioni per Grid Network, Admin Network e Client Network.

- **IPv4 Address (CIDR)**: Indirizzo di rete CIDR per l'interfaccia di rete. Ad esempio: 172.16.10.100/24

> Se si scopre che i nodi hanno indirizzi IP duplicati sulla rete Grid durante l'approvazione dei nodi, è necessario annullare l'espansione, ridistribuire le macchine virtuali o le appliance con un IP non duplicato e riavviare l'espansione.

- **Gateway**: Il gateway predefinito del nodo Grid. Ad esempio: 172.16.10.1
- **Subnet (CIDR)**: Una o più sottoreti per la rete di amministrazione.

e. Selezionare **Salva**.

Il nodo della griglia approvata passa all'elenco dei nodi approvati.

- Per modificare le proprietà di un nodo della griglia approvato, selezionare il relativo pulsante di opzione e selezionare **Modifica**.
- Per spostare di nuovo un nodo della griglia approvato nell'elenco Pending Nodes (nodi in sospeso), selezionare il relativo pulsante di opzione e selezionare **Reset** (Ripristina).
- Per rimuovere in modo permanente un nodo di rete approvato, spegnere il nodo. Quindi, selezionare il pulsante di opzione corrispondente e selezionare **Rimuovi**.

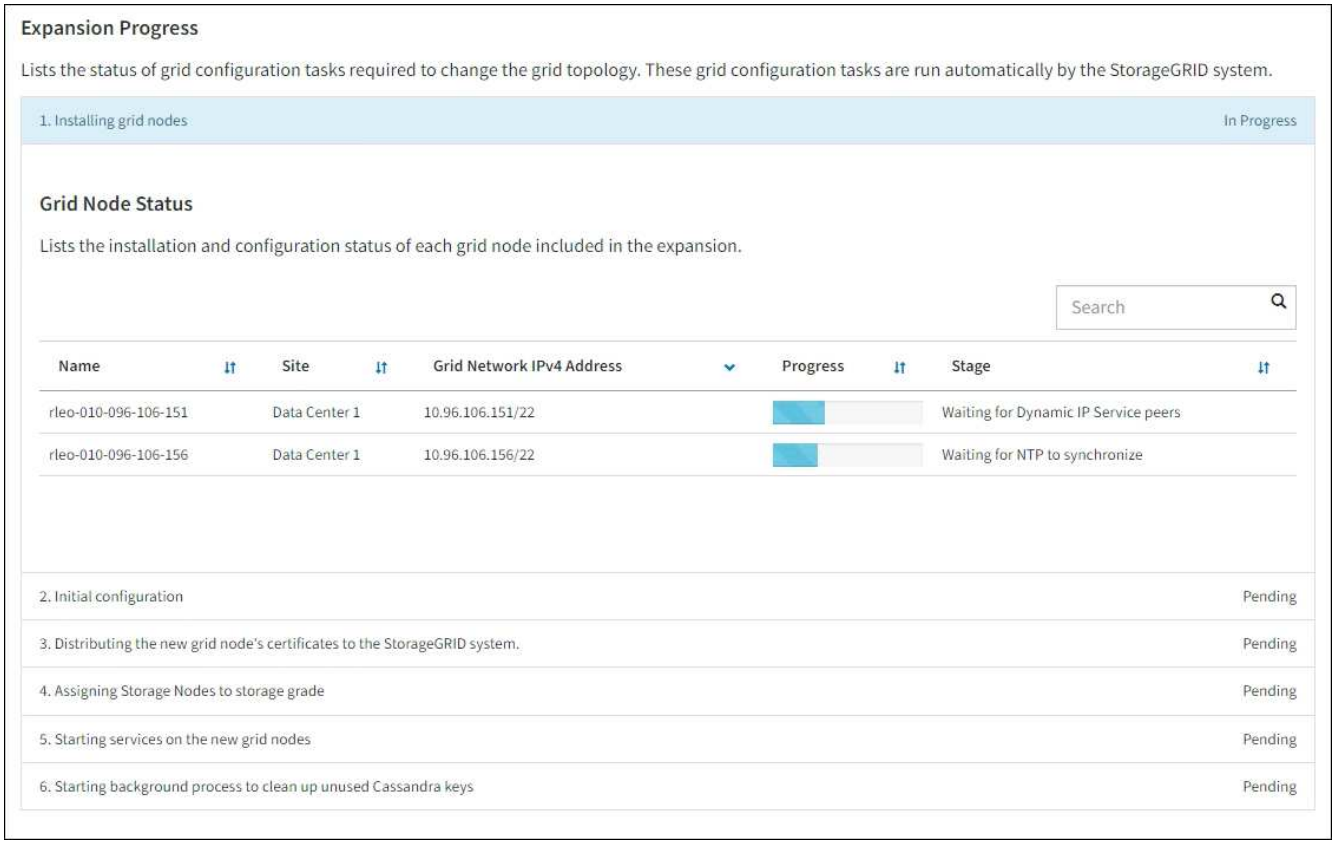
f. Ripetere questi passaggi per ogni nodo griglia in sospeso che si desidera approvare.

> Se possibile, è necessario approvare tutte le note della griglia in sospeso ed eseguire una singola espansione. Se si eseguono più piccole espansioni, sarà necessario più tempo.

7. Una volta approvati tutti i nodi della griglia, immettere la **Provisioning Passphrase** e selezionare **Espandi**.

Dopo alcuni minuti, questa pagina viene aggiornata per visualizzare lo stato della procedura di espansione. Quando sono in corso attività che influiscono sui singoli nodi della griglia, la sezione Grid Node Status (Stato nodo griglia) elenca lo stato corrente di ciascun nodo della griglia.

> Durante la fase "Installazione dei nodi griglia" per una nuova appliance, il programma di installazione dell'appliance StorageGRID mostra il passaggio dall'installazione della fase 3 alla fase 4, completamento dell'installazione. Al termine della fase 4, il controller viene riavviato.



Un'espansione del sito include un'attività aggiuntiva per configurare Cassandra per il nuovo sito.

8. Non appena viene visualizzato il collegamento **Download Recovery Package**, scaricare il file Recovery Package.

   È necessario scaricare una copia aggiornata del file del pacchetto di ripristino il prima possibile dopo aver apportato modifiche alla topologia della griglia al sistema StorageGRID. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

   a. Selezionare il collegamento per il download.
   b. Inserire la passphrase di provisioning e selezionare **Avvia download**.
   c. Al termine del download, aprire `.zip` archiviare e confermare che è possibile accedere ai contenuti, incluso il `Passwords.txt` file.
   d. Copiare il file del pacchetto di ripristino scaricato (`.zip`) in due posizioni sicure e separate.

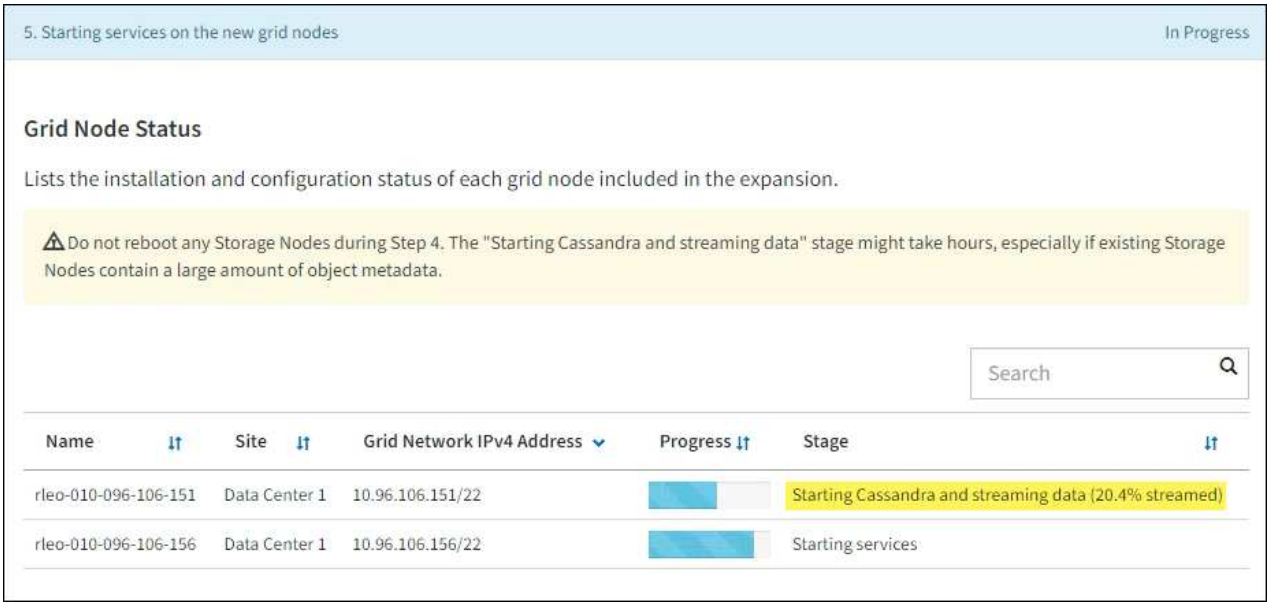
   Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

9. Se si aggiungono nodi di storage a un sito esistente o si aggiunge un sito, monitorare le fasi di Cassandra, che si verificano quando i servizi vengono avviati sui nuovi nodi di griglia.

   Non riavviare i nodi di storage durante le fasi di "espansione del cluster Cassandra" o "avvio di Cassandra e dati in streaming". Il completamento di queste fasi potrebbe richiedere molte ore per ogni nuovo nodo di storage, soprattutto se i nodi di storage esistenti contengono una grande quantità di metadati degli oggetti.

Aggiunta di nodi di storage

Se si aggiungono nodi di storage a un sito esistente, esaminare la percentuale indicata nel messaggio di stato "Avvio di Cassandra e streaming dei dati".



Questa percentuale stima il completamento dell'operazione di streaming Cassandra in base alla quantità totale di dati Cassandra disponibili e alla quantità già scritta nel nuovo nodo.

Aggiunta del sito

Se si aggiunge un nuovo sito, utilizzare `nodetool status` Monitorare i progressi dello streaming Cassandra e verificare quanti metadati sono stati copiati nel nuovo sito durante la fase di "espansione del cluster Cassandra". Il carico totale di dati sul nuovo sito deve essere inferiore a circa il 20% del totale di un sito corrente.

10. Continuare a monitorare l'espansione fino al completamento di tutte le attività e alla ricomposizione del pulsante **Configure Expansion** (Configura espansione).

Al termine

A seconda dei tipi di nodi griglia aggiunti, eseguire ulteriori operazioni di integrazione e configurazione. Vedere "Fasi di configurazione dopo l'espansione".

Configurare il sistema esteso

Fasi di configurazione dopo l'espansione

Dopo aver completato un'espansione, è necessario eseguire ulteriori operazioni di integrazione e configurazione.

A proposito di questa attività

È necessario completare le attività di configurazione elencate di seguito per i nodi o i siti di griglia che si stanno aggiungendo all'espansione. Alcune attività potrebbero essere facoltative, a seconda delle opzioni selezionate durante l'installazione e l'amministrazione del sistema e di come si desidera configurare i nodi e i siti aggiunti durante l'espansione.

Fasi

1. Se è stato aggiunto un sito:
   - "Creare un pool di storage" Per il sito e per ogni livello di storage selezionato per i nuovi nodi di storage.
   - Verificare che la policy ILM soddisfi i nuovi requisiti. Se sono necessarie modifiche alle regole, "creare nuove regole" e. "Aggiornare il criterio ILM". Se le regole sono già corrette, "attivare una nuova policy" Senza modifiche alle regole per garantire che StorageGRID utilizzi i nuovi nodi.
   - Verificare che i server NTP (Network Time Protocol) siano accessibili da tale sito. Vedere "Gestire i server NTP".

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

2. Se sono stati aggiunti uno o più nodi di storage a un sito esistente:
   - "Visualizzare i dettagli del pool di storage" Per confermare che ciascun nodo aggiunto sia incluso nei pool di storage previsti e utilizzato nelle regole ILM previste.
   - Verificare che la policy ILM soddisfi i nuovi requisiti. Se sono necessarie modifiche alle regole, "creare nuove regole" e. "Aggiornare il criterio ILM". Se le regole sono già corrette, "attivare una nuova policy" Senza modifiche alle regole per garantire che StorageGRID utilizzi i nuovi nodi.
   - "Verificare che il nodo di storage sia attivo" e in grado di acquisire oggetti.
   - Se non è stato possibile aggiungere il numero consigliato di nodi di storage, ribilanciare i dati con codifica di cancellazione. Vedere "Ribilanciare i dati con codifica di cancellazione dopo l'aggiunta di nodi di storage".
3. Se è stato aggiunto un nodo gateway:
   - Se si utilizzano gruppi ad alta disponibilità (ha) per le connessioni client, aggiungere facoltativamente il nodo gateway a un gruppo ha. Selezionare **CONFIGURATION** > **Network** > **High Availability groups** per rivedere l'elenco dei gruppi ha esistenti e aggiungere il nuovo nodo. Vedere "Configurare i gruppi ad alta disponibilità".
4. Se è stato aggiunto un nodo amministratore:
   a. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, creare un trust per la parte di base per il nuovo nodo di amministrazione. Non è possibile accedere al nodo fino a quando non si crea questo trust per la parte di base. Vedere "Configurare il single sign-on".
   b. Se si intende utilizzare il servizio Load Balancer sui nodi Admin, aggiungere facoltativamente il nuovo nodo Admin a un gruppo ha. Selezionare **CONFIGURATION** > **Network** > **High Availability groups** per rivedere l'elenco dei gruppi ha esistenti e aggiungere il nuovo nodo. Vedere "Configurare i gruppi ad alta disponibilità".
   c. Facoltativamente, copiare il database del nodo di amministrazione dal nodo di amministrazione primario al nodo di amministrazione di espansione se si desidera mantenere costanti le informazioni di attributo e controllo su ciascun nodo di amministrazione. Vedere "Copiare il database Admin Node".
   d. Facoltativamente, copiare il database Prometheus dal nodo di amministrazione primario al nodo di amministrazione di espansione se si desidera mantenere costanti le metriche storiche su ciascun nodo di amministrazione. Vedere "Copia le metriche Prometheus".

e. Facoltativamente, copiare i registri di controllo esistenti dal nodo di amministrazione principale al nodo di amministrazione dell'espansione se si desidera mantenere coerenti le informazioni di registro cronologiche su ciascun nodo di amministrazione. Vedere "Copia dei registri di audit".

5. Per verificare se i nodi di espansione sono stati aggiunti con una rete client non attendibile o per modificare se la rete client di un nodo è non attendibile o attendibile, andare a **CONFIGURAZIONE** > **sicurezza** > **controllo firewall**.

   Se la rete client sul nodo di espansione non è attendibile, le connessioni al nodo sulla rete client devono essere effettuate utilizzando un endpoint di bilanciamento del carico. Vedere "Configurare gli endpoint del bilanciamento del carico" e. "Gestire i controlli firewall".

6. Configurare il DNS.

   Se le impostazioni DNS sono state specificate separatamente per ciascun nodo della griglia, è necessario aggiungere impostazioni DNS personalizzate per nodo per i nuovi nodi. Vedere "Modificare la configurazione DNS per un nodo griglia singolo".

Per garantire il corretto funzionamento, specificare due o tre server DNS. Se si specificano più di tre, è possibile che ne vengano utilizzati solo tre a causa delle limitazioni del sistema operativo note su alcune piattaforme. Se nel proprio ambiente sono presenti restrizioni di routing, è possibile "Personalizzare l'elenco dei server DNS" Per i singoli nodi (in genere tutti i nodi di un sito) di utilizzare un set diverso di un massimo di tre server DNS.

Se possibile, utilizzare i server DNS a cui ciascun sito può accedere localmente per garantire che un sito islanded possa risolvere i FQDN per le destinazioni esterne.

Verificare che il nodo di storage sia attivo

Al termine di un'operazione di espansione che aggiunge nuovi nodi di storage, il sistema StorageGRID dovrebbe avviarsi automaticamente utilizzando i nuovi nodi di storage. È necessario utilizzare il sistema StorageGRID per verificare che il nuovo nodo di storage sia attivo.

Fasi

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Selezionare **NODES** > ***Expansion Storage Node*** > **Storage**.
3. Posizionare il cursore sul grafico **Storage Used - Object Data** (archiviazione utilizzata - dati oggetto) per visualizzare il valore di **Used**, che corrisponde alla quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
4. Verificare che il valore di **used** aumenti man mano che si sposta il cursore a destra sul grafico.

Copia database nodo amministratore

Quando si aggiungono nodi di amministrazione tramite una procedura di espansione, è possibile copiare il database dal nodo di amministrazione primario al nuovo nodo di amministrazione. La copia del database consente di conservare informazioni cronologiche su attributi, avvisi e avvisi.

Prima di iniziare

- Sono state completate le fasi di espansione richieste per aggiungere un nodo di amministrazione.
- Hai il `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

Il processo di attivazione del software StorageGRID crea un database vuoto per il servizio NMS sul nodo di amministrazione dell'espansione. Quando il servizio NMS viene avviato nel nodo di amministrazione dell'espansione, registra le informazioni relative ai server e ai servizi che fanno parte del sistema o che vengono aggiunti in seguito. Questo database del nodo di amministrazione include le seguenti informazioni:

- Cronologia degli avvisi
- Cronologia degli allarmi
- Dati storici degli attributi, utilizzati nei grafici e nei report di testo disponibili nella pagina **SUPPORTO** > **Strumenti** > **topologia griglia**

Per garantire che il database Admin Node sia coerente tra i nodi, è possibile copiare il database dal nodo Admin primario al nodo Admin di espansione.

> La copia del database dal nodo di amministrazione principale (il nodo di amministrazione___ di origine) a un nodo di amministrazione di espansione può richiedere fino a diverse ore per il completamento. Durante questo periodo, il Grid Manager non è accessibile.

Prima di copiare il database, attenersi alla procedura descritta di seguito per arrestare il servizio MI e il servizio API di gestione sul nodo di amministrazione primario e sul nodo di amministrazione dell'espansione.

Fasi

1. Completare i seguenti passaggi sul nodo di amministrazione principale:
   a. Accedere al nodo di amministrazione:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file.
   b. Eseguire il seguente comando: `recover-access-points`
   c. Inserire la passphrase di provisioning.
   d. Arrestare il servizio MI: `service mi stop`
   e. Arrestare il servizio Management Application Program Interface (mgmt-api): `service mgmt-api stop`
2. Completare i seguenti passaggi sul nodo di amministrazione dell'espansione:
   a. Accedere al nodo di amministrazione dell'espansione:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file.

b. Arrestare il servizio MI: `service mi stop`

c. Arrestare il servizio mgmt-api: `service mgmt-api stop`

d. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`

e. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

f. Copiare il database dal nodo Admin di origine al nodo Admin di espansione: `/usr/local/mi/bin/mi-clone-db.sh` *`Source_Admin_Node_IP`*

g. Quando richiesto, confermare che si desidera sovrascrivere il database MI nel nodo di amministrazione dell'espansione.

   Il database e i relativi dati storici vengono copiati nel nodo di amministrazione dell'espansione. Al termine dell'operazione di copia, lo script avvia l'espansione Admin Node.

h. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`

3. Riavviare i servizi sul nodo di amministrazione primario: `service servermanager start`

Copia le metriche Prometheus

Dopo aver aggiunto un nuovo nodo di amministrazione, è possibile copiare facoltativamente le metriche storiche gestite da Prometheus dal nodo di amministrazione primario al nuovo nodo di amministrazione. La copia delle metriche garantisce che le metriche storiche siano coerenti tra i nodi di amministrazione.

Prima di iniziare

- Il nuovo nodo di amministrazione è installato e in esecuzione.
- Hai il `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

Quando si aggiunge un nodo di amministrazione, il processo di installazione del software crea un nuovo database Prometheus. È possibile mantenere costanti le metriche storiche tra i nodi copiando il database Prometheus dal nodo di amministrazione primario (il *nodo di amministrazione di origine*) al nuovo nodo di amministrazione.

> La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:

   a. Immettere il seguente comando: `ssh admin@`*`grid_node_IP`*

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

2. Dal nodo Admin di origine, arrestare il servizio Prometheus: `service prometheus stop`
3. Completare i seguenti passaggi sul nuovo nodo di amministrazione:
   a. Accedere al nuovo nodo di amministrazione:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file.
   b. Interrompere il servizio Prometheus: `service prometheus stop`
   c. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`
   d. Inserire la password di accesso SSH elencata in `Passwords.txt` file.
   e. Copiare il database Prometheus dal nodo Admin di origine al nuovo nodo Admin: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. Quando richiesto, premere **Invio** per confermare che si desidera distruggere il nuovo database Prometheus nel nuovo nodo di amministrazione.

      Il database Prometheus originale e i relativi dati storici vengono copiati nel nuovo nodo di amministrazione. Al termine dell'operazione di copia, lo script avvia il nuovo nodo di amministrazione. Viene visualizzato il seguente stato:

```
Database cloned, starting services
```

   a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:

```
ssh-add -D
```

4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.

```
service prometheus start
```

Copia dei registri di audit

Quando si aggiunge un nuovo nodo amministratore mediante una procedura di espansione, il servizio AMS registra solo gli eventi e le azioni che si verificano dopo l'accesso al sistema. Se necessario, è possibile copiare i registri di controllo da un nodo amministratore precedentemente installato nel nuovo nodo amministratore di espansione in modo che sia sincronizzato con il resto del sistema StorageGRID.

Prima di iniziare

- Sono state completate le fasi di espansione richieste per aggiungere un nodo di amministrazione.
- Hai il `Passwords.txt` file.

A proposito di questa attività

Per rendere disponibili i messaggi di audit storici su un nuovo nodo di amministrazione, è necessario copiare

manualmente i file di log di audit da un nodo di amministrazione esistente al nodo di amministrazione dell'espansione.

> Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile saltare questi passaggi se si verifica una delle seguenti condizioni:
>
> - È stato configurato un server syslog esterno e i registri di controllo vengono inviati al server syslog invece che ai nodi di amministrazione.
> - È stato specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.
>
> Vedere "Configurare i messaggi di audit e le destinazioni dei log" per ulteriori informazioni.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@_primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
2. Arrestare il servizio AMS per impedire la creazione di un nuovo file: `service ams stop`
3. Accedere alla directory di esportazione della verifica:

   ```
   cd /var/local/log
   ```
4. Rinominare l'origine `audit.log` File per assicurarsi che non sovrascriva il file sul nodo di amministrazione dell'espansione in cui si sta copiando:

   ```
   ls -l
   mv audit.log _new_name_.txt
   ```
5. Copiare tutti i file di registro di controllo nella posizione di destinazione sul nodo di amministrazione di espansione:

   ```
   scp -p * IP_address:/var/local/log
   ```
6. Se viene richiesta la passphrase per `/root/.ssh/id_rsa`, Immettere la password di accesso SSH per il nodo di amministrazione principale elencato in `Passwords.txt` file.
7. Ripristinare l'originale `audit.log` file:

   ```
   mv new_name.txt audit.log
   ```
8. Avviare il servizio AMS:

```
service ams start
```

9. Disconnettersi dal server:

```
exit
```

10. Accedere al nodo di amministrazione dell'espansione:
    a. Immettere il seguente comando: `ssh admin@expansion_Admin_Node_IP`
    b. Immettere la password elencata in `Passwords.txt` file.
    c. Immettere il seguente comando per passare a root: `su -`
    d. Immettere la password elencata in `Passwords.txt` file.

    Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

11. Aggiornare le impostazioni dell'utente e del gruppo per i file di log di controllo:

```
cd /var/local/log

chown ams-user:bycast *
```

12. Disconnettersi dal server:

```
exit
```

Ribilanciare i dati con codifica di cancellazione dopo l'aggiunta di nodi di storage

Dopo aver aggiunto i nodi di storage, è possibile utilizzare la procedura di ribilanciamento EC per ridistribuire i frammenti con codifica di erasure tra i nodi di storage esistenti e nuovi.

Prima di iniziare

- Sono state completate le fasi di espansione per aggiungere i nuovi nodi di storage.
- Hai esaminato il "considerazioni per il ribilanciamento dei dati con codifica erasure".
- Si comprende che i dati degli oggetti replicati non verranno spostati da questa procedura e che la procedura di ribilanciamento EC non prende in considerazione l'utilizzo dei dati replicati su ciascun nodo di storage quando si determina dove spostare i dati con codifica di cancellazione.
- Hai il `Passwords.txt` file.

Cosa succede quando viene eseguita questa procedura

Prima di iniziare la procedura, prendere nota di quanto segue:

- La procedura di ribilanciamento EC non si avvia se uno o più volumi sono offline (non montati) o se sono online (montati) ma in uno stato di errore.
- La procedura di ribilanciamento EC riserva temporaneamente una grande quantità di storage. Gli avvisi relativi allo storage potrebbero essere attivati, ma verranno risolti al termine del ribilanciamento. Se lo storage non è sufficiente per la prenotazione, la procedura di ribilanciamento EC non avrà esito positivo. Le riserve di storage vengono rilasciate al termine della procedura di ribilanciamento EC, indipendentemente dal fatto che la procedura abbia avuto esito negativo o positivo.

- Se un volume non è in linea mentre è in corso la procedura di riequilibrio EC, la procedura di riequilibrio terminerà. Tutti i frammenti di dati che sono stati già spostati rimarranno nelle nuove posizioni e i dati non andranno persi.

  È possibile eseguire nuovamente la procedura dopo che tutti i volumi sono stati nuovamente online.

- Quando la procedura di ribilanciamento EC è in esecuzione, le prestazioni delle operazioni ILM e delle operazioni dei client S3 e Swift potrebbero risentire.

  > Le operazioni delle API S3 e Swift per caricare oggetti (o parti di oggetti) potrebbero non riuscire durante la procedura di ribilanciamento EC se richiedono più di 24 ore per il completamento. Le operazioni PUT di lunga durata non avranno esito positivo se la regola ILM applicabile utilizza un posizionamento bilanciato o rigoroso all'acquisizione. Viene segnalato il seguente errore: `500 Internal Server Error`.

- Durante questa procedura, tutti i nodi hanno un limite di capacità storage del 80%. I nodi che superano questo limite, ma che rimangono al di sotto della partizione dei dati di destinazione, sono esclusi da:
  - Il valore di squilibrio del sito
  - Qualsiasi condizione di completamento del lavoro

  > La partizione dei dati di destinazione viene calcolata dividendo i dati totali di un sito per il numero di nodi.

- **Condizioni di completamento del lavoro**. Il "Procedura di riequilibrio CE" è considerato completo quando si verifica una delle seguenti condizioni:
  - Impossibile spostare altri dati sottoposti a erasure coding.
  - I dati in tutti i nodi rientrano in una deviazione del 5% della partizione dei dati di destinazione.
  - La procedura è in corso da 30 giorni.

Fasi

1. Rivedi i dettagli dello storage a oggetti corrente per il sito che intendi ribilanciare.
   a. Selezionare **NODI**.
   b. Selezionare il primo nodo di storage nel sito.
   c. Selezionare la scheda **Storage**.
   d. Posizionare il cursore sul grafico Storage Used - Object Data (Storage utilizzato - dati oggetto) per visualizzare la quantità corrente di dati replicati e i dati con codifica di cancellazione sul nodo di storage.
   e. Ripetere questa procedura per visualizzare gli altri nodi di storage del sito.
2. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

3. Avviare la procedura:

   `rebalance-data start --site "*site-name*"

   Per "*site-name*", specificare il primo sito in cui sono stati aggiunti nuovi nodi di archiviazione. Racchiudere `site-name` tra virgolette.

   Viene avviata la procedura di ribilanciamento EC e viene restituito un ID lavoro.

4. Copiare l'ID lavoro.
5. monitorare lo stato della procedura di riequilibrio CE.

   - Per visualizzare lo stato di una singola procedura di ribilanciamento EC:

     `rebalance-data status --job-id *job-id*`

     Per *`job-id`*, Specificare l'ID restituito all'avvio della procedura.

   - Per visualizzare lo stato della procedura di ribilanciamento EC corrente e delle procedure precedentemente completate:

     `rebalance-data status`

   > Per ottenere assistenza sul comando ribilanciamento-dati:
   >
   > `rebalance-data --help`

6. Eseguire ulteriori operazioni in base allo stato restituito:

   - Se `State` è `In progress`, L'operazione di ribilanciamento EC è ancora in esecuzione. È necessario monitorare periodicamente la procedura fino al completamento.

     Utilizzare `Site Imbalance` Valore per valutare l'utilizzo non bilanciato dei dati dell'erasure coding nei nodi storage del sito. Questo valore può essere compreso tra 1,0 e 0, con 0 che indica che l'utilizzo dei dati con erasure coding è completamente bilanciato in tutti i nodi storage del sito.

   Il processo di riequilibrio EC è considerato completo e si interrompe quando i dati in tutti i nodi rientrano in una deviazione del 5% della partizione dei dati di destinazione.

   - Se `State` è `Success`, facoltativamente esaminare lo storage a oggetti per visualizzare i dettagli aggiornati del sito.

     I dati con codifica erasure dovrebbero ora essere più bilanciati tra i nodi di storage del sito.

   - Se `State` è `Failure`:

     i. Verificare che tutti i nodi di storage del sito siano connessi alla rete.

     ii. Controllare e risolvere eventuali avvisi che potrebbero influire su questi nodi di storage.

     iii. Riavviare la procedura di ribilanciamento EC:

     `rebalance-data start --job-id *job-id*`

     iv. Visualizzare lo stato della nuova procedura. Se `State` è fermo `Failure`, contattare il supporto

tecnico.

7. Se la procedura di ribilanciamento EC genera un carico eccessivo (ad esempio, le operazioni di acquisizione sono interessate), sospendere la procedura.

   `rebalance-data pause --job-id job-id`

8. Se è necessario terminare la procedura di ribilanciamento EC (ad esempio, in modo da poter eseguire un aggiornamento del software StorageGRID), immettere quanto segue:

   `rebalance-data terminate --job-id job-id`

   > Quando si termina una procedura di riequilibrio EC, tutti i frammenti di dati che sono già stati spostati rimangono nelle nuove posizioni. I dati non vengono spostati di nuovo nella posizione originale.

9. Se si utilizza la codifica erasure in più siti, eseguire questa procedura per tutti gli altri siti interessati.

Risolvere i problemi di espansione

Se si verificano errori durante il processo di espansione della griglia che non è possibile risolvere o se un'operazione della griglia non riesce, raccogliere i file di registro e contattare il supporto tecnico.

Prima di contattare il supporto tecnico, raccogliere i file di registro necessari per agevolare la risoluzione dei problemi.

Fasi

1. Connettersi al nodo di espansione che ha riscontrato errori:

   a. Immettere il seguente comando:`ssh -p 8022 admin@grid_node_IP`

      > La porta 8022 è la porta SSH del sistema operativo di base, mentre la porta 22 è la porta SSH del motore dei container che esegue StorageGRID.

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Dopo aver effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. A seconda della fase di installazione raggiunta, recuperare uno dei seguenti log disponibili nel nodo grid:

Piattaforma	Registri
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`

Piattaforma	Registri
Linux	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf` (per ogni nodo guasto) • `/var/log/storagegrid/nodes/<node-name>.log` (per ogni nodo guasto; potrebbe non esistere)

Gestire un sistema StorageGRID

Manutenzione della griglia: Panoramica

Le attività di manutenzione della rete includono il decommissioning di un nodo o sito, la ridenominazione di una griglia, di un nodo o di un sito e la manutenzione delle reti. È inoltre possibile eseguire procedure host e middleware e procedure dei nodi di rete.

> In queste istruzioni, "Linux" si riferisce a una distribuzione di Red Hat® Enterprise Linux®, Ubuntu® o Debian®. Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Prima di iniziare

- Hai una vasta conoscenza del sistema StorageGRID.
- Hai esaminato la topologia del sistema StorageGRID e hai compreso la configurazione della griglia.
- Si comprende che è necessario seguire tutte le istruzioni con precisione e prestare attenzione a tutte le avvertenze.
- Comprendete che le procedure di manutenzione non descritte non sono supportate o richiedono un intervento di assistenza.

Procedure di manutenzione per le appliance

Per le procedure hardware, vedere "Istruzioni di manutenzione per l'apparecchio StorageGRID".

Scarica Recovery Package

Il file del pacchetto di ripristino consente di ripristinare il sistema StorageGRID in caso di errore.

Prima di iniziare

- Dal nodo di amministrazione principale, si è connessi a Grid Manager utilizzando un "browser web supportato".
- Si dispone della passphrase di provisioning.
- Lo hai fatto "autorizzazioni di accesso specifiche".

Scaricare il file del pacchetto di ripristino corrente prima di apportare modifiche alla topologia della griglia al sistema StorageGRID o prima di aggiornare il software. Quindi, scaricare una nuova copia del pacchetto di ripristino dopo aver apportato modifiche alla topologia della griglia o dopo aver aggiornato il software.

Fasi

1. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.
2. Immettere la passphrase di provisioning e selezionare **Avvia download**.

   Il download viene avviato immediatamente.

3. Al termine del download, aprire `.zip` archiviare e confermare che è possibile accedere ai contenuti,

incluso il `Passwords.txt` file.

4. Copiare il file del pacchetto di ripristino scaricato (`.zip`) in due posizioni 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.

Decommissiona i nodi o il sito

Procedura di decommissionamento: Panoramica

È possibile eseguire una procedura di decommissionamento per rimuovere in modo permanente i nodi della griglia o un intero sito dal sistema StorageGRID.

Per rimuovere un nodo della griglia o un sito, eseguire una delle seguenti procedure di decommissionamento:

- Eseguire una "decommissionare il nodo di rete" per rimuovere uno o più nodi, che possono trovarsi in uno o più siti. I nodi rimossi possono essere online e connessi al sistema StorageGRID oppure offline e disconnessi.
- Eseguire una "decommissionare il sito" per rimuovere un sito. Se tutti i nodi sono connessi a StorageGRID, viene eseguita la **decommissionazione del sito connesso**. Se tutti i nodi sono disconnessi da StorageGRID, viene eseguita una **decommissionazione sito disconnessa**. Se il sito contiene una combinazione di nodi connessi e disconnessi, è necessario riportare tutti i nodi offline in linea.

> Prima di eseguire un decommissionamento del sito disconnesso, contatta il tuo rappresentante NetApp. NetApp esaminerà i tuoi requisiti prima di attivare tutte le fasi della procedura guidata Decommission Site. Non tentare di decommissionare un sito disconnesso se si ritiene possibile ripristinare il sito o i dati degli oggetti dal sito.

Decommissionamento dei nodi

Decommissionare il nodo Grid: Panoramica

È possibile utilizzare la procedura di decommissionamento dei nodi per rimuovere uno o più nodi della griglia in uno o più siti. Impossibile decommissionare il nodo di amministrazione primario.

Quando decommissionare un nodo

Utilizzare la procedura di decommissionamento del nodo quando si verifica una delle seguenti condizioni:

- È stato aggiunto un nodo di archiviazione più grande in un'espansione e si desidera rimuovere uno o più nodi di archiviazione più piccoli, conservando al tempo stesso gli oggetti.

> Se si desidera sostituire un'appliance precedente con un'appliance più recente, prendere in considerazione l'opzione "clonare il nodo appliance" invece di aggiungere un nuovo apparecchio in un'espansione e quindi di smantellare il vecchio apparecchio.

- Richiede meno storage totale.

- Non è più necessario un nodo gateway.
- Non è più necessario un nodo di amministrazione non primario.
- La griglia include un nodo disconnesso che non è possibile ripristinare o ripristinare online.
- La griglia include un nodo di archiviazione.

Come decommissionare un nodo

È possibile dismettere nodi di rete connessi o nodi di rete disconnessi.

Decommissiona i nodi connessi

In generale, è necessario disattivare i nodi della griglia solo quando sono connessi al sistema StorageGRID e solo quando tutti i nodi sono in condizioni normali (le icone verdi sono presenti nelle pagine **NODI** e nella pagina **nodi di decompressione**).

Per istruzioni, vedere "Decommissionare i nodi di rete connessi".

Decommissiona i nodi disconnessi

In alcuni casi, potrebbe essere necessario smantellare un nodo di rete che non è attualmente connesso alla rete (uno il cui stato è sconosciuto o amministrativamente inattivo). Ad esempio, è possibile decommissionare un nodo di archivio solo se è disconnesso.

Per istruzioni, vedere "Decommissionare nodi di rete disconnessi".

Cosa considerare prima del decommissionamento di un nodo

Prima di eseguire una delle due procedure, esaminare le considerazioni relative a ciascun tipo di nodo:

- "Considerazioni per Admin, Gateway o Archive Node decommissioning"
- "Considerazioni per la decommissionazione del nodo di storage"

Considerazioni sulla disattivazione dei nodi Admin, Gateway o Archive

Esaminare le considerazioni relative allo smantellamento di un nodo amministrativo, di un nodo gateway o di un nodo archivio.

Considerazioni sul nodo amministrativo

- Impossibile decommissionare il nodo di amministrazione primario.
- Non è possibile decommissionare un nodo amministrativo se una delle sue interfacce di rete fa parte di un gruppo ad alta disponibilità (ha). Rimuovere prima le interfacce di rete dal gruppo ha. Consultare le istruzioni per "Gestione dei gruppi ha".
- Se necessario, è possibile modificare in modo sicuro i criteri ILM durante il decommissioning di un nodo amministrativo.
- Se si decommissiona un nodo amministratore e si attiva l'accesso singolo (SSO) per il sistema StorageGRID, è necessario ricordare di rimuovere l'attendibilità della parte di base del nodo dai servizi di federazione di Active Directory (ad FS).
- Se si utilizza "federazione di grid", Assicurarsi che l'indirizzo IP del nodo che si sta smantellando non sia stato specificato per una connessione a federazione di griglia.
- Quando si decommissiona un nodo di amministrazione disconnesso, i registri di controllo andranno persi da quel nodo; tuttavia, questi registri dovrebbero esistere anche nel nodo di amministrazione primario.

Considerazioni per il nodo gateway

- Non è possibile decommissionare un nodo gateway se una delle sue interfacce di rete fa parte di un gruppo ad alta disponibilità (ha). Rimuovere prima le interfacce di rete dal gruppo ha. Consultare le istruzioni per "Gestione dei gruppi ha".
- Se necessario, è possibile modificare in modo sicuro i criteri ILM durante il decommissionamento di un nodo gateway.
- Se si utilizza "federazione di grid", Assicurarsi che l'indirizzo IP del nodo che si sta smantellando non sia stato specificato per una connessione a federazione di griglia.
- È possibile decommissionare in modo sicuro un nodo gateway mentre è disconnesso.

considerazioni sul nodo di archiviazione

> Il supporto per i nodi di archivio e l'opzione Cloud Tiering - Simple Storage Service (S3) è stato obsoleto. Il supporto del nodo di archivio verrà rimosso completamente in una versione futura.

- Non è possibile smantellare un nodo di archivio se è ancora connesso alla rete. Per rimuovere un nodo di archivio, verificare che il nodo non sia più utilizzato, che i dati siano stati migrati in una posizione diversa e che il nodo sia spento. Quindi, utilizzare la procedura di decommissionamento per i nodi disconnessi.
- Se il nodo di archivio è ancora in uso, assicurarsi che la pianificazione includa un tempo sufficiente per spostare i dati esistenti nei nodi di storage o in un pool di archiviazione cloud. Lo spostamento dei dati da un nodo di archiviazione può richiedere diversi giorni o settimane.

Fasi

1. Se si sta utilizzando un nodo di archiviazione con l'opzione Cloud Tiering - Simple Storage Service (S3), "Migrare gli oggetti in un pool di storage cloud".
2. Verificare che il nodo di archiviazione non sia più utilizzato da nessuna regola ILM nei criteri ILM attivi.
   a. Andare alla pagina **ILM** > **Storage Pools**.
   b. Dall'elenco dei pool di archiviazione, selezionare tutti i pool di archiviazione che contengono solo nodi di archiviazione.
   c. Selezionare la scheda **utilizzo ILM**.
   d. Se sono elencate regole ILM, esaminare la colonna **utilizzato nei criteri attivi** per determinare se il pool di archiviazione del nodo di archiviazione viene utilizzato in un criterio attivo.
   e. Se si utilizza il pool di storage, "Creare una nuova policy ILM" Che non utilizza più il nodo di archiviazione.
   f. Attivare la nuova policy.
   g. Attendere che tutti gli oggetti vengano spostati dal pool di archiviazione del nodo di archiviazione. Questa operazione potrebbe richiedere diversi giorni o settimane.
3. Dopo aver verificato che tutti gli oggetti sono stati spostati dal nodo di archiviazione, spegnere il nodo.
4. Eseguire "procedura di decommissionamento per i nodi disconnessi".

Considerazioni sui nodi storage

Considerazioni per la disattivazione dei nodi di storage

Prima del decommissioning di un nodo storage, prendi in considerazione la possibilità di clonare il nodo. Quindi, se si decide di decommissionare il nodo, controlla il modo in cui

StorageGRID gestisce oggetti e metadati durante la procedura di decommissionamento.

Quando clonare un nodo invece di decommissionarlo

Se vuoi sostituire un nodo storage di un'appliance più vecchia con un'appliance più recente o più grande, prendi in considerazione la possibilità di clonare il nodo appliance invece di aggiungere una nuova appliance in un'espansione e poi dismettere la vecchia appliance.

Il cloning dei nodi dell'appliance consente di sostituire facilmente un nodo dell'appliance esistente con un'appliance compatibile nello stesso sito StorageGRID. Il processo di cloning trasferisce tutti i dati nella nuova appliance, mette in funzione la nuova appliance e lascia la vecchia appliance in uno stato preinstallato.

È possibile clonare un nodo appliance se è necessario:

- Sostituite un apparecchio che sta per esaurirsi.
- Aggiorna un nodo esistente per sfruttare la tecnologia di appliance migliorata.
- Aumenta la capacità dello storage grid senza modificare il numero di nodi di storage nel sistema StorageGRID.
- Migliorare l'efficienza dello storage, ad esempio cambiando la modalità RAID.

Vedere "Cloning del nodo dell'appliance: Panoramica" per ulteriori informazioni.

Considerazioni sui nodi di storage connessi

Esaminare le considerazioni per lo smantellamento di un nodo di storage connesso.

- Non è consigliabile decommissionare più di 10 nodi di storage in una singola procedura Decommission Node.
- Il sistema deve sempre includere nodi storage sufficienti per soddisfare i requisiti operativi, tra cui "Quorum ADC" e l'attivo "Policy ILM". Per soddisfare questa restrizione, potrebbe essere necessario aggiungere un nuovo nodo di storage in un'operazione di espansione prima di poter decommissionare un nodo di storage esistente.

  Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

- Quando si rimuove un nodo di storage, grandi volumi di dati di oggetti vengono trasferiti sulla rete. Sebbene questi trasferimenti non debbano influenzare le normali operazioni del sistema, possono influire sulla quantità totale di larghezza di banda della rete consumata dal sistema StorageGRID.
- Le attività associate allo smantellamento del nodo di storage hanno una priorità inferiore rispetto alle attività associate alle normali operazioni di sistema. Ciò significa che lo smantellamento non interferisce con le normali operazioni del sistema StorageGRID e non deve essere pianificato per un periodo di inattività del sistema. Poiché lo smantellamento viene eseguito in background, è difficile stimare il tempo necessario per il completamento del processo. In generale, lo smantellamento termina più rapidamente quando il sistema non funziona correttamente o se viene rimosso un solo nodo di storage alla volta.
- La decommissionazione di un nodo di storage potrebbe richiedere giorni o settimane. Pianificare questa procedura di conseguenza. Sebbene il processo di decommissionamento sia progettato per non influire sulle operazioni del sistema, può limitare altre procedure. In generale, prima di rimuovere i nodi di rete, è necessario eseguire eventuali upgrade o espansioni del sistema pianificati.

- Se è necessario eseguire un'altra procedura di manutenzione durante la rimozione dei nodi di archiviazione, è possibile farlo "sospendere la procedura di decommissionamento" e riprenderlo al termine dell'altra procedura.

> Il pulsante **Pause** (Pausa) viene attivato solo quando vengono raggiunte le fasi di decommissionamento dei dati con codifica di cancellazione o valutazione ILM; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background.

- Non è possibile eseguire operazioni di riparazione dei dati su nodi grid quando è in esecuzione un'attività di decommissionamento.
- Non apportare modifiche a un criterio ILM durante la chiusura di un nodo storage.
- Quando si decommissiona un nodo di archiviazione, è possibile che vengano attivati i seguenti avvisi e allarmi e che si ricevano le relative notifiche via e-mail e SNMP:
  - **Impossibile comunicare con l'avviso Node**. Questo avviso viene attivato quando si decommissiona un nodo di storage che include il servizio ADC. L'avviso viene risolto al termine dell'operazione di decommissionamento.
  - Allarme VSTU (Object Verification Status). Questo allarme a livello di avviso indica che il nodo di storage sta entrando in modalità di manutenzione durante il processo di decommissionamento.
  - Allarme CASA (Data Store Status). Questo allarme di livello maggiore indica che il database Cassandra è in stato di inattività a causa dell'interruzione dei servizi.
- Per rimuovere i dati in modo permanente e sicuro, è necessario cancellare le unità del nodo di archiviazione al termine della procedura di decommissionamento.

Considerazioni sui nodi storage disconnessi

Esaminare le considerazioni per il decommissionamento di un nodo di storage disconnesso.

- Non dismettere mai un nodo disconnesso a meno che non si sia certi che non possa essere messo in linea o ripristinato.

> Non eseguire questa procedura se si ritiene che sia possibile ripristinare i dati dell'oggetto dal nodo. Contattare invece il supporto tecnico per determinare se è possibile eseguire il ripristino del nodo.

- Quando si decommissiona un nodo di storage disconnesso, StorageGRID utilizza i dati provenienti da altri nodi di storage per ricostruire i dati dell'oggetto e i metadati che si trovavano nel nodo disconnesso.
- La perdita di dati può verificarsi se si decommissiona più di un nodo di storage disconnesso. Il sistema potrebbe non essere in grado di ricostruire i dati se non sono disponibili un numero sufficiente di copie di oggetti, frammenti con codifica di cancellazione o metadati di oggetti. Durante il decommissioning dei nodi storage in un grid con nodi solo metadati basati su software, il decommissioning di tutti i nodi configurati per memorizzare sia oggetti che metadati rimuove tutto lo storage a oggetti dal grid. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

> Se si dispone di più nodi di storage disconnessi che non è possibile ripristinare, contattare il supporto tecnico per determinare la procedura migliore.

- Quando si decommissiona un nodo di storage disconnesso, StorageGRID avvia i lavori di riparazione dei dati al termine del processo di decommissionamento. Questi processi tentano di ricostruire i dati dell'oggetto e i metadati memorizzati nel nodo disconnesso.

- Quando si decommissiona un nodo di storage disconnesso, la procedura di decommissionamento viene completata in modo relativamente rapido. Tuttavia, i lavori di riparazione dei dati possono richiedere giorni o settimane e non vengono monitorati dalla procedura di decommissionamento. È necessario monitorare manualmente questi lavori e riavviarli secondo necessità. Vedere "Controllare i lavori di riparazione dei dati".
- Se si decommissiona un nodo di storage disconnesso che contiene l'unica copia di un oggetto, l'oggetto andrà perso. I processi di riparazione dei dati possono ricostruire e ripristinare gli oggetti solo se nei nodi di storage attualmente connessi sono presenti almeno una copia replicata o un numero sufficiente di frammenti con codifica di cancellazione.

Cos'è il quorum ADC?

Potrebbe non essere possibile smantellare alcuni nodi di archiviazione in un sito se dopo lo smantellamento rimanessero pochi servizi ADC (Administrative Domain Controller).

Il servizio ADC, presente in alcuni nodi di archiviazione, mantiene le informazioni sulla topologia della griglia e fornisce servizi di configurazione alla griglia. Il sistema StorageGRID richiede un quorum di servizi ADC per essere sempre disponibile in ogni sito.

Non è possibile decommissionare un nodo di storage se la rimozione del nodo causerebbe il mancato rispetto del quorum di ADC. Per soddisfare il quorum ADC durante una disattivazione, è necessario che almeno tre nodi di archiviazione in ogni sito dispongano del servizio ADC. Se in un sito sono presenti più di tre nodi di archiviazione con il servizio ADC, la maggior parte di questi nodi deve rimanere disponibile dopo lo smantellamento: `((0.5 * Storage Nodes with ADC) + 1)`

> Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

Ad esempio, si supponga che un sito attualmente includa sei nodi di storage con servizi ADC e che si desideri smantellare tre nodi di storage. A causa del requisito di quorum di ADC, è necessario completare due procedure di decommissionamento, come indicato di seguito:

- Nella prima procedura di decommissionamento, è necessario assicurarsi che siano disponibili quattro nodi di storage con servizi ADC: `((0.5 * 6) + 1)`. Ciò significa che all'inizio è possibile decommissionare solo due nodi di storage.
- Nella seconda procedura di decommissionamento, è possibile rimuovere il terzo nodo di storage poiché il quorum ADC ora richiede solo tre servizi ADC per rimanere disponibili: `((0.5 * 4) + 1)`.

Se è necessario smantellare un nodo di archiviazione ma non è possibile farlo a causa del requisito quorum ADC, aggiungere un nuovo nodo di archiviazione in un "espansione" E specificare che deve disporre di un servizio ADC. Quindi, smantellare il nodo di storage esistente.

Esaminare i criteri ILM e la configurazione dello storage

Se si prevede di decommissionare un nodo di storage, è necessario rivedere la policy ILM del sistema StorageGRID prima di avviare il processo di decommissionamento.

Durante lo smantellamento, tutti i dati degli oggetti vengono migrati dal nodo di storage decommissionato ad altri nodi di storage.

La policy ILM di cui disponi *durante* la decommissionazione sarà quella utilizzata *dopo* la decommissionazione. È necessario assicurarsi che questa policy soddisfi i requisiti dei dati prima di iniziare la decommissionazione e dopo il completamento della decommissionazione.

È necessario rivedere le regole in ciascuna di esse "Criterio ILM attivo" Per garantire che il sistema StorageGRID continui a disporre di capacità sufficiente del tipo corretto e nelle posizioni corrette per consentire lo smantellamento di un nodo di archiviazione.

Considerare quanto segue:

- I servizi di valutazione ILM potranno copiare i dati degli oggetti in modo che le regole ILM siano soddisfatte?
- Cosa succede se un sito diventa temporaneamente non disponibile mentre è in corso la disattivazione? È possibile eseguire copie aggiuntive in una posizione alternativa?
- In che modo il processo di disattivazione influirà sulla distribuzione finale dei contenuti? Come descritto in "Consolidare i nodi di storage", è necessario "Aggiungere nuovi nodi di storage" prima di mettere fuori servizio quelli vecchi. Se si aggiunge un nodo di storage sostitutivo più grande dopo la disattivazione di un nodo di storage più piccolo, i vecchi nodi di storage potrebbero essere vicini alla capacità e il nuovo nodo di storage potrebbe non avere quasi alcun contenuto. La maggior parte delle operazioni di scrittura per i nuovi dati a oggetti verrebbe quindi indirizzata al nuovo nodo di storage, riducendo l'efficienza complessiva delle operazioni di sistema.
- Il sistema includerà sempre nodi storage sufficienti per soddisfare le policy ILM attive?

Un criterio ILM che non può essere soddisfatto porterà a backlog e avvisi e potrebbe arrestare il funzionamento del sistema StorageGRID.

Verificare che la topologia proposta risultante dal processo di disattivazione soddisfi la politica ILM valutando le aree elencate nella tabella.

Area da valutare	Che cosa considerare
Capacità disponibile	Ci sarà una capacità storage sufficiente per ospitare tutti i dati a oggetti archiviati nel sistema StorageGRID, incluse le copie permanenti dei dati a oggetti attualmente archiviati nel nodo storage da dismettere? Ci sarà capacità sufficiente per gestire la crescita prevista dei dati degli oggetti memorizzati per un ragionevole intervallo di tempo dopo il completamento del decommissionamento?
Ubicazione dello storage	Se nel sistema StorageGRID rimane una capacità sufficiente, la capacità è nelle posizioni giuste per soddisfare le regole di business del sistema StorageGRID?

Area da valutare	Che cosa considerare
Tipo di storage	Sarà disponibile uno storage sufficiente del tipo appropriato dopo il completamento dello smantellamento? Ad esempio, le regole ILM possono spostare i contenuti da un tipo di storage a un altro in base al tempo in cui i contenuti diventano obsoleti. In questo caso, è necessario assicurarsi che nella configurazione finale del sistema StorageGRID sia disponibile una quantità sufficiente di spazio di archiviazione del tipo appropriato.

Consolidare i nodi di storage

È possibile consolidare i nodi di storage per ridurre il numero di nodi di storage per un sito o un'implementazione, aumentando al contempo la capacità di storage.

Quando si consolidano i nodi storage "Espandere il sistema StorageGRID" Aggiungendo nuovi nodi di storage con capacità maggiore e disattivando i vecchi nodi di storage con capacità minore. Durante la procedura di decommissionamento, gli oggetti vengono migrati dai vecchi nodi di storage ai nuovi nodi di storage.

> Se si consolidano appliance più vecchie e più piccole con nuovi modelli o appliance con capacità maggiore, si consideri "clonare il nodo appliance" (oppure utilizza la clonazione dei nodi di appliance e la procedura di decommissionamento se non stai eseguendo una sostituzione one-to-one).

Ad esempio, è possibile aggiungere due nuovi nodi di storage con capacità maggiore per sostituire tre nodi di storage meno recenti. Prima di tutto, utilizzare la procedura di espansione per aggiungere i due nuovi nodi di storage di dimensioni maggiori, quindi utilizzare la procedura di decommissionamento per rimuovere i tre nodi di storage di capacità inferiore.

Aggiungendo nuova capacità prima di rimuovere i nodi di storage esistenti, è possibile garantire una distribuzione più equilibrata dei dati nel sistema StorageGRID. Inoltre, si riduce la possibilità che un nodo di storage esistente venga spinto oltre il livello di filigrana dello storage.

Decommissionare più nodi di storage

Se è necessario rimuovere più di un nodo di storage, è possibile decommissionarli in sequenza o in parallelo.

> Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

- Se si decommissionano i nodi di storage in modo sequenziale, è necessario attendere che il primo nodo di storage completi la decommissionamento prima di iniziare a decommissionare il nodo di storage successivo.
- Se i nodi di storage vengono decommissionati in parallelo, i nodi di storage elaborano contemporaneamente le attività di decommissionamento per tutti i nodi di storage da decommissionare. Ciò può causare una situazione in cui tutte le copie permanenti di un file sono contrassegnate come "sola lettura", disattivando temporaneamente l'eliminazione nelle griglie in cui questa funzionalità è attivata.

Controllare i lavori di riparazione dei dati

Prima di disattivare un nodo di rete, è necessario confermare che non sono attivi lavori di riparazione dei dati. Se le riparazioni non sono riuscite, è necessario riavviarle e lasciarle completare prima di eseguire la procedura di decommissionamento.

A proposito di questa attività

Se è necessario decommissionare un nodo di storage disconnesso, completare questi passaggi anche al termine della procedura di decommissionamento per garantire che il lavoro di riparazione dei dati sia stato completato correttamente. È necessario assicurarsi che tutti i frammenti erasure-coded presenti nel nodo rimosso siano stati ripristinati correttamente.

Questi passaggi si applicano solo ai sistemi che dispongono di oggetti con codifica per la cancellazione.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@`*`grid_node_IP`*
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Verificare la presenza di riparazioni in corso: `repair-data show-ec-repair-status`
   - Se non si è mai eseguito un lavoro di riparazione dei dati, l'output è `No job found`. Non è necessario riavviare alcun lavoro di riparazione.
   - Se il lavoro di riparazione dei dati è stato eseguito in precedenza o è in esecuzione, l'output elenca le informazioni per la riparazione. Ogni riparazione ha un ID di riparazione univoco.

```
root@ADM1-0:~ # repair-data show-ec-repair-status
            Repair ID    Affected Nodes / Volumes                  Start Time                    End Time       State   Estimated Bytes Affected   Bytes Repaired   Percentage
==================================================================================================================================================================================
   4216507958013005550   DC1-S1-0-182 (Volumes: 2)   2022-08-17T21:37:30.051543   2022-08-17T21:37:37.320998   Completed                 1015788876                0             0
  18214680851049518682   DC1-S1-0-182 (Volumes: 1)   2022-08-17T20:37:58.869362   2022-08-17T20:38:45.299688   Completed                          0                0           100
   7962734388032289010   DC1-S1-0-182 (Volumes: 0)   2022-08-17T20:42:29.578740                                 Stopped                                                   Unknown
```

> In alternativa, è possibile utilizzare Grid Manager per monitorare i processi di ripristino in corso e visualizzare una cronologia di ripristino. Vedere "Ripristinare i dati degli oggetti utilizzando Grid Manager".

3. Se lo stato per tutte le riparazioni è `Completed`, non è necessario riavviare alcun lavoro di riparazione.
4. Se lo stato per qualsiasi riparazione è `Stopped`, è necessario riavviare la riparazione.
   a. Ottenere l'ID della riparazione per la riparazione non riuscita dall'output.
   b. Eseguire `repair-data start-ec-node-repair` comando.

      Utilizzare `--repair-id` Opzione per specificare l'ID riparazione. Ad esempio, se si desidera riprovare una riparazione con l'ID riparazione 949292, eseguire questo comando: `repair-data start-ec-node-repair --repair-id 949292`

   c. Continuare a tenere traccia dello stato delle riparazioni dei dati EC fino a quando lo stato di tutte le

riparazioni non è `Completed`.

Raccogliere il materiale necessario

Prima di eseguire la decommissionazione di un nodo di rete, è necessario ottenere le seguenti informazioni.

Elemento	Note
Pacchetto di ripristino `.zip` file	È necessario "Scarica il pacchetto di ripristino più recente" `.zip` file (`sgws-recovery-package-id-revision.zip`). È possibile utilizzare il file Recovery Package per ripristinare il sistema in caso di errore.
`Passwords.txt` file	Questo file contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando ed è incluso nel pacchetto di ripristino.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non si trova in `Passwords.txt` file.
Descrizione della topologia del sistema StorageGRID prima dello smantellamento	Se disponibile, procurarsi la documentazione che descrive la topologia corrente del sistema.

Informazioni correlate

"Requisiti del browser Web"

Accedere alla pagina nodi di smantellamento

Quando si accede alla pagina nodi di disattivazione in Grid Manager, è possibile visualizzare a colpo d'occhio i nodi che possono essere disattivati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".

> Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

Fasi

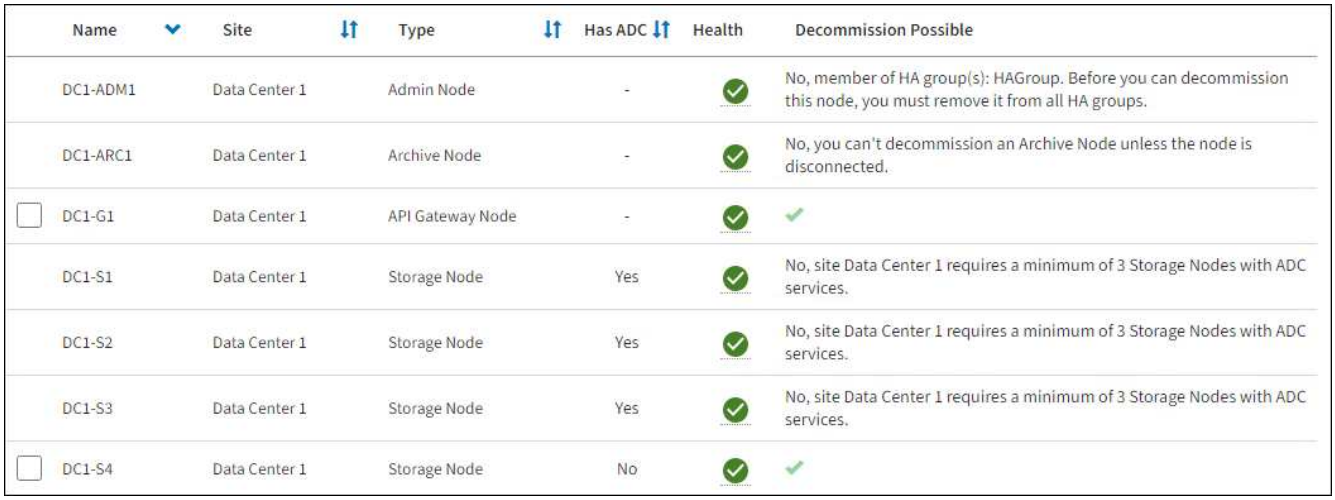
1. Selezionare **MANUTENZIONE** > **attività** > **Smantella**.
2. Selezionare **nodi di decommissionazione**.

   Viene visualizzata la pagina nodi di decommissionazione. Da questa pagina è possibile:

   - Determinare quali nodi di rete possono essere attualmente dismessi.

- Scopri lo stato di salute di tutti i nodi della griglia
- Ordinare l'elenco in ordine crescente o decrescente per **Nome**, **Sito**, **tipo** o **con ADC**.
- Inserisci i termini di ricerca per trovare rapidamente nodi specifici.

  In questo esempio, la colonna Decommission possible (Decommission possibile) indica che è possibile decommissionare il nodo gateway e uno dei quattro nodi di archiviazione.



Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-		No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-ARC1	Data Center 1	Archive Node	-		No, you can't decommission an Archive Node unless the node is disconnected.
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.
DC1-S4	Data Center 1	Storage Node	No		✓

3. Esaminare la colonna **Dismissione possibile** per ciascun nodo che si desidera decommissionare.

   Se è possibile disattivare un nodo della griglia, questa colonna include un segno di spunta verde e la colonna di sinistra contiene una casella di controllo. Se un nodo non può essere decommissionato, questa colonna descrive il problema. Se vi sono più motivi per cui un nodo non può essere dismesso, viene visualizzato il motivo più critico.

Motivo possibile della decommissionazione	**Descrizione**	**Procedura da seguire per risolvere il problema**
No, la disattivazione *node type* non è supportata.	Impossibile decommissionare il nodo di amministrazione primario.	Nessuno.
No, almeno un nodo della griglia è scollegato. **Nota:** questo messaggio viene visualizzato solo per i nodi di rete connessi.	Non è possibile decommissionare un nodo di rete connesso se un nodo di rete è scollegato. La colonna **Health** include una di queste icone per i nodi della griglia disconnessi: • (Grigio): Amministrativamente in basso • (Blu): Sconosciuto	È necessario riportare tutti i nodi disconnessi in linea o. "decommissionare tutti i nodi disconnessi" prima di rimuovere un nodo connesso. **Nota**: Se la griglia contiene più nodi disconnessi, il software richiede di disattivarli tutti contemporaneamente, aumentando il rischio di risultati imprevisti.

Motivo possibile della decommissionazione	Descrizione	Procedura da seguire per risolvere il problema
No, uno o più nodi richiesti sono attualmente disconnessi e devono essere ripristinati. **Nota:** questo messaggio viene visualizzato solo per i nodi della griglia disconnessi.	Non è possibile decommissionare un nodo di rete disconnesso se anche uno o più nodi richiesti sono disconnessi (ad esempio, un nodo di storage necessario per il quorum ADC).	a. Esaminare i messaggi Decommission possible per tutti i nodi disconnessi. b. Determinare quali nodi non possono essere dismessi perché sono necessari. ◦ Se lo stato di salute di un nodo richiesto è amministrativamente inattivo, riportare il nodo in linea. ◦ Se l'integrità di un nodo richiesto è sconosciuta, eseguire una procedura di ripristino del nodo per ripristinare il nodo richiesto.
No, membro dei gruppi ha: *Nome gruppo*. Prima di poter decommissionare questo nodo, è necessario rimuoverlo da tutti i gruppi ha.	Non è possibile decommissionare un nodo amministrativo o un nodo gateway se un'interfaccia di nodo appartiene a un gruppo ad alta disponibilità (ha).	Modificare il gruppo ha per rimuovere l'interfaccia del nodo o rimuovere l'intero gruppo ha. Vedere "Configurare i gruppi ad alta disponibilità".
No, il sito *x* richiede un minimo di *n* nodi di storage con servizi ADC.	**Solo nodi di storage.** non è possibile decommissionare un nodo di storage se nel sito rimangono nodi insufficienti per supportare i requisiti di quorum ADC.	Eseguire un'espansione. Aggiungere un nuovo nodo di storage al sito e specificare che deve disporre di un servizio ADC. Vedere le informazioni su "Quorum ADC".

Motivo possibile della decommissionazione	Descrizione	Procedura da seguire per risolvere il problema
No, uno o più profili di erasure coding necessitano di almeno *n* nodi di storage. Se il profilo non viene utilizzato in una regola ILM, è possibile disattivarlo.	**Solo nodi di archiviazione.** non è possibile decommissionare un nodo di archiviazione a meno che non rimangano un numero sufficiente di nodi per i profili di erasure coding esistenti. Ad esempio, se esiste un profilo di erasure coding per l'erasure coding 4+2, devono rimanere almeno 6 nodi storage.	Per ogni profilo di erasure coding interessato, eseguire una delle seguenti operazioni, in base al modo in cui viene utilizzato il profilo: • **Utilizzato nei criteri ILM attivi**: Eseguire un'espansione. Aggiungere un numero sufficiente di nuovi nodi di storage per consentire la cancellazione del codice. Consultare le istruzioni per "espandere la tua griglia". • **Utilizzato in una regola ILM ma non nei criteri ILM attivi**: Modificare o eliminare la regola e quindi disattivare il profilo di erasure coding. • **Non utilizzato in alcuna regola ILM**: Disattivare il profilo di erasure coding. **Nota:** viene visualizzato un messaggio di errore se si tenta di disattivare un profilo di erasure coding e i dati dell'oggetto sono ancora associati al profilo. Potrebbe essere necessario attendere alcune settimane prima di provare di nuovo il processo di disattivazione. Scopri di più "disattivazione di un profilo di erasure coding".
No, non è possibile smantellare un nodo di archiviazione a meno che il nodo non sia disconnesso.	Se un nodo archivio è ancora connesso, non è possibile rimuoverlo.	Completare i passaggi descritti in "Considerazioni per il nodo di archivio" e poi "decommissionare il nodo disconnesso".

Decommissionare nodi di rete disconnessi

Potrebbe essere necessario decommissionare un nodo che non è attualmente connesso alla rete (un nodo il cui stato di salute è sconosciuto o amministrativamente inattivo).

Prima di iniziare

- Comprendete le considerazioni per la disattivazione "Nodi Admin, Gateway e Archive" e le considerazioni

per lo smantellamento "Nodi di storage".

- Sono stati ottenuti tutti gli elementi prerequisiti.
- Hai garantito che non siano attivi lavori di riparazione dei dati. Vedere "Controllare i lavori di riparazione dei dati".
- Hai confermato che il ripristino del nodo di storage non è in corso in nessun punto della griglia. In tal caso, è necessario attendere il completamento di qualsiasi ricostruzione Cassandra eseguita come parte del ripristino. È quindi possibile procedere con lo smantellamento.
- Si è assicurato che non verranno eseguite altre procedure di manutenzione mentre la procedura di decommissionamento del nodo è in esecuzione, a meno che la procedura di decommissionamento del nodo non sia in pausa.
- La colonna **Dismissione possibile** per il nodo o i nodi disconnessi che si desidera decommissionare include un segno di spunta verde.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

È possibile identificare i nodi disconnessi cercando le icone sconosciute (blu) o amministrative (grigie) nella colonna **Health**. Nell'esempio, il nodo di archiviazione denominato DC1-ARC1 è disconnesso.

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1-105-230	Data Center 1	Admin Node	-		No, primary Admin Node decommissioning is not supported.
DC1-ARC1-105-237	Data Center 1	Archive Node	-		✓
DC1-G1-105-231	Data Center 1	API Gateway Node	-		No, at least one grid node is disconnected.

Prima di disattivare qualsiasi nodo disconnesso, tenere presente quanto segue:

- Questa procedura è principalmente destinata alla rimozione di un singolo nodo disconnesso. Se la griglia contiene più nodi disconnessi, il software richiede di decommissionarli tutti contemporaneamente, aumentando il potenziale di risultati imprevisti.

> La perdita di dati può verificarsi se si decommissiona più di un nodo di storage disconnesso alla volta. Vedere "Considerazioni sui nodi storage disconnessi".

> Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

- Se non è possibile rimuovere un nodo disconnesso (ad esempio, un nodo di storage necessario per il quorum ADC), non è possibile rimuovere nessun altro nodo disconnesso.

Fasi

1. A meno che non si stia smantellando un nodo di archiviazione (che deve essere disconnesso), tentare di riportare in linea tutti i nodi di griglia disconnessi o di ripristinarli.

   Vedere "Procedure di ripristino del nodo Grid" per istruzioni.

2. Se non si riesce a ripristinare un nodo di rete disconnesso e si desidera decommissionarlo mentre è disconnesso, selezionare la casella di controllo corrispondente.

Se la griglia contiene più nodi disconnessi, il software richiede di decommissionarli tutti contemporaneamente, aumentando il potenziale di risultati imprevisti.

Prestare attenzione quando si sceglie di decommissionare più di un nodo di rete disconnesso alla volta, soprattutto se si selezionano più nodi di storage disconnessi. Se si dispone di più nodi di storage disconnessi che non è possibile ripristinare, contattare il supporto tecnico per determinare la procedura migliore.

3. Inserire la passphrase di provisioning.

   Il pulsante **Avvia decommissionazione** è attivato.

4. Fare clic su **Avvia decommissionazione**.

   Viene visualizzato un avviso che indica che è stato selezionato un nodo disconnesso e che i dati dell'oggetto andranno persi se il nodo dispone dell'unica copia di un oggetto.

5. Esaminare l'elenco dei nodi e fare clic su **OK**.

   Viene avviata la procedura di decommissionamento e l'avanzamento viene visualizzato per ciascun nodo. Durante la procedura, viene generato un nuovo pacchetto di ripristino contenente la modifica della configurazione della griglia.

6. Non appena il nuovo pacchetto di ripristino sarà disponibile, fare clic sul collegamento o selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino** per accedere alla pagina del pacchetto di ripristino. Quindi, scaricare `.zip` file.

   Consultare le istruzioni per "Download del pacchetto di ripristino".

   Scarica il pacchetto di ripristino il prima possibile per assicurarti di ripristinare la griglia in caso di problemi durante la procedura di decommissionamento.

   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.

7. Monitorare periodicamente la pagina Decommissionare per assicurarsi che tutti i nodi selezionati siano dismessi correttamente.

   I nodi di storage possono richiedere giorni o settimane per la decommissionazione. Una volta completate tutte le attività, viene visualizzato nuovamente l'elenco di selezione dei nodi con un messaggio di esito positivo. Se si decommissiona un nodo di storage disconnesso, un messaggio di informazioni indica che i lavori di riparazione sono stati avviati.

8. Dopo che i nodi si sono spenti automaticamente nell'ambito della procedura di decommissionamento, rimuovere eventuali macchine virtuali o altre risorse rimanenti associate al nodo decommissionato.

   Non eseguire questo passaggio fino a quando i nodi non si sono spenti automaticamente.

9. Se si sta smantellando un nodo di storage, monitorare lo stato dei lavori di riparazione di **dati replicati** e **dati con codifica di cancellazione (EC)** che vengono avviati automaticamente durante il processo di decommissionamento.

Dati replicati

- Per ottenere una percentuale di completamento stimata per la riparazione replicata, aggiungere `show-replicated-repair-status` al comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Per determinare se le riparazioni sono state completate:
  a. Selezionare **NODI** > ***nodo di storage in riparazione*** > **ILM**.
  b. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
  a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
  b. Selezionare ***Grid*** > ***Storage Node in riparazione*** > **LDR** > **Data Store**.
  c. Utilizzare una combinazione dei seguenti attributi per determinare, come possibile, se le riparazioni replicate sono complete.

  > Le incongruenze di Cassandra potrebbero essere presenti e le riparazioni non riuscite non vengono monitorate.

  - **Tentativi di riparazione (XRPA)**: Utilizzare questo attributo per tenere traccia dell'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo superiore al periodo di scansione corrente (fornito dall'attributo **Scan Period — Estimated**), significa che la scansione ILM non ha rilevato oggetti ad alto rischio che devono essere riparati su alcun nodo.

    > Gli oggetti ad alto rischio sono oggetti che rischiano di essere completamente persi. Non sono inclusi oggetti che non soddisfano la configurazione ILM.

  - **Periodo di scansione — stimato (XSCM)**: Utilizzare questo attributo per stimare quando verrà applicata una modifica di policy agli oggetti precedentemente acquisiti. Se l'attributo **riparazioni tentate** non aumenta per un periodo superiore al periodo di scansione corrente, è probabile che vengano eseguite riparazioni replicate. Si noti che il periodo di scansione può cambiare. L'attributo **Scan Period — Estimated (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione del nodo. È possibile eseguire una query nella cronologia degli attributi **Scan Period — Estimated** per la griglia per determinare un intervallo di tempo appropriato.

Dati con erasure coding (EC)

Per monitorare la riparazione dei dati con codifica erasure e riprovare eventuali richieste che potrebbero non essere riuscite:

1. Determinare lo stato delle riparazioni dei dati con codice di cancellazione:
   - Selezionare **SUPPORTO** > **Strumenti** > **metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).

- Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` funzionamento:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilizzare questo comando per elencare tutte le riparazioni:

  ```
  repair-data show-ec-repair-status
  ```

L'output elenca le informazioni, tra cui `repair ID`, per tutte le riparazioni precedentemente e attualmente in esecuzione.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

   Questo comando prova di nuovo una riparazione del nodo non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Questo comando prova di nuovo una riparazione del volume non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Al termine

Non appena i nodi disconnessi sono stati decommissionati e tutti i lavori di riparazione dei dati sono stati completati, è possibile decommissionare qualsiasi nodo di rete connesso secondo necessità.

Quindi, completare questi passaggi dopo aver completato la procedura di decommissionamento:

- Assicurarsi che i dischi del nodo della griglia decommissionata siano puliti. Utilizzare uno strumento o un servizio di cancellazione dei dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dai dischi.
- Se un nodo dell'appliance è stato disattivato e i dati dell'appliance sono stati protetti mediante la crittografia del nodo, utilizzare il programma di installazione dell'appliance StorageGRID per cancellare la configurazione del server di gestione delle chiavi (Cancella KMS). Se si desidera aggiungere l'appliance a un'altra griglia, è necessario cancellare la configurazione KMS. Per istruzioni, vedere "Monitorare la crittografia dei nodi in modalità di manutenzione".

Decommissionare i nodi di rete connessi

È possibile decommissionare e rimuovere in modo permanente i nodi collegati alla rete.

Prima di iniziare

- Comprendete le considerazioni per la disattivazione "Nodi Admin, Gateway e Archive" e le considerazioni per lo smantellamento "Nodi di storage".
- Hai raccolto tutti i materiali necessari.
- Hai garantito che non siano attivi lavori di riparazione dei dati.
- Hai confermato che il ripristino del nodo di storage non è in corso in nessun punto della griglia. In tal caso,

attendere il completamento di qualsiasi ricostruzione Cassandra eseguita come parte del ripristino. È quindi possibile procedere con lo smantellamento.

- Si è assicurato che non verranno eseguite altre procedure di manutenzione mentre la procedura di decommissionamento del nodo è in esecuzione, a meno che la procedura di decommissionamento del nodo non sia in pausa.
- Si dispone della passphrase di provisioning.
- I nodi della griglia sono connessi.
- La colonna **Dismissione possibile** per il nodo o i nodi che si desidera decommissionare include un segno di spunta verde.

> La decommissionazione non si avvia se uno o più volumi sono offline (non montati) o se sono online (montati) ma in uno stato di errore.

> Se uno o più volumi vengono disconnessi mentre è in corso una decommissionazione, il processo di decommissionamento viene completato dopo che questi volumi sono tornati online.

- Tutti i nodi della griglia hanno uno stato di salute normale (verde) . Se nella colonna **Health** viene visualizzata una di queste icone, provare a risolvere il problema:

Icona	Colore	Severità
	Giallo	Avviso
	Arancione chiaro	Minore
	Arancione scuro	Maggiore
	Rosso	Critico

- Se in precedenza è stato dismesso un nodo di storage disconnesso, tutti i lavori di riparazione dei dati sono stati completati correttamente. Vedere "Controllare i lavori di riparazione dei dati".

> Non rimuovere la macchina virtuale o altre risorse di un nodo griglia fino a quando non viene richiesto in questa procedura.

> Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere "Tipi di nodi storage" Per ulteriori informazioni sui nodi di storage solo metadati.

A proposito di questa attività

Quando un nodo viene smantellato, i suoi servizi vengono disattivati e il nodo si arresta automaticamente.

Fasi

1. Nella pagina nodi di decommissionazione, selezionare la casella di controllo per ciascun nodo della griglia che si desidera decommissionare.
2. Inserire la passphrase di provisioning.

   Il pulsante **Avvia decommissionazione** è attivato.

3. Selezionare **Avvia demissione**.
4. Esaminare l'elenco dei nodi nella finestra di dialogo di conferma e selezionare **OK**.

   Viene avviata la procedura di decommissionamento del nodo e viene visualizzato l'avanzamento per ciascun nodo.

   > Non scollegare un nodo di storage dopo l'avvio della procedura di decommissionamento. La modifica dello stato potrebbe causare la mancata copia di alcuni contenuti in altre posizioni.

5. Non appena il nuovo pacchetto di ripristino è disponibile, selezionare il collegamento pacchetto di ripristino nel banner o selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino** per accedere alla pagina pacchetto di ripristino. Quindi, scaricare `.zip` file.

   Vedere "Download del pacchetto di ripristino".

   > Scarica il pacchetto di ripristino il prima possibile per assicurarti di ripristinare la griglia in caso di problemi durante la procedura di decommissionamento.

6. Monitorare periodicamente la pagina nodi di decommissionazione per assicurarsi che tutti i nodi selezionati vengano decommissionati correttamente.

   > I nodi di storage possono richiedere giorni o settimane per la decommissionazione.

   Una volta completate tutte le attività, viene visualizzato nuovamente l'elenco di selezione dei nodi con un messaggio di esito positivo.

Al termine

Completare questi passaggi dopo aver completato la procedura di decommissionamento del nodo:

1. Seguire la fase appropriata per la piattaforma. Ad esempio:
   - **Linux**: Si consiglia di scollegare i volumi ed eliminare i file di configurazione del nodo creati durante l'installazione. Vedere "Installare StorageGRID su Red Hat Enterprise Linux" e. "Installare StorageGRID su Ubuntu o Debian".
   - **VMware**: Potrebbe essere necessario utilizzare l'opzione "Elimina da disco" di vCenter per eliminare la macchina virtuale. Potrebbe essere necessario eliminare anche i dischi dati indipendenti dalla macchina virtuale.
   - **Appliance StorageGRID**: Il nodo appliance torna automaticamente allo stato non distribuito, dove è possibile accedere al programma di installazione dell'appliance StorageGRID. È possibile spegnere l'apparecchio o aggiungerlo a un altro sistema StorageGRID.
2. Assicurarsi che i dischi del nodo della griglia decommissionata siano puliti. Utilizzare uno strumento o un servizio di cancellazione dei dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dai dischi.

3. Se un nodo dell'appliance è stato disattivato e i dati dell'appliance sono stati protetti mediante la crittografia del nodo, utilizzare il programma di installazione dell'appliance StorageGRID per cancellare la configurazione del server di gestione delle chiavi (Cancella KMS). Se si desidera aggiungere l'appliance a un'altra griglia, è necessario cancellare la configurazione KMS. Per istruzioni, vedere "Monitorare la crittografia dei nodi in modalità di manutenzione".

Mettere in pausa e riprendere il processo di decommissionamento per i nodi di storage

Se è necessario eseguire una seconda procedura di manutenzione, è possibile sospendere la procedura di decommissionamento per un nodo di storage durante determinate fasi. Al termine dell'altra procedura, è possibile riprendere la decommissionamento.

> Il pulsante **Pause** (Pausa) viene attivato solo quando vengono raggiunte le fasi di decommissionamento dei dati con codifica di cancellazione o valutazione ILM; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".

Fasi

1. Selezionare **MANUTENZIONE** > **attività** > **Smantella**.

   Viene visualizzata la pagina Decommission.

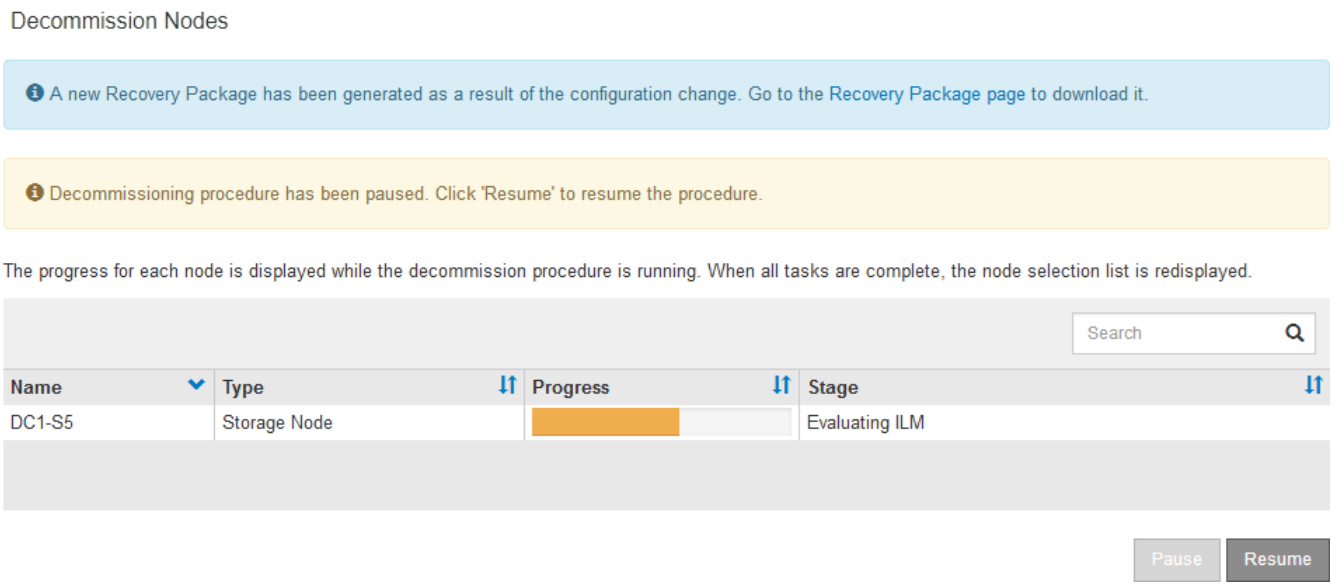
2. Selezionare **nodi di decommissionazione**.

   Viene visualizzata la pagina nodi di decommissionazione. Quando la procedura di decommissionamento raggiunge una delle seguenti fasi, il pulsante **Pause** (Pausa) viene attivato.

   - Valutazione di ILM
   - Decommissionamento dei dati codificati a cancellazione

3. Selezionare **Pausa** per sospendere la procedura.

   La fase corrente viene messa in pausa e il pulsante **Riprendi** viene attivato.



4. Al termine dell'altra procedura di manutenzione, selezionare **Riprendi** per procedere con la decommissionazione.

Risolvere i problemi relativi alla disattivazione del nodo

Se la procedura di decommissionamento del nodo si interrompe a causa di un errore, è possibile eseguire operazioni specifiche per risolvere il problema.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

Se si arresta il nodo della griglia da smantellare, l'attività si interrompe fino al riavvio del nodo della griglia. Il nodo Grid deve essere in linea.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Nell'albero Grid Topology, espandere ogni voce Storage Node e verificare che i servizi DDS e LDR siano entrambi online.

   Per eseguire la disattivazione dei nodi di storage, tutti i nodi e tutti i servizi devono essere integri all'inizio della disattivazione di un nodo/sito online.

3. Per visualizzare le attività attive della griglia, selezionare **nodo amministratore primario** > **CMN** > **attività griglia** > **Panoramica**.
4. Controllare lo stato dell'attività della griglia di disattivazione.

   a. Se lo stato dell'attività griglia di decommissionamento indica un problema con il salvataggio dei pacchetti di attività griglia, selezionare **nodo amministrativo principale** > **CMN** > **Eventi** > **Panoramica**.

   b. Controllare il numero di relè di audit disponibili.

      Se l'attributo Available Audit Relay è uno o più, il servizio CMN è connesso ad almeno un servizio ADC. I servizi ADC fungono da relè di audit.

Il servizio CMN deve essere connesso ad almeno un servizio ADC e la maggior parte (50% più uno) dei servizi ADC del sistema StorageGRID deve essere disponibile per consentire a un'attività Grid di passare da una fase di disattivazione a un'altra e terminare.

a. Se il servizio CMN non è connesso a un numero sufficiente di servizi ADC, assicurarsi che i nodi di storage siano in linea e controllare la connettività di rete tra il nodo di amministrazione primario e i nodi di storage.

Decommissionamento del sito

Considerazioni per la rimozione di un sito

Prima di utilizzare la procedura di decommissionamento del sito per rimuovere un sito, è necessario esaminare le considerazioni.

Cosa accade quando si decommissiona un sito

Quando si decommissiona un sito, StorageGRID rimuove in modo permanente tutti i nodi del sito e del sito stesso dal sistema StorageGRID.

Una volta completata la procedura di decommissionamento del sito:

- Non è più possibile utilizzare StorageGRID per visualizzare o accedere al sito o a uno qualsiasi dei nodi del sito.
- Non puoi più utilizzare pool di storage o profili di erasure coding riferiti al sito. Quando StorageGRID disimpegna un sito, rimuove automaticamente questi pool di storage e disattiva questi profili di erasure coding.

Differenze tra le procedure di decommissionamento del sito connesso e disconnesso

È possibile utilizzare la procedura di decommissionamento del sito per rimuovere un sito in cui tutti i nodi sono connessi a StorageGRID (chiamata decommissionazione di un sito connesso) o per rimuovere un sito in cui tutti i nodi sono disconnessi da StorageGRID (chiamata decommissionazione di un sito disconnesso). Prima di iniziare, è necessario comprendere le differenze tra queste procedure.

> Se un sito contiene una combinazione di) e nodi disconnessi (oppure), è necessario riportare tutti i nodi offline in linea.

- La decommissionazione di un sito connesso consente di rimuovere un sito operativo dal sistema StorageGRID. Ad esempio, è possibile eseguire la decommissionazione di un sito connesso per rimuovere un sito funzionante ma non più necessario.
- Quando StorageGRID rimuove un sito connesso, utilizza ILM per gestire i dati dell'oggetto nel sito. Prima di avviare la decommissionazione di un sito connesso, è necessario rimuovere il sito da tutte le regole ILM e attivare una nuova policy ILM. I processi ILM per la migrazione dei dati degli oggetti e i processi interni per la rimozione di un sito possono essere eseguiti contemporaneamente, ma la procedura consigliata consiste nel consentire il completamento dei passaggi ILM prima di avviare la procedura di decommissionamento effettiva.
- La decommissionazione di un sito disconnesso consente di rimuovere un sito guasto dal sistema StorageGRID. Ad esempio, è possibile eseguire la decommissionazione di un sito disconnesso per rimuovere un sito distrutto da un incendio o un'inondazione.

  Quando StorageGRID rimuove un sito disconnesso, considera tutti i nodi irripristinabili e non tenta di

conservare i dati. Tuttavia, prima di avviare una decommissionazione disconnessa del sito, è necessario rimuovere il sito da tutte le regole ILM e attivare una nuova policy ILM.

> Prima di eseguire una procedura di decommissionamento del sito disconnesso, è necessario contattare il rappresentante commerciale NetApp. NetApp esaminerà i tuoi requisiti prima di attivare tutte le fasi della procedura guidata Decommission Site. Non tentare di decommissionare un sito disconnesso se si ritiene possibile ripristinare il sito o i dati degli oggetti dal sito.

Requisiti generali per la rimozione di un sito connesso o disconnesso

Prima di rimuovere un sito connesso o disconnesso, è necessario conoscere i seguenti requisiti:

- Non è possibile decommissionare un sito che include il nodo di amministrazione primario.
- Impossibile decommissionare un sito che include un nodo di archiviazione.
- Non è possibile decommissionare un sito se uno dei nodi dispone di un'interfaccia che appartiene a un gruppo ad alta disponibilità (ha). È necessario modificare il gruppo ha per rimuovere l'interfaccia del nodo o rimuovere l'intero gruppo ha.
- Non è possibile decommissionare un sito se contiene una combinazione di connesso ( ) e disconnessi (oppure).
- Non è possibile decommissionare un sito se un nodo di un altro sito è disconnesso (oppure).
- Non è possibile avviare la procedura di decommissionamento del sito se è in corso un'operazione di riparazione del nodo ec. Vedere "Controllare i lavori di riparazione dei dati" per tenere traccia delle riparazioni dei dati con codice di cancellazione.
- Durante l'esecuzione della procedura di decommissionamento del sito:
  - Non è possibile creare regole ILM che si riferiscono al sito da smantellare. Inoltre, non è possibile modificare una regola ILM esistente per fare riferimento al sito.
  - Non è possibile eseguire altre procedure di manutenzione, ad esempio l'espansione o l'aggiornamento.

    > Se è necessario eseguire un'altra procedura di manutenzione durante la decommissionazione di un sito connesso, è possibile "Sospendere la procedura durante la rimozione dei nodi di storage". Il pulsante **Pause** (Pausa) viene attivato solo quando vengono raggiunte le fasi di decommissionamento dei dati con codifica di cancellazione o valutazione ILM; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background. Una volta completata la seconda procedura di manutenzione, è possibile riprendere la decommissionamento.

  - Se è necessario ripristinare un nodo dopo aver avviato la procedura di decommissionamento del sito, contattare il supporto.
- Non è possibile decommissionare più di un sito alla volta.
- Se il sito include uno o più nodi di amministrazione ed è abilitato il Single Sign-on (SSO) per il sistema StorageGRID, è necessario rimuovere tutti i trust delle parti che si basano sul sito dai servizi di federazione Active Directory (ad FS).

Requisiti per la gestione del ciclo di vita delle informazioni (ILM)

Durante la rimozione di un sito, è necessario aggiornare la configurazione ILM. La procedura guidata Decommission Site (Sito di rimozione) guida l'utente attraverso una serie di passaggi necessari per garantire quanto segue:

- Il sito non è oggetto di alcuna politica ILM. In tal caso, è necessario modificare i criteri o creare e attivare i criteri con nuove regole ILM.
- Nessuna regola ILM si riferisce al sito, anche se tali regole non sono utilizzate in alcuna politica. È necessario eliminare o modificare tutte le regole che fanno riferimento al sito.

Quando StorageGRID decomprime il sito, disattiva automaticamente tutti i profili di erasure coding inutilizzati che fanno riferimento al sito ed elimina automaticamente eventuali pool di storage inutilizzati che fanno riferimento al sito. Se il pool di storage di tutti i nodi di storage esiste (StorageGRID 11.6 e versioni precedenti), viene rimosso perché utilizza tutti i siti.

> Prima di rimuovere un sito, potrebbe essere necessario creare nuove regole ILM e attivare un nuovo criterio ILM. Queste istruzioni presuppongono una buona comprensione del funzionamento di ILM e la sua conoscenza della creazione di pool di storage, dei profili di erasure coding, delle regole ILM e della simulazione e attivazione di un criterio ILM. Vedere "Gestire gli oggetti con ILM".

Considerazioni per i dati dell'oggetto in un sito connesso

Se si sta eseguendo una decommissionazione del sito connesso, è necessario decidere cosa fare con i dati dell'oggetto esistenti nel sito quando si creano nuove regole ILM e un nuovo criterio ILM. È possibile eseguire una o entrambe le operazioni seguenti:

- Sposta i dati degli oggetti dal sito selezionato a uno o più altri siti della griglia.

  Esempio per lo spostamento dei dati: Supponiamo di voler decommissionare un sito in Raleigh perché hai aggiunto un nuovo sito in Sunnyvale. In questo esempio, si desidera spostare tutti i dati dell'oggetto dal sito precedente al nuovo sito. Prima di aggiornare le regole ILM e i criteri ILM, è necessario esaminare la capacità in entrambi i siti. È necessario assicurarsi che il sito Sunnyvale disponga di capacità sufficiente per ospitare i dati dell'oggetto provenienti dal sito Raleigh e che la capacità di Sunnyvale rimanga adeguata per la crescita futura.

  > Per garantire che sia disponibile una capacità adeguata, potrebbe essere necessario "espandere una griglia" Aggiungendo volumi di storage o nodi di storage a un sito esistente o aggiungendo un nuovo sito prima di eseguire questa procedura.

- Elimina le copie degli oggetti dal sito selezionato.

  Esempio per l'eliminazione dei dati: Si supponga di utilizzare una regola ILM a 3 copie per replicare i dati degli oggetti su tre siti. Prima di smantellare un sito, è possibile creare una regola ILM equivalente a 2 copie per memorizzare i dati solo in due siti. Quando si attiva un nuovo criterio ILM che utilizza la regola 2-copy, StorageGRID elimina le copie dal terzo sito perché non soddisfano più i requisiti ILM. Tuttavia, i dati dell'oggetto rimangono protetti e la capacità dei due siti rimanenti rimane invariata.

Non creare mai una regola ILM a copia singola per consentire la rimozione di un sito. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Requisiti aggiuntivi per la decommissionazione di un sito connesso

Prima che StorageGRID possa rimuovere un sito connesso, è necessario assicurarsi che:

- Tutti i nodi nel sistema StorageGRID devono avere uno stato di connessione di **connesso** ( ); tuttavia, i nodi possono avere avvisi attivi.

  Se uno o più nodi sono disconnessi, è possibile completare i passaggi 1-4 della procedura guidata Smantella sito. Tuttavia, non è possibile completare la fase 5 della procedura guidata, che avvia il processo di decommissionamento, a meno che tutti i nodi non siano connessi.

- Se il sito che si intende rimuovere contiene un nodo gateway o un nodo amministratore utilizzato per il bilanciamento del carico, potrebbe essere necessario "espandere una griglia" per aggiungere un nuovo nodo equivalente in un altro sito. Assicurarsi che i client possano connettersi al nodo sostitutivo prima di avviare la procedura di decommissionamento del sito.
- Se il sito che si intende rimuovere contiene nodi gateway o nodi amministratore che si trovano in un gruppo ad alta disponibilità (ha), è possibile completare i passaggi 1-4 della procedura guidata Decommission Site. Tuttavia, non è possibile completare la fase 5 della procedura guidata, che avvia il processo di decommissionamento, fino a quando non si rimuovono questi nodi da tutti i gruppi ha. Se i client esistenti si connettono a un gruppo ha che include nodi dal sito, è necessario assicurarsi che possano continuare a connettersi a StorageGRID dopo la rimozione del sito.
- Se i client si connettono direttamente ai nodi di storage nel sito che si intende rimuovere, è necessario assicurarsi che possano connettersi ai nodi di storage in altri siti prima di avviare la procedura di decommissionamento del sito.
- È necessario fornire spazio sufficiente sugli altri siti per ospitare i dati degli oggetti che verranno spostati a causa di modifiche a qualsiasi policy ILM attiva. In alcuni casi, potrebbe essere necessario "espandere una griglia" Aggiungendo nodi di storage, volumi di storage o nuovi siti prima di completare la decommissionazione di un sito connesso.
- Per completare la procedura di decommissionamento, è necessario attendere il tempo necessario. I processi ILM di StorageGRID potrebbero richiedere giorni, settimane o persino mesi per spostare o eliminare i dati degli oggetti dal sito prima che il sito possa essere disattivato.

  Lo spostamento o l'eliminazione dei dati degli oggetti da un sito potrebbe richiedere giorni, settimane o persino mesi, a seconda della quantità di dati nel sito, del carico sul sistema, delle latenze di rete e della natura delle modifiche ILM richieste.

- Se possibile, completare i passaggi 1-4 della procedura guidata Decommission Site il prima possibile. La procedura di decommissionamento viene completata più rapidamente e con meno interruzioni e impatti sulle performance se si consente lo spostamento dei dati dal sito prima di avviare la procedura di decommissionamento effettiva (selezionando **Avvia decommissionamento** nella fase 5 della procedura guidata).

Requisiti aggiuntivi per la decommissionazione di un sito disconnesso

Prima che StorageGRID possa rimuovere un sito disconnesso, è necessario assicurarsi che:

- Hai contattato il tuo rappresentante commerciale NetApp. NetApp esaminerà i tuoi requisiti prima di attivare tutte le fasi della procedura guidata Decommission Site.

  > Non tentare di decommissionare un sito disconnesso se si ritiene che sia possibile ripristinare il sito o i dati degli oggetti dal sito. Vedere "Come il supporto tecnico recupera un sito".

- Tutti i nodi del sito devono avere uno stato di connessione di uno dei seguenti:
  - **Sconosciuto** ( ): Per un motivo sconosciuto, un nodo è disconnesso o i servizi sul nodo sono inaspettatamente inattivi. Ad esempio, un servizio sul nodo potrebbe essere stato arrestato o il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione dell'alimentazione o di un'interruzione imprevista.
  - **Amministrativamente inattivo** ( ): Il nodo non è connesso alla rete per un motivo previsto. Ad esempio, il nodo o i servizi sul nodo sono stati normalmente chiusi.
- Tutti i nodi di tutti gli altri siti devono avere uno stato di connessione di **connesso** ( ); tuttavia, questi altri nodi possono avere avvisi attivi.
- È necessario comprendere che non sarà più possibile utilizzare StorageGRID per visualizzare o recuperare i dati degli oggetti memorizzati nel sito. Quando StorageGRID esegue questa procedura, non tenta di conservare i dati del sito disconnesso.

  > Se le regole e i criteri ILM sono stati progettati per proteggere dalla perdita di un singolo sito, le copie degli oggetti rimangono nei siti rimanenti.

- È necessario comprendere che se il sito conteneva l'unica copia di un oggetto, l'oggetto viene perso e non può essere recuperato.

Considerazioni per la coerenza quando si rimuove un sito

La coerenza per un bucket S3 o un container Swift determina se StorageGRID replica completamente i metadati degli oggetti in tutti i nodi e i siti prima di comunicare al client il successo dell'acquisizione degli oggetti. La coerenza fornisce un equilibrio tra la disponibilità degli oggetti e la loro coerenza in diversi nodi e siti storage.

Quando StorageGRID rimuove un sito, deve assicurarsi che non vengano scritti dati sul sito da rimuovere. Di conseguenza, sovrascrive temporaneamente la consistenza per ciascun contenitore o bucket. Dopo aver avviato il processo di decommissionamento del sito, StorageGRID utilizza temporaneamente una forte coerenza del sito per impedire che i metadati degli oggetti vengano scritti nel sito.

Come risultato di questa override temporanea, tenere presente che le operazioni di scrittura, aggiornamento ed eliminazione dei client che si verificano durante la decommissionazione di un sito possono avere esito negativo se più nodi diventano non disponibili negli altri siti.

Raccogliere il materiale necessario

Prima di decommissionare un sito, è necessario procurarsi i seguenti materiali.

Elemento	Note
Pacchetto di ripristino `.zip` file	È necessario scaricare il pacchetto di ripristino più recente `.zip` file (`sgws-recovery-package-id-revision.zip`). È possibile utilizzare il file Recovery Package per ripristinare il sistema in caso di errore. "Scaricare il pacchetto di ripristino"
`Passwords.txt` file	Questo file contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando ed è incluso nel pacchetto di ripristino.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non si trova in `Passwords.txt` file.
Descrizione della topologia del sistema StorageGRID prima dello smantellamento	Se disponibile, procurarsi la documentazione che descrive la topologia corrente del sistema.

Informazioni correlate

"Requisiti del browser Web"

Fase 1: Selezionare Site (Sito)

Per determinare se un sito può essere decommissionato, iniziare accedendo alla procedura guidata Decommissionare il sito.

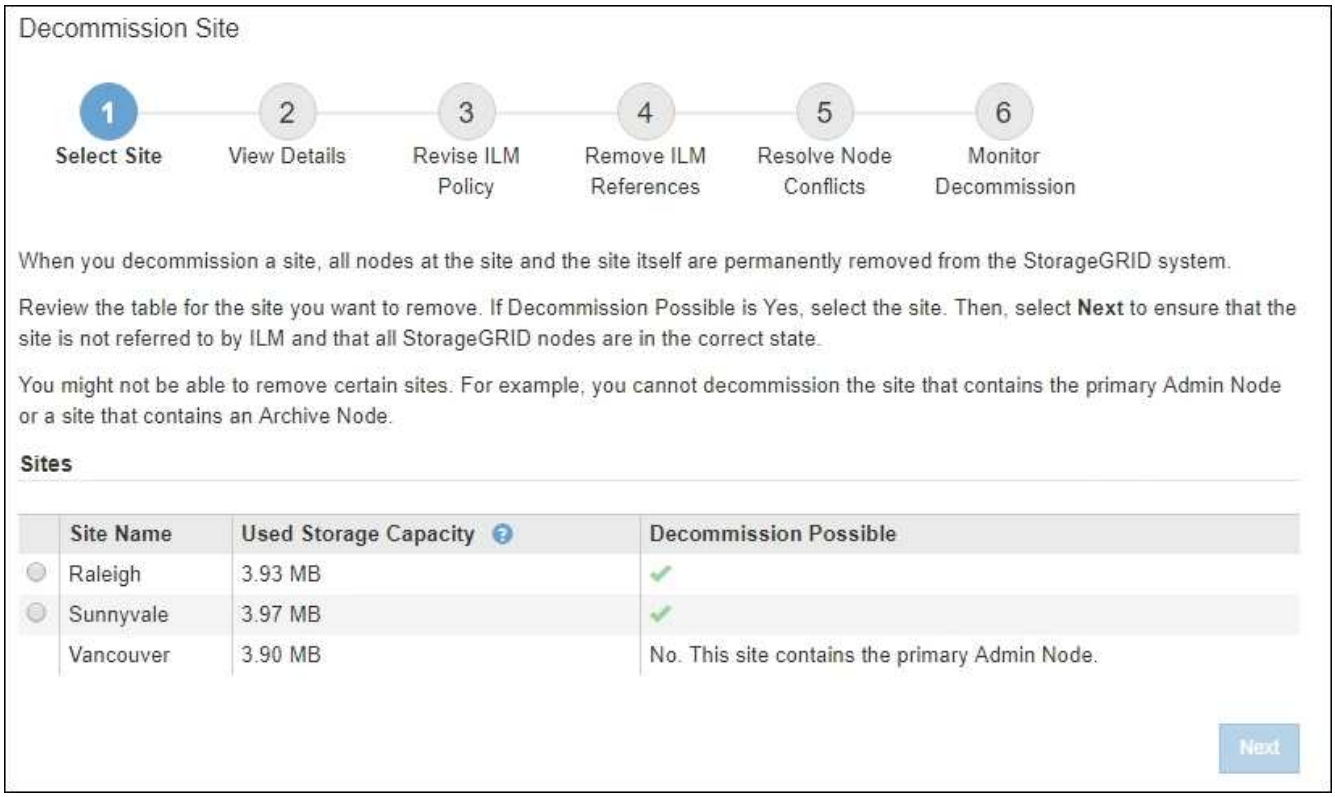
Prima di iniziare

- Hai ottenuto tutti i materiali richiesti.
- Hai esaminato le considerazioni per la rimozione di un sito.
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root o autorizzazioni Maintenance e ILM".

Fasi

1. Selezionare **MANUTENZIONE** > **attività** > **Smantella**.
2. Selezionare **Smantella sito**.

   Viene visualizzata la fase 1 (Seleziona sito) della procedura guidata Smantella sito. Questo passaggio include un elenco alfabetico dei siti nel sistema StorageGRID.



3. Visualizzare i valori nella colonna **capacità di storage utilizzata** per determinare la quantità di storage attualmente utilizzata per i dati a oggetti in ogni sito.

   La capacità di storage utilizzata è una stima. Se i nodi sono offline, la capacità di storage utilizzata è l'ultimo valore noto per il sito.

   - Per la decommissionazione di un sito connesso, questo valore rappresenta la quantità di dati dell'oggetto da spostare in altri siti o da eliminare da ILM prima di poter decommissionare il sito in modo sicuro.
   - Per la decommissionazione di un sito disconnesso, questo valore rappresenta la quantità di storage dei dati del sistema che diventa inaccessibile quando si decommissiona questo sito.

   > ⓘ Se la policy ILM è stata progettata per proteggere dalla perdita di un singolo sito, le copie dei dati dell'oggetto dovrebbero comunque esistere sui siti rimanenti.

4. Esaminare i motivi nella colonna **Smantella possibile** per determinare quali siti possono essere attualmente dismessi.

   > ⓘ Se vi sono più motivi per cui un sito non può essere dismesso, viene visualizzato il motivo più critico.

Motivo possibile della decommissionazione	Descrizione	Passo successivo
Segno di spunta verde (✔)	È possibile decommissionare questo sito.	Passare a. il passo successivo.

Motivo possibile della decommissionazione	Descrizione	Passo successivo
No Questo sito contiene il nodo di amministrazione principale.	Impossibile decommissionare un sito contenente il nodo di amministrazione primario.	Nessuno. Impossibile eseguire questa procedura.
No Questo sito contiene uno o più nodi di archiviazione.	Impossibile decommissionare un sito contenente un nodo di archiviazione.	Nessuno. Impossibile eseguire questa procedura.
No Tutti i nodi di questo sito sono disconnessi. Contatta il tuo rappresentante commerciale NetApp.	Non è possibile eseguire la decommissionazione di un sito connesso a meno che tutti i nodi del sito non siano connessi ( ).	Se si desidera eseguire una decommissionazione del sito disconnesso, è necessario contattare il rappresentante commerciale NetApp, che esaminerà i requisiti e attiverà il resto della procedura guidata Decommission Site. **IMPORTANTE**: Non scollegare mai i nodi online per poter rimuovere un sito. I dati andranno persi.

L'esempio mostra un sistema StorageGRID con tre siti. Il segno di spunta verde ( ) Per i siti Raleigh e Sunnyvale indica che è possibile decommissionarli. Tuttavia, non è possibile decommissionare il sito di Vancouver perché contiene il nodo di amministrazione primario.

1. Se è possibile decommissionare, selezionare il pulsante di opzione corrispondente al sito.

   Il pulsante **Avanti** è attivato.

2. Selezionare **Avanti**.

   Viene visualizzato il punto 2 (Visualizza dettagli).

Fase 2: Visualizzare i dettagli

Dalla fase 2 (Visualizza dettagli) della procedura guidata Decommission Site, è possibile esaminare i nodi inclusi nel sito, verificare la quantità di spazio utilizzata su ciascun nodo di storage e valutare la quantità di spazio libero disponibile negli altri siti della griglia.

Prima di iniziare

Prima di decommissionare un sito, è necessario esaminare la quantità di dati oggetto presenti nel sito.

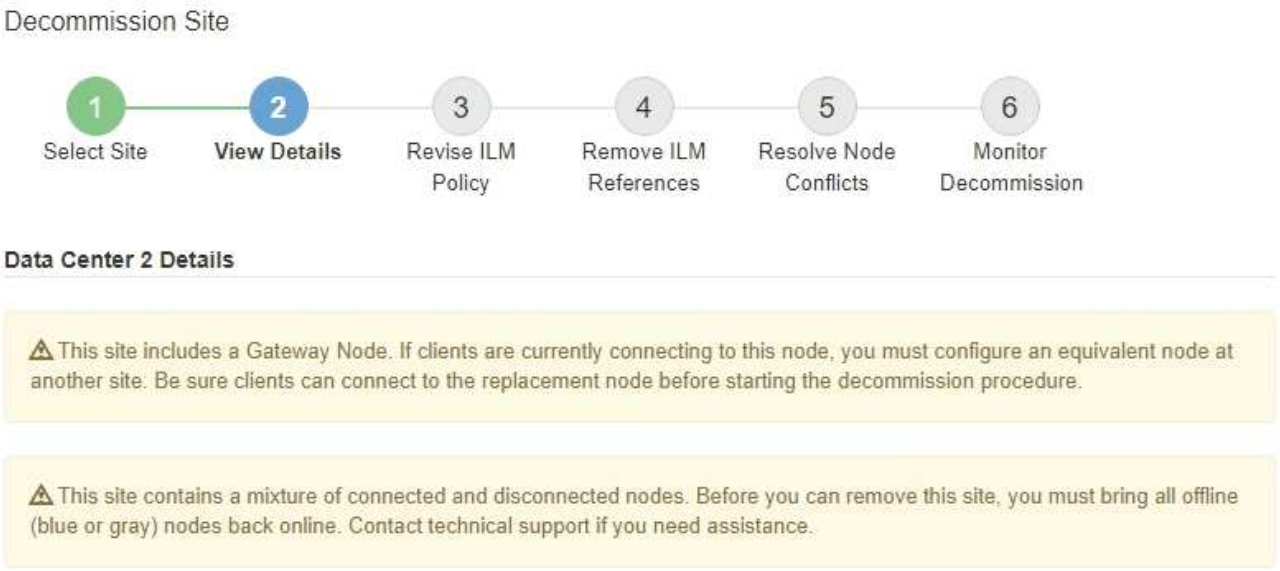
- Se si sta eseguendo una decommissionazione del sito connesso, è necessario comprendere la quantità di dati oggetto attualmente presenti nel sito prima di aggiornare ILM. In base alle capacità del sito e alle esigenze di protezione dei dati, è possibile creare nuove regole ILM per spostare i dati in altri siti o per eliminare i dati degli oggetti dal sito.

- Eseguire le espansioni dei nodi di storage necessarie prima di avviare la procedura di decommissionamento, se possibile.
- Se si esegue una decommissionazione disconnessa del sito, è necessario comprendere la quantità di dati oggetto che diventeranno inaccessibili in modo permanente quando si rimuove il sito.

> Se si sta eseguendo una decommissionazione disconnessa del sito, ILM non può spostare o eliminare i dati dell'oggetto. Tutti i dati che rimangono nel sito andranno persi. Tuttavia, se la policy ILM è stata progettata per proteggere dalla perdita di un singolo sito, le copie dei dati dell'oggetto rimangono nei siti rimanenti. Vedere "Abilita la protezione contro la perdita di sito".

Fasi

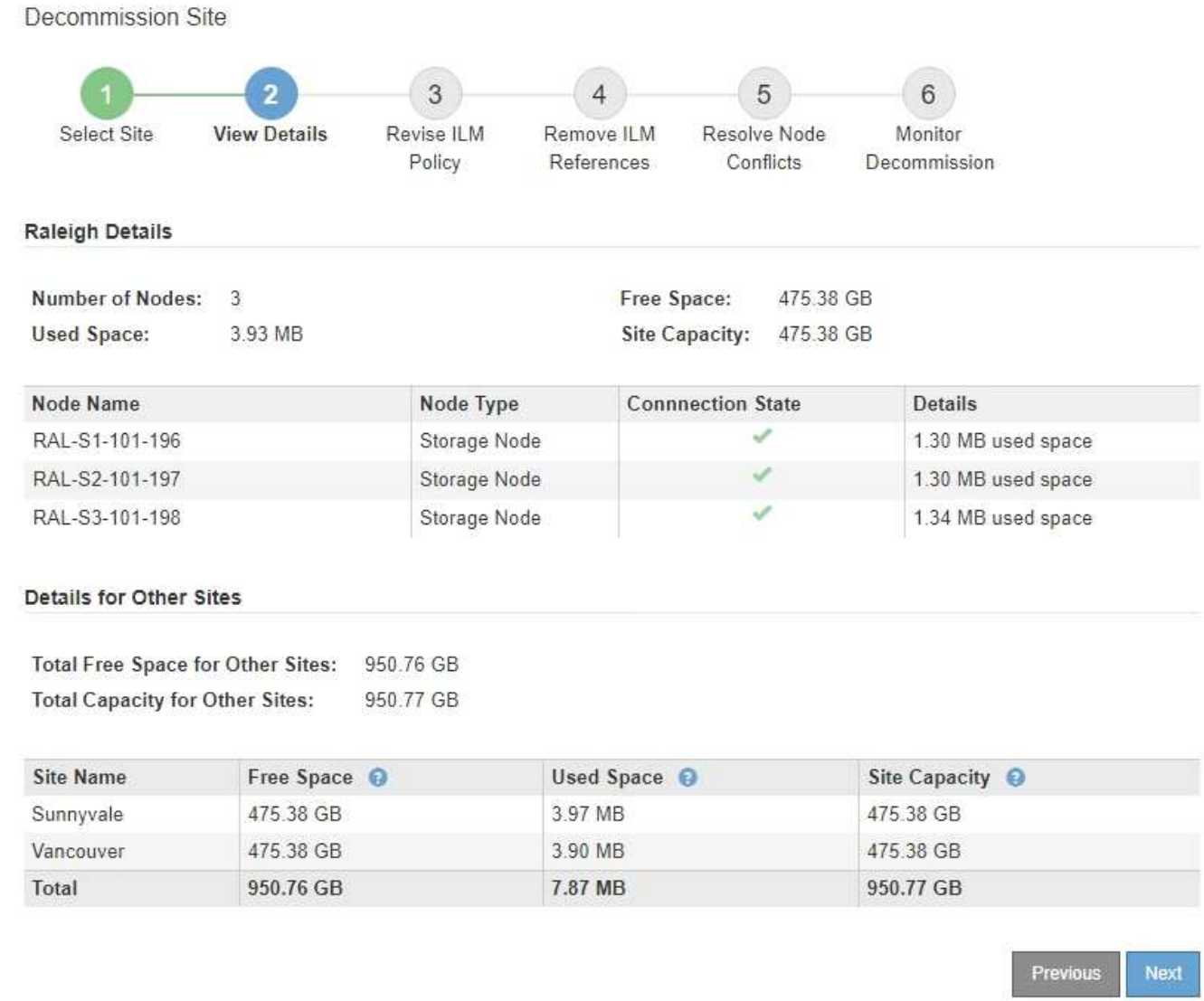
1. Dal passaggio 2 (Visualizza dettagli), esaminare eventuali avvisi relativi al sito selezionato per la rimozione.



   Viene visualizzato un avviso nei seguenti casi:

   - Il sito include un nodo gateway. Se i client S3 e Swift si stanno connettendo a questo nodo, è necessario configurare un nodo equivalente in un altro sito. Assicurarsi che i client possano connettersi al nodo sostitutivo prima di continuare con la procedura di decommissionamento.
   - Il sito contiene una combinazione di) e nodi disconnessi (oppure). Prima di poter rimuovere questo sito, è necessario riportare tutti i nodi offline in linea.

2. Esaminare i dettagli del sito selezionato per la rimozione.



Per il sito selezionato sono incluse le seguenti informazioni:

- Numero di nodi
- Lo spazio utilizzato totale, lo spazio libero e la capacità di tutti i nodi di storage nel sito.
  - Per la decommissionazione di un sito connesso, il valore **Used Space** rappresenta la quantità di dati oggetto che devono essere spostati in altri siti o cancellati con ILM.
  - Per la decommissionazione di un sito disconnesso, il valore **spazio utilizzato** indica la quantità di dati oggetto che diventeranno inaccessibili quando si rimuove il sito.
- Nomi, tipi e stati di connessione dei nodi:
  - (Connesso)
  - (Amministrazione non disponibile)
  - (Sconosciuto)
- Dettagli su ciascun nodo:
  - Per ciascun nodo di storage, la quantità di spazio utilizzata per i dati dell'oggetto.

- Per i nodi Admin e Gateway, se il nodo è attualmente utilizzato in un gruppo ad alta disponibilità (ha). Non è possibile decommissionare un nodo Admin o un nodo Gateway utilizzato in un gruppo ha. Prima di iniziare la decommissionazione, modificare i gruppi ha per rimuovere tutti i nodi nel sito o rimuovere il gruppo ha se include solo i nodi da questo sito. Per istruzioni, vedere "Gestire i gruppi ad alta disponibilità (ha)".

3. Nella sezione Dettagli per altri siti della pagina, valuta lo spazio disponibile negli altri siti della griglia.

Se si sta eseguendo una decommissionazione del sito connesso e si prevede di utilizzare ILM per spostare i dati dell'oggetto dal sito selezionato (invece di eliminarli semplicemente), è necessario assicurarsi che gli altri siti abbiano una capacità sufficiente per ospitare i dati spostati e che rimanga una capacità adeguata per la crescita futura.

> Viene visualizzato un avviso se lo spazio utilizzato * del sito che si desidera rimuovere è maggiore di **spazio libero totale per altri siti**. Per garantire che sia disponibile una capacità di storage adeguata dopo la rimozione del sito, potrebbe essere necessario eseguire un'espansione prima di eseguire questa procedura.

4. Selezionare **Avanti**.

   Viene visualizzato il punto 3 (revisione policy ILM).

Fase 3: Revisione dei criteri ILM

Dal passaggio 3 (Rivedi criteri ILM) della procedura guidata Decommission Site, è possibile determinare se il sito è referenziato da qualsiasi criterio ILM.

Prima di iniziare

Avete una buona comprensione di come "Gestire gli oggetti con ILM". Hai familiarità con la creazione di pool di storage e regole ILM e con la simulazione e l'attivazione di una policy ILM.

A proposito di questa attività

StorageGRID non può decommissionare un sito se una regola ILM di qualsiasi policy (attiva o inattiva) fa riferimento a quel sito.

Se un criterio ILM fa riferimento al sito che si desidera decommissionare, è necessario rimuovere tali criteri o modificarli in modo che soddisfino i seguenti requisiti:

- Proteggere completamente tutti i dati degli oggetti.
- Non fare riferimento al sito che si sta smantellando.

- Non utilizzare pool di archiviazione che si riferiscono al sito o utilizzare l'opzione tutti i siti.
- Non utilizzare profili di erasure coding che fanno riferimento al sito.
- Non utilizzare la regola Crea 2 copie da StorageGRID 11,6 o da installazioni precedenti.

> Non creare mai una regola ILM a copia singola per consentire la rimozione di un sito. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

> Se si esegue un *sito connesso decommissionamento*, è necessario considerare come StorageGRID deve gestire i dati dell'oggetto attualmente presenti nel sito che si desidera rimuovere. A seconda dei requisiti di data Protection, nuove regole possono spostare i dati degli oggetti esistenti in siti diversi o possono eliminare eventuali copie aggiuntive degli oggetti che non sono più necessarie.

Contatta il supporto tecnico se hai bisogno di assistenza nella progettazione di una nuova policy.

Fasi

1. Dalla fase 3 (revisione dei criteri ILM), determinare se i criteri ILM fanno riferimento al sito selezionato per la disattivazione.
2. Se non sono elencati criteri, selezionare **Avanti** per passare a. "Fase 4: Rimuovere i riferimenti ILM".
3. Se sono elencati uno o più criteri ILM *Active*, clonare ogni criterio esistente o creare nuovi criteri che non fanno riferimento al sito da smantellare:

   a. Selezionare il collegamento per il criterio nella colonna Nome criterio.

      La pagina dei dettagli del criterio ILM per il criterio viene visualizzata in una nuova scheda del browser. La pagina Decommission Site rimane aperta nella scheda Other (Altro).

   b. Attenersi alle seguenti linee guida e istruzioni, se necessario:

      - Utilizzare le regole ILM:
        - "Creare uno o più pool di storage" che non si riferiscono al sito.
        - "Modificare o sostituire le regole" che fanno riferimento al sito.

          > Non selezionare la regola **Crea 2 copie** perché questa regola utilizza il pool di storage **tutti i nodi di storage**, che non è consentito.

      - Utilizzare i criteri ILM:
        - "Clonazione di una policy ILM esistente" oppure "Creare una nuova policy ILM".
        - Assicurarsi che la regola predefinita e le altre regole non facciano riferimento al sito.

          > Verificare che le regole ILM siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio.

   c. Acquisire gli oggetti di test e simulare la policy per applicare le regole corrette.

Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile. Esaminare attentamente e simulare la policy prima di attivarla per confermare che funzionerà come previsto.

Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

d. Attivare le nuove policy e assicurarsi che le vecchie policy siano ora inattive.

   Se si desidera attivare più criteri, "Seguire la procedura per creare i tag dei criteri ILM".

Se si sta eseguendo una decommissionazione del sito connesso, StorageGRID inizia a rimuovere i dati dell'oggetto dal sito selezionato non appena si attiva il nuovo criterio ILM. Lo spostamento o l'eliminazione di tutte le copie degli oggetti potrebbe richiedere settimane. Sebbene sia possibile avviare in sicurezza la decommissionazione di un sito mentre i dati degli oggetti sono ancora presenti nel sito, la procedura di decommissionazione viene completata più rapidamente e con meno interruzioni e impatti sulle performance se si consente di spostare i dati dal sito prima di avviare la procedura di decommissionazione effettiva (Selezionando **Avvia decommissionazione** nella fase 5 della procedura guidata).

4. Per ciascun criterio *inattivo*, modificarlo o rimuoverlo selezionando prima il collegamento per ciascun criterio come descritto nei passaggi precedenti.
   - "Modificare il criterio" quindi non fa riferimento al sito da smantellare.
   - "Rimuovere un criterio".
5. Al termine delle modifiche alle regole e ai criteri ILM, non dovrebbero essere più elencati nel passaggio 3 (revisione dei criteri ILM). Selezionare **Avanti**.

   Viene visualizzato il punto 4 (Rimuovi riferimenti ILM).

Fase 4: Rimuovere i riferimenti ILM

Dal passaggio 4 (Rimuovi riferimenti ILM) della procedura guidata Decommission Site (Sito di decontaminazione), è necessario eliminare o modificare eventuali regole ILM non utilizzate che fanno riferimento al sito, anche se le regole non sono utilizzate in alcun criterio ILM.

Fasi

1. Determinare se eventuali regole ILM inutilizzate fanno riferimento al sito.

   Se sono elencate regole ILM, tali regole fanno ancora riferimento al sito ma non vengono utilizzate in alcuna politica.

Quando StorageGRID decomprime il sito, disattiva automaticamente tutti i profili di erasure coding inutilizzati che fanno riferimento al sito ed elimina automaticamente eventuali pool di storage inutilizzati che fanno riferimento al sito. Il pool di storage All Storage Node (StorageGRID 11.6 e versioni precedenti) viene rimosso perché utilizza il sito All Sites.

2. Modificare o eliminare ogni regola inutilizzata:
   - Per modificare una regola, andare alla pagina ILM rules (regole ILM) e aggiornare tutti i posizionamenti che utilizzano un profilo di erasure coding o un pool di storage che fa riferimento al sito. Quindi, tornare al **Passo 4 (Rimozione dei riferimenti ILM)**.
   - Per eliminare una regola, selezionare l'icona del cestino E selezionare **OK**.

   È necessario eliminare la regola **Make 2 copies** prima di poter decommissionare un sito.

3. Verificare che nessuna regola ILM non utilizzata faccia riferimento al sito e che il pulsante **Avanti** sia attivato.
4. Selezionare **Avanti**.

   Tutti i pool storage rimanenti e i profili di erasure coding relativi al sito non saranno più validi quando il sito viene rimosso. Quando StorageGRID decomprime il sito, disattiva automaticamente tutti i profili di erasure coding inutilizzati che fanno riferimento al sito ed elimina automaticamente eventuali pool di storage inutilizzati che fanno riferimento al sito. Il pool di storage All Storage Node (StorageGRID 11.6 e versioni precedenti) viene rimosso perché utilizza il sito All Sites.

   Viene visualizzato il punto 5 (Risolvi conflitti di nodi).

Fase 5: Risolvere i conflitti dei nodi (e avviare la decommissionazione)

Dalla fase 5 (Risolvi conflitti di nodi) della procedura guidata Smantella sito, è possibile determinare se i nodi nel sistema StorageGRID sono disconnessi o se i nodi nel sito selezionato appartengono a un gruppo ad alta disponibilità (ha). Una volta risolti i conflitti di nodo, avviare la procedura di decommissionamento da questa pagina.

Prima di iniziare

È necessario assicurarsi che tutti i nodi nel sistema StorageGRID siano nello stato corretto, come indicato di seguito:

- Tutti i nodi nel sistema StorageGRID devono essere connessi ( ).

  Se si sta eseguendo una decommissionazione del sito disconnesso, tutti i nodi del sito che si sta rimuovendo devono essere disconnessi e tutti i nodi di tutti gli altri siti devono essere connessi.

  La decommissionazione non si avvia se uno o più volumi sono offline (non montati) o se sono online (montati) ma in uno stato di errore.

  Se uno o più volumi vengono disconnessi mentre è in corso una decommissionazione, il processo di decommissionamento viene completato dopo che questi volumi sono tornati online.

- Nessun nodo del sito che si sta rimuovendo può avere un'interfaccia che appartiene a un gruppo ad alta disponibilità (ha).

A proposito di questa attività

Se un nodo è elencato per la fase 5 (Risolvi conflitti di nodi), è necessario correggere il problema prima di poter avviare la decommissionazione.

Prima di iniziare la procedura di decommissionamento del sito da questa pagina, fare riferimento alle seguenti considerazioni:

- Per completare la procedura di decommissionamento, è necessario attendere il tempo necessario.

> Lo spostamento o l'eliminazione dei dati degli oggetti da un sito potrebbe richiedere giorni, settimane o persino mesi, a seconda della quantità di dati nel sito, del carico sul sistema, delle latenze di rete e della natura delle modifiche ILM richieste.

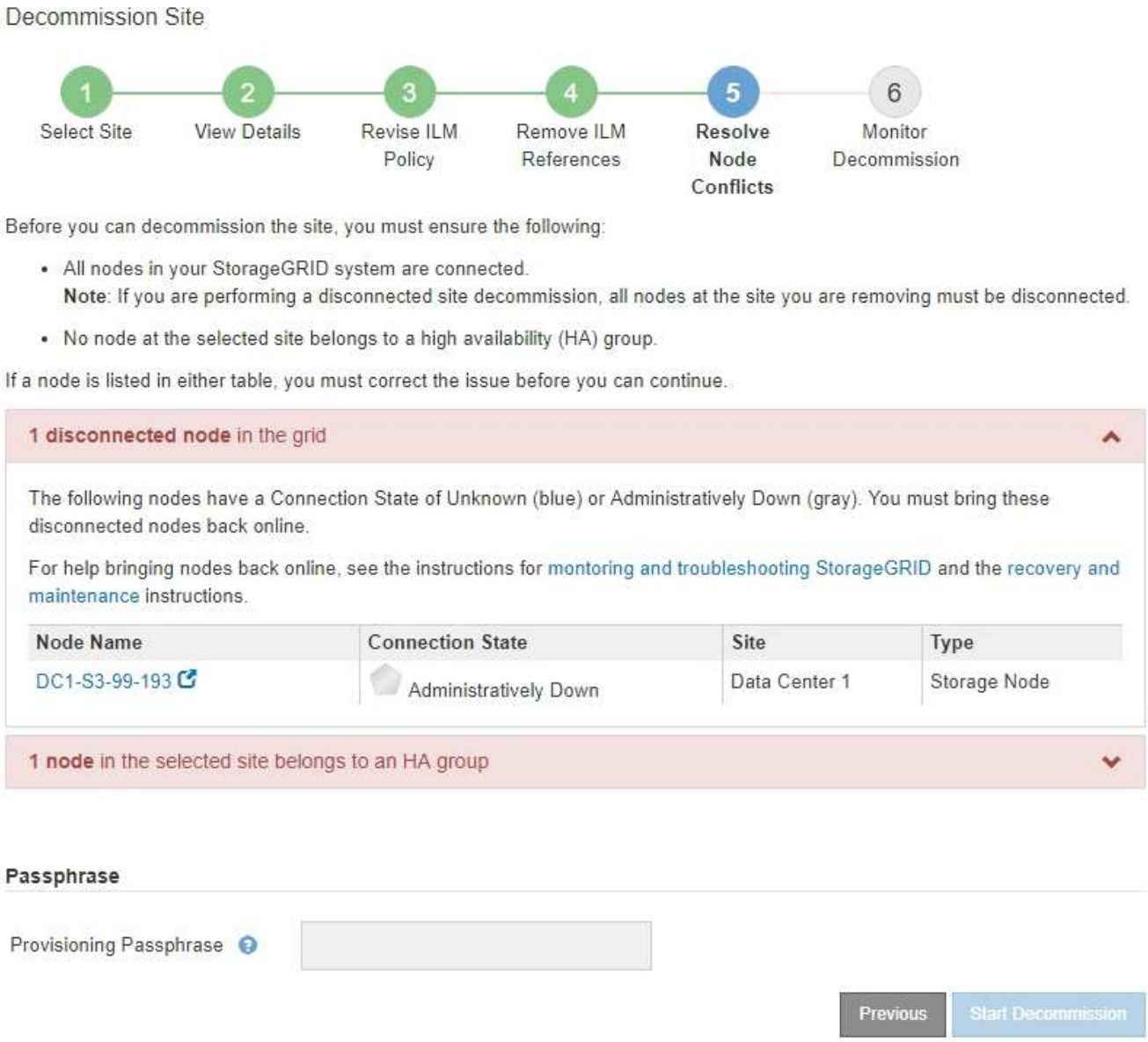
- Durante l'esecuzione della procedura di decommissionamento del sito:
  - Non è possibile creare regole ILM che si riferiscono al sito da smantellare. Inoltre, non è possibile modificare una regola ILM esistente per fare riferimento al sito.
  - Non è possibile eseguire altre procedure di manutenzione, ad esempio l'espansione o l'aggiornamento.

> Se è necessario eseguire un'altra procedura di manutenzione durante la decommissionazione di un sito connesso, è possibile sospendere la procedura durante la rimozione dei nodi di storage. Il pulsante **Pause** viene attivato durante la fase "decommissionamento dei dati replicati ed Erasure-Coded Data" (disattivazione dei dati replicati ed Erasure-Coded Data).

  - Se è necessario ripristinare un nodo dopo aver avviato la procedura di decommissionamento del sito, contattare il supporto.

Fasi

1. Consultare la sezione nodi disconnessi del passaggio 5 (Risolvi conflitti di nodi) per determinare se uno stato di connessione dei nodi nel sistema StorageGRID è sconosciuto ( ) O dal punto di vista amministrativo ( ).

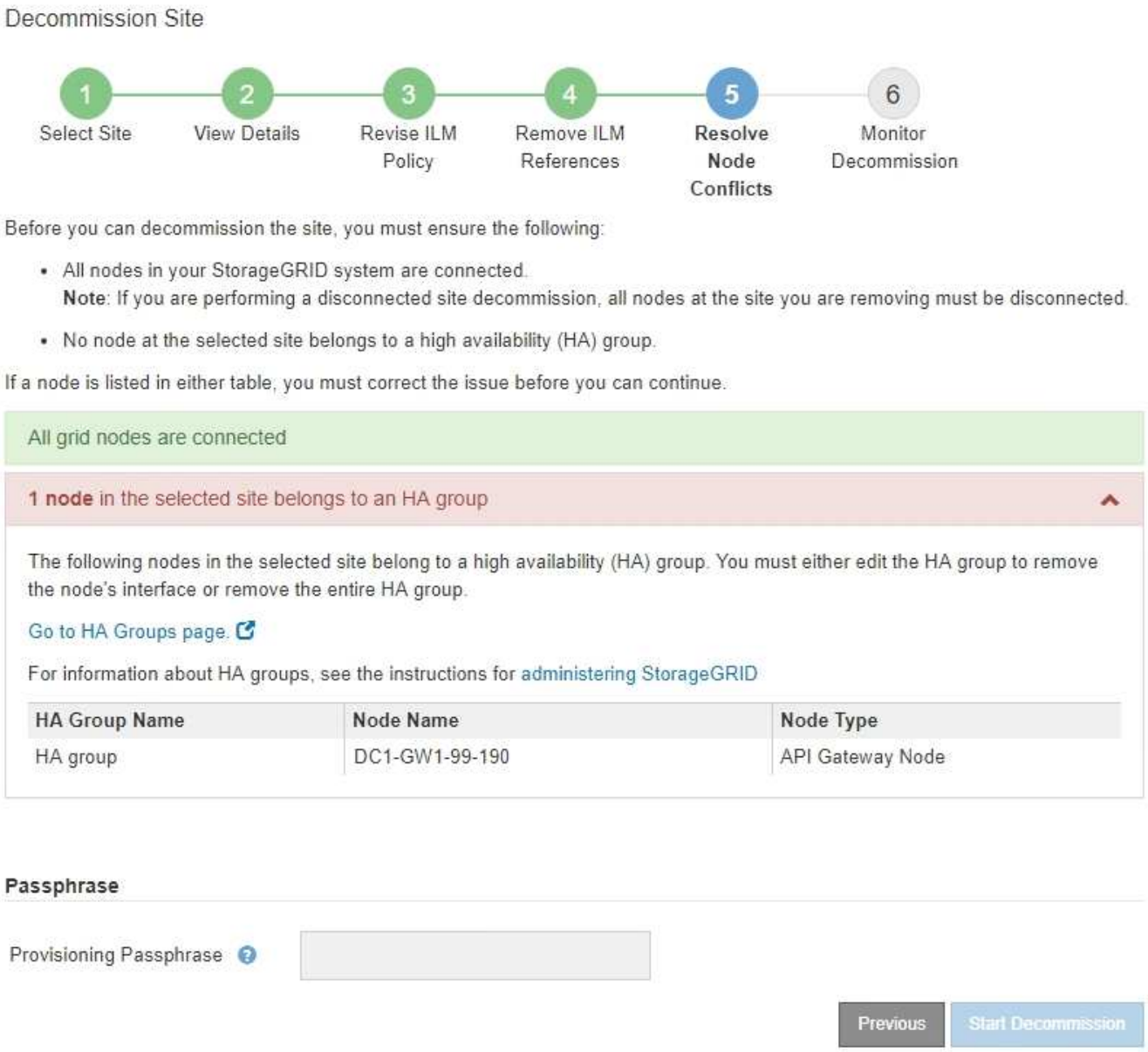


2. Se alcuni nodi sono disconnessi, riportarli in linea.

   Vedere "Procedure dei nodi". Se hai bisogno di assistenza, contatta il supporto tecnico.

3. Quando tutti i nodi disconnessi sono stati riportati online, consultare la sezione gruppi ha del passaggio 5 (Risolvi i conflitti dei nodi).

   Questa tabella elenca tutti i nodi del sito selezionato che appartengono a un gruppo ad alta disponibilità (ha).

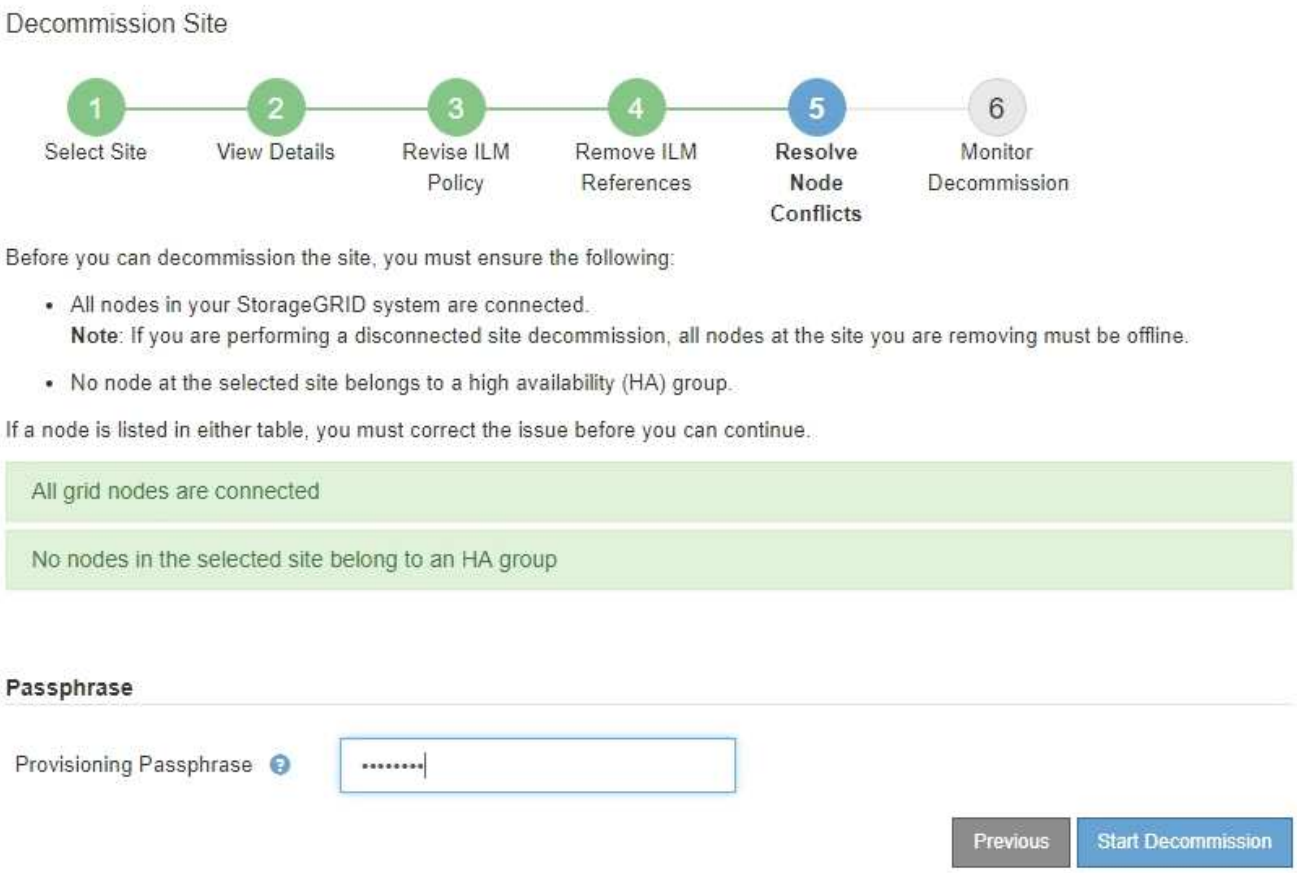


4. Se nell'elenco sono presenti nodi, eseguire una delle seguenti operazioni:
   - Modificare ciascun gruppo ha interessato per rimuovere l'interfaccia del nodo.
   - Rimuovere un gruppo ha che include solo i nodi da questo sito.
     Consultare le istruzioni per l'amministrazione di StorageGRID.

   Se tutti i nodi sono connessi e nessun nodo nel sito selezionato viene utilizzato in un gruppo ha, viene attivato il campo **Provisioning Passphrase**.

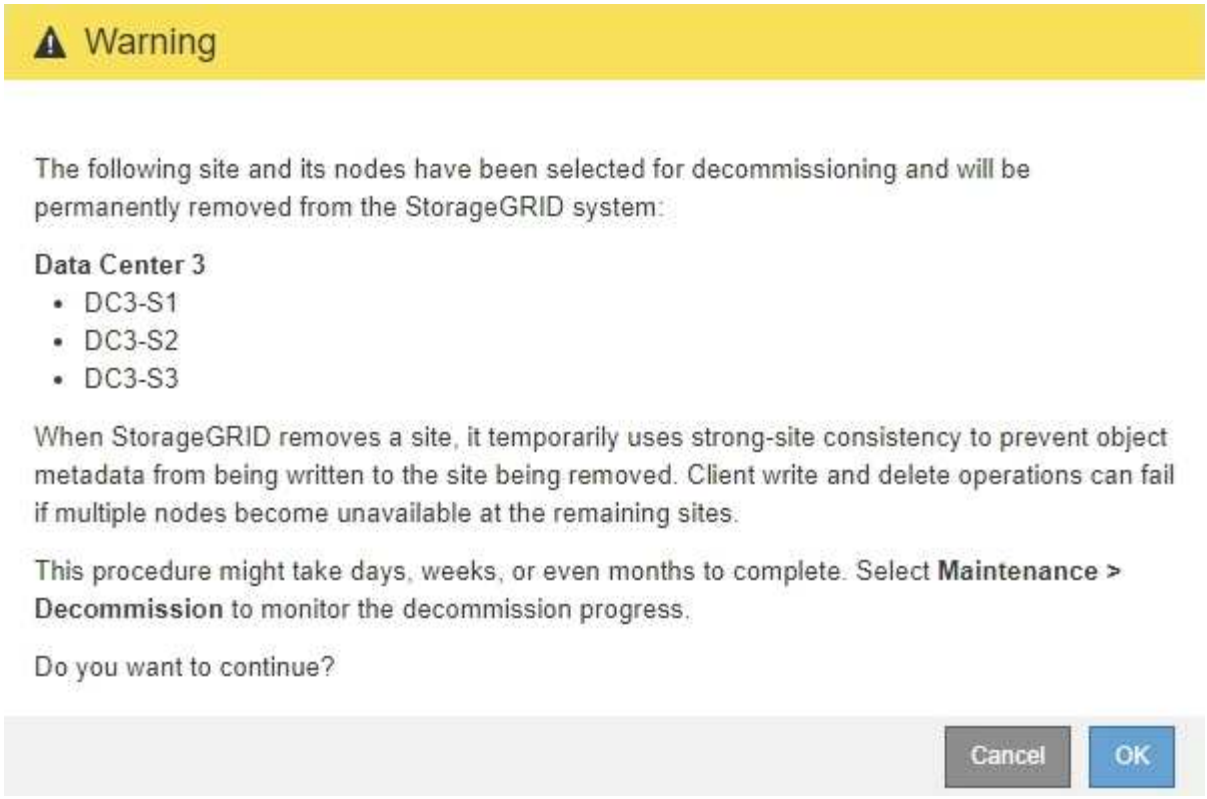
5. Inserire la passphrase di provisioning.

   Il pulsante **Avvia decommissionazione** viene attivato.



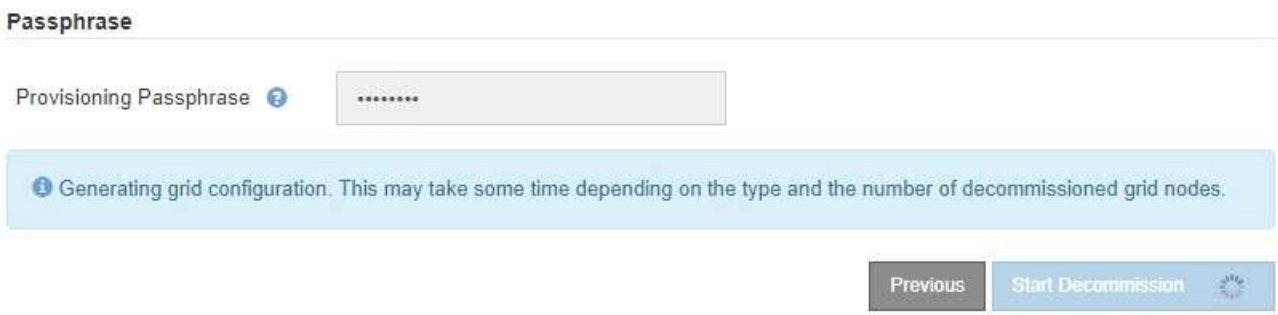
6. Se si è pronti per avviare la procedura di decommissionamento del sito, selezionare **Avvia decommissionazione**.

   Un avviso elenca il sito e i nodi che verranno rimossi. Ti ricordiamo che potrebbero essere necessari giorni, settimane o mesi per rimuovere completamente il sito.



7. Esaminare l'avviso. Se si è pronti per iniziare, selezionare **OK**.

   Quando viene generata la nuova configurazione della griglia, viene visualizzato un messaggio. Questo processo potrebbe richiedere del tempo, a seconda del tipo e del numero di nodi di rete decommissionati.



   Una volta generata la nuova configurazione della griglia, viene visualizzato il punto 6 (Monitor Decommission).

   Il pulsante **precedente** rimane disattivato fino al completamento della decommissionazione.

Fase 6: Rimozione del monitor

Dalla fase 6 (Monitor Decommission) della procedura guidata della pagina Decommission Site (Smantella sito), è possibile monitorare l'avanzamento della procedura di rimozione del sito.

A proposito di questa attività

Quando StorageGRID rimuove un sito connesso, rimuove i nodi nel seguente ordine:

1. Nodi gateway
2. Nodi di amministrazione
3. Nodi di storage

Quando StorageGRID rimuove un sito disconnesso, rimuove i nodi nel seguente ordine:

1. Nodi gateway
2. Nodi di storage
3. Nodi di amministrazione

Ogni nodo gateway o nodo amministratore potrebbe richiedere solo pochi minuti o un'ora per la rimozione; tuttavia, i nodi storage potrebbero richiedere giorni o settimane.

Fasi

1. Non appena viene generato un nuovo pacchetto di ripristino, scaricare il file.

> Scarica il pacchetto di ripristino il prima possibile per assicurarti di ripristinare la griglia in caso di problemi durante la procedura di decommissionamento.

   a. Selezionare il collegamento nel messaggio o selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.

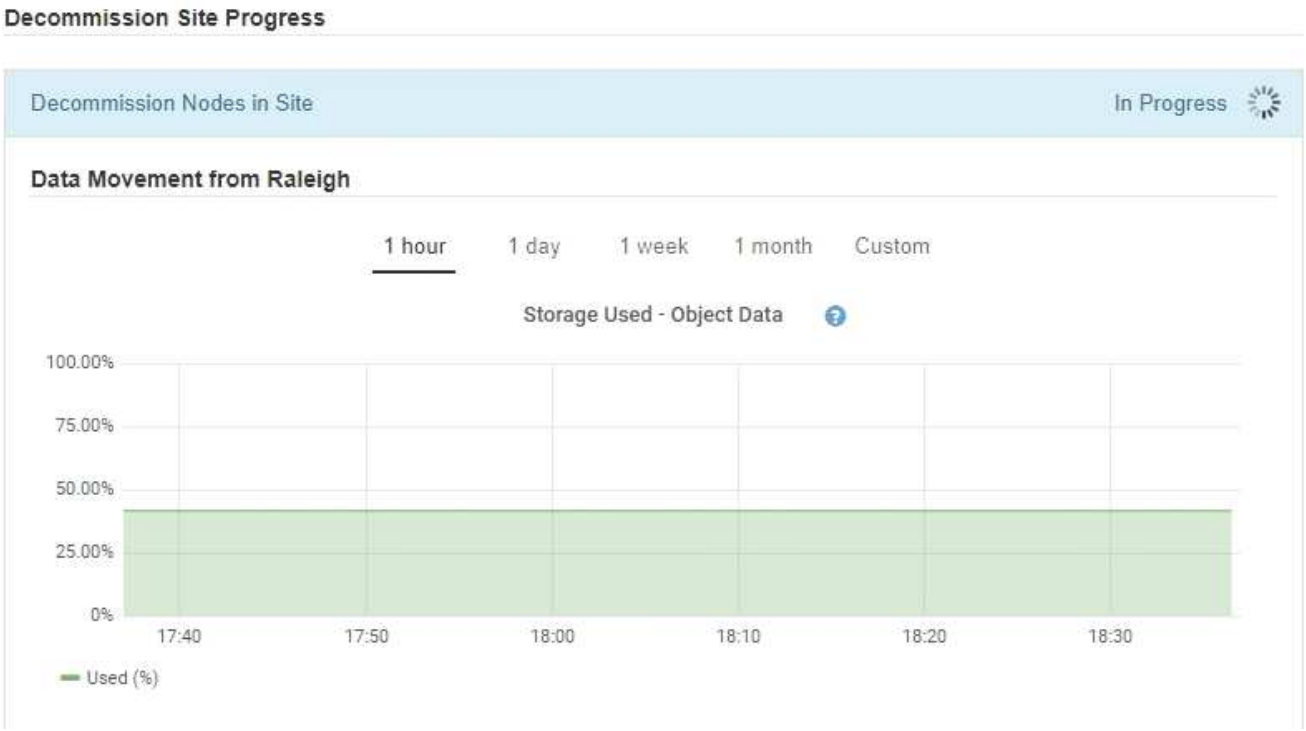
   b. Scaricare il `.zip` file.

      Consultare le istruzioni per "Download del pacchetto di ripristino".

> 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.

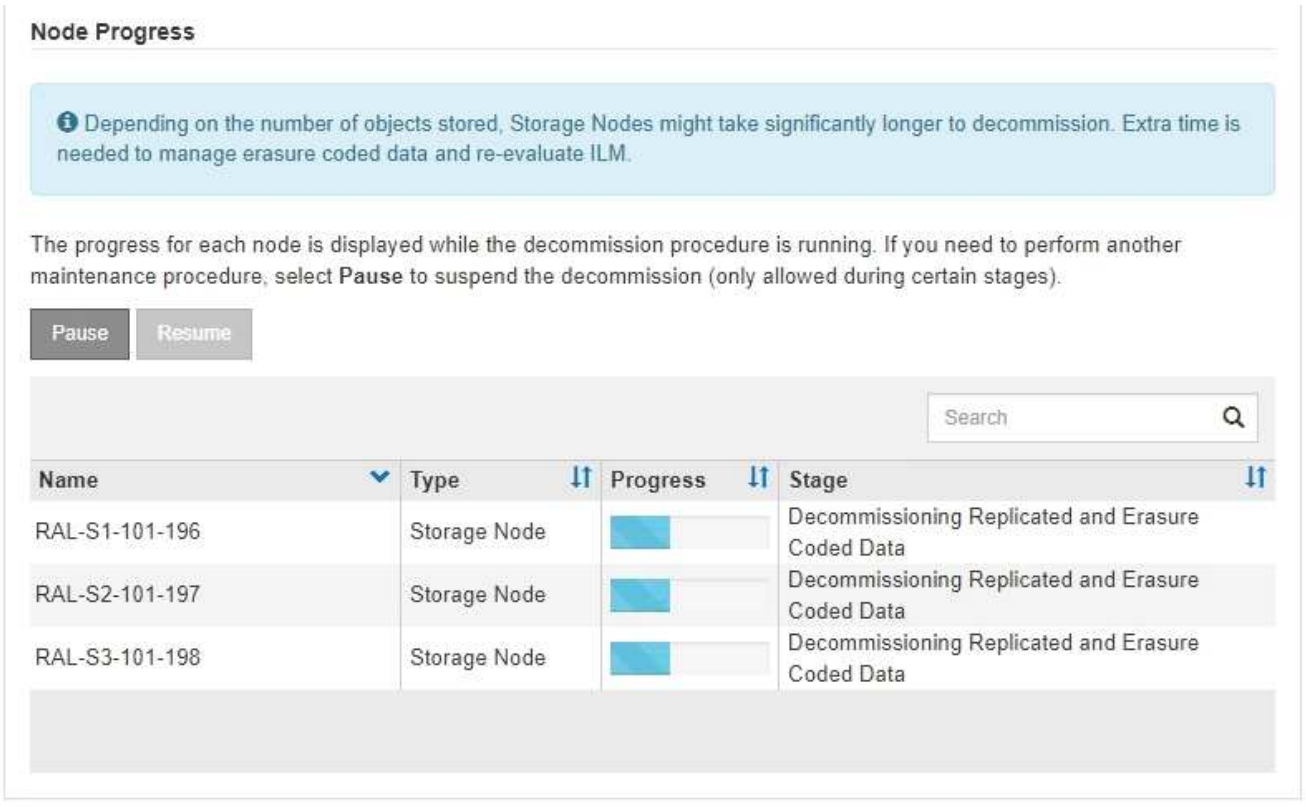
2. Utilizzando il grafico spostamento dati, monitorare lo spostamento dei dati oggetto da questo sito ad altri siti.

   Lo spostamento dei dati ha avuto inizio quando è stata attivata la nuova policy ILM nella fase 3 (revisione policy ILM). Lo spostamento dei dati avviene durante l'intera procedura di decommissionamento.



3. Nella sezione Node Progress della pagina, monitorare l'avanzamento della procedura di decommissionamento man mano che i nodi vengono rimossi.

   Quando un nodo di storage viene rimosso, ciascun nodo passa attraverso una serie di fasi. Sebbene la maggior parte di queste fasi si verifichi rapidamente o anche in modo impercettibile, potrebbe essere necessario attendere giorni o addirittura settimane per il completamento di altre fasi, in base alla quantità di dati da spostare. Per gestire i dati con codifica di cancellazione e rivalutare ILM è necessario un tempo aggiuntivo.



Se si sta monitorando l'avanzamento della decommissionazione di un sito connesso, fare riferimento a questa tabella per comprendere le fasi di decommissionamento di un nodo di storage:

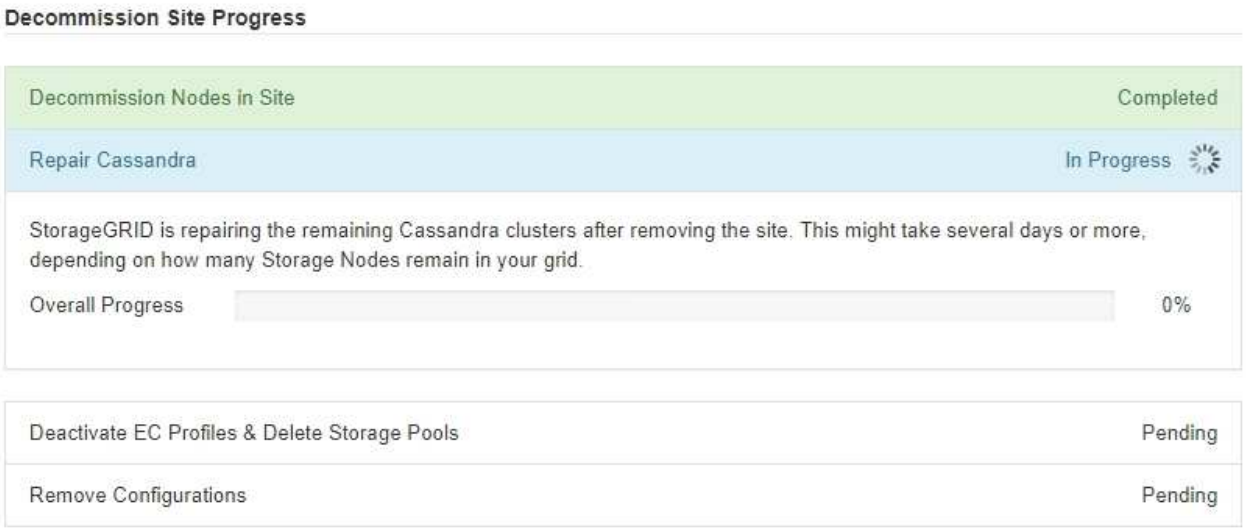
Fase	Durata stimata
In sospeso	Minuti o meno
Attendere i blocchi	Minuti
Preparare l'attività	Minuti o meno
Contrassegno LDR disattivato	Minuti
Decommissionamento dei dati replicati ed Erasure-Coded	Ore, giorni o settimane in base alla quantità di dati **Nota**: Se è necessario eseguire altre attività di manutenzione, è possibile sospendere la decommissionazione del sito in questa fase.
Stato impostato LDR	Minuti
Svuotare le code di audit	Da minuti a ore, in base al numero di messaggi e alla latenza di rete.
Completo	Minuti

Se si sta monitorando l'avanzamento di una decommissionazione di un sito disconnesso, fare riferimento a questa tabella per comprendere le fasi di decommissionamento di un nodo di storage:

Fase	Durata stimata
In sospeso	Minuti o meno
Attendere i blocchi	Minuti
Preparare l'attività	Minuti o meno
Disattiva servizi esterni	Minuti
Revoca del certificato	Minuti
Annulla registrazione nodo	Minuti
Livello di storage Annulla registrazione	Minuti
Rimozione del gruppo di storage	Minuti
Rimozione entità	Minuti

Fase	Durata stimata
Completo	Minuti

4. Una volta che tutti i nodi hanno raggiunto la fase completa, attendere il completamento delle restanti operazioni di decommissionamento del sito.
   - Durante la fase **Riparazione Cassandra**, StorageGRID effettua le riparazioni necessarie ai cluster Cassandra che rimangono nella vostra griglia. Queste riparazioni potrebbero richiedere diversi giorni o più, a seconda del numero di nodi di storage rimasti nel vostro grid.

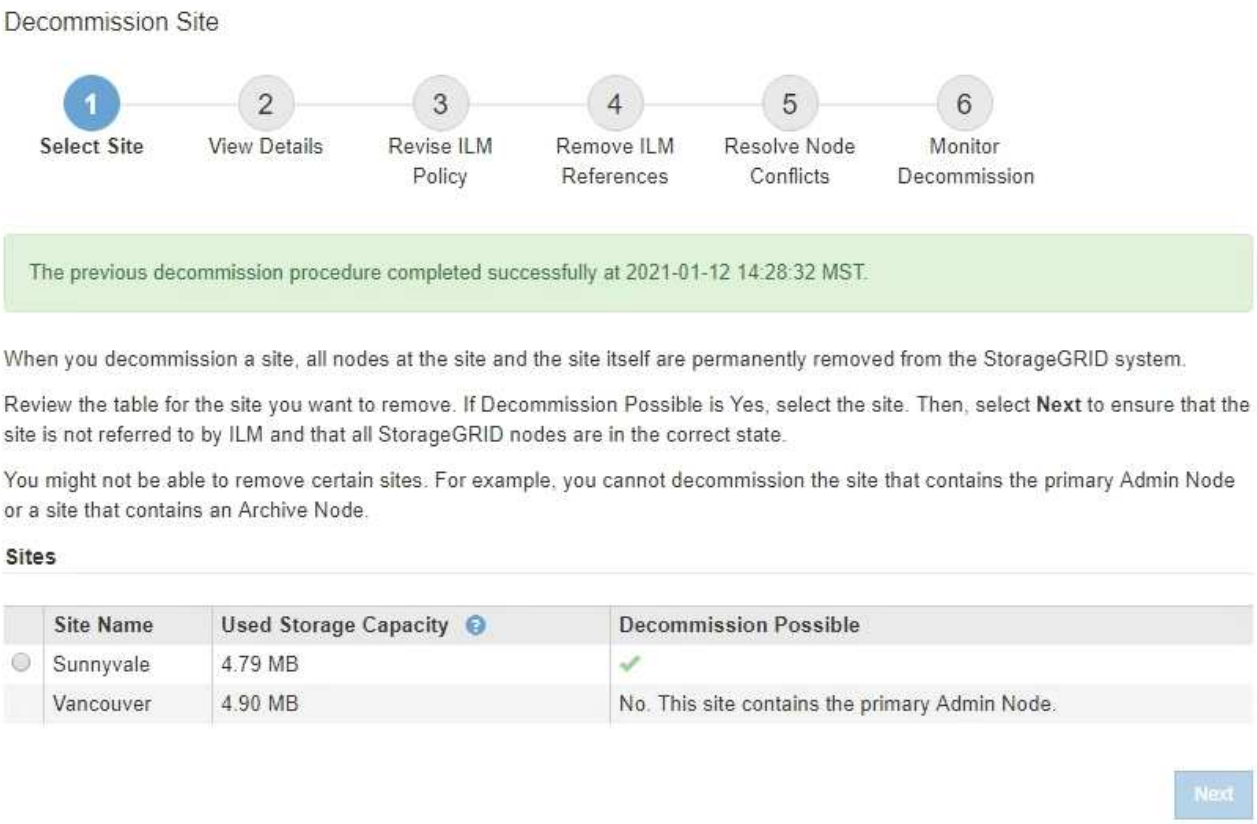


   - Durante la fase **Disattiva profili EC ed elimina pool di storage**, vengono apportate le seguenti modifiche ILM:
     - Tutti i profili di erasure coding che fanno riferimento al sito sono disattivati.
     - Tutti i pool di storage che fanno riferimento al sito vengono eliminati.

> Viene rimosso anche il pool di storage di tutti i nodi di storage (StorageGRID 11.6 e versioni precedenti) in quanto utilizza il sito All Sites.

   - Infine, durante la fase **Remove Configuration**, tutti i riferimenti rimanenti al sito e ai relativi nodi vengono rimossi dal resto della griglia.

5. Una volta completata la procedura di decommissionamento, la pagina Decommission Site (Sito di decommissionamento) mostra un messaggio di esito positivo e il sito rimosso non viene più visualizzato.



Al termine

Completare queste attività dopo aver completato la procedura di decommissionamento del sito:

- Assicurarsi che i dischi di tutti i nodi di storage nel sito decommissionato siano puliti. Utilizzare uno strumento o un servizio di cancellazione dei dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dai dischi.
- Se il sito includeva uno o più nodi di amministrazione e l'SSO (Single Sign-on) è attivato per il sistema StorageGRID, rimuovere tutti i trust delle parti che si affidano al sito dai servizi di federazione di Active Directory (ad FS).
- Una volta spenti automaticamente i nodi durante la procedura di decommissionamento del sito connesso, rimuovere le macchine virtuali associate.

Rinominare la griglia, il sito o il nodo

Rinomina griglia, siti e nodi: Panoramica

Se necessario, è possibile modificare i nomi visualizzati in Grid Manager per l'intera griglia, ciascun sito e ciascun nodo. È possibile aggiornare i nomi visualizzati in modo sicuro e in qualsiasi momento.

Qual è la procedura di ridenominazione?

Quando si installa inizialmente StorageGRID, specificare un nome per la griglia, ciascun sito e ciascun nodo. Questi nomi iniziali sono noti come *nomi di sistema* e sono i nomi inizialmente mostrati in StorageGRID.

I nomi di sistema sono richiesti per le operazioni StorageGRID interne e non possono essere modificati. Tuttavia, è possibile utilizzare la procedura di ridenominazione per definire nuovi *nomi di visualizzazione* per la griglia, ciascun sito e ciascun nodo. Questi nomi visualizzati vengono visualizzati in diverse posizioni StorageGRID invece dei nomi di sistema sottostanti (o in alcuni casi, oltre a questi).

Utilizzare la procedura di ridenominazione per correggere gli errori di battitura, implementare una convenzione di naming diversa o per indicare che un sito e tutti i suoi nodi sono stati ricollocati. A differenza dei nomi di sistema, i nomi visualizzati possono essere aggiornati quando richiesto e senza influire sulle operazioni StorageGRID.

Dove vengono visualizzati i nomi di sistema e di visualizzazione?

La seguente tabella riassume i nomi dei sistemi e dei display nell'interfaccia utente di StorageGRID e nei file StorageGRID.

Posizione	Nome del sistema	Nome visualizzato
Pagine di Grid Manager	Visualizzato a meno che l'elemento non venga rinominato	Se un elemento viene rinominato, viene visualizzato invece del nome del sistema in queste posizioni: • Dashboard • Pagina nodi • Pagine di configurazione per gruppi ad alta disponibilità, endpoint del bilanciamento del carico, interfacce VLAN, server di gestione delle chiavi, password grid, e il controllo del firewall • Avvisi • Definizioni del pool di storage • Pagina di ricerca dei metadati degli oggetti • Pagine relative alle procedure di manutenzione, tra cui upgrade, hotfix, upgrade del sistema operativo SANtricity, decommissionamento, espansione, ripristino e controllo dell'esistenza di oggetti • Pagine di supporto (registri e diagnostica) • Pagina Single Sign-on (accesso singolo), accanto al nome host del nodo di amministrazione nella tabella per i dettagli del nodo di amministrazione

Posizione	Nome del sistema	Nome visualizzato
Scheda **NODES** > **Overview** per un nodo	Sempre mostrato	Visualizzato solo se l'elemento viene rinominato
Pagine legacy in Grid Manager (ad esempio, **SUPPORT** > **Grid Topology**)	In figura	Non mostrato
API **node-Health**	Sempre restituito	Restituito solo se l'elemento viene rinominato

Prompt quando si utilizza SSH per accedere a un nodo	Visualizzato come nome principale a meno che l'elemento non sia stato rinominato:
	
	`admin@SYSTEM-NAME: ~ $`
	
	Incluso tra parentesi quando l'elemento viene rinominato:
	
	`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`
		Visualizzato come nome principale quando l'elemento viene rinominato:
		
		`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`

`Passwords.txt` Nel pacchetto di ripristino	Mostrato come `Server Name`	Mostrato come `Display Name`
`/etc/hosts` file su tutti i nodi Ad esempio: `10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host`	Sempre mostrato nella seconda colonna	Quando l'elemento viene rinominato, visualizzato nella quarta colonna
`topology-display-names.json`, Incluso con i dati AutoSupport	Non incluso	Vuoto a meno che gli elementi non siano stati rinominati; in caso contrario, gli ID di griglia, sito e nodo vengono mappati sui rispettivi nomi visualizzati.

Requisiti per i nomi visualizzati

Prima di utilizzare questa procedura, esaminare i requisiti per i nomi visualizzati.

Visualizza i nomi dei nodi

I nomi visualizzati per i nodi devono seguire queste regole:

- Deve essere unico nel tuo sistema StorageGRID.
- Non può essere uguale al nome di sistema per qualsiasi altro elemento nel sistema StorageGRID.
- Deve contenere almeno 1 e non più di 32 caratteri.
- Può contenere numeri, trattini (-) e lettere maiuscole e minuscole.
- Può iniziare o terminare con una lettera o un numero, ma non può iniziare o terminare con un trattino.
- Non possono essere tutti i numeri.
- Sono insensibili alle maiuscole e alle minuscole. Ad esempio, `DC1-ADM` e. `dc1-adm` sono considerati duplicati.

È possibile rinominare un nodo con un nome visualizzato precedentemente utilizzato da un nodo diverso, a condizione che la ridenominazione non comporti un nome visualizzato o un nome di sistema duplicati.

Visualizza i nomi della griglia e dei siti

I nomi visualizzati per la griglia e i siti seguono le stesse regole con le seguenti eccezioni:

- Può includere spazi.
- Può includere questi caratteri speciali: `= - _ : , . @ !`
- Può iniziare e terminare con i caratteri speciali, inclusi i trattini.
- Può essere composto da tutti i numeri o da caratteri speciali.

Best practice per i nomi visualizzati

Se si prevede di rinominare più elementi, documentare lo schema di denominazione generale prima di utilizzare questa procedura. Un sistema che garantisce nomi univoci, coerenti e facili da comprendere a colpo d'occhio.

È possibile utilizzare qualsiasi convenzione di naming che soddisfi i requisiti dell'organizzazione. Prendi in considerazione questi suggerimenti di base su cosa includere:

- **Site indicator**: Se si dispone di più siti, aggiungere un codice sito a ciascun nome di nodo.
- **Node type**: I nomi dei nodi indicano generalmente il tipo di nodo. È possibile utilizzare abbreviazioni come `s`, `adm`, `gw`, e. `arc` (Nodo storage, nodo amministratore, nodo gateway e nodo archivio).
- **Node Number**: Se un sito contiene più di uno di un particolare tipo di nodo, aggiungere un numero univoco al nome di ciascun nodo.

Pensa due volte prima di aggiungere dettagli specifici ai nomi che potrebbero cambiare nel tempo. Ad esempio, non includere gli indirizzi IP nei nomi dei nodi perché è possibile modificarli. Allo stesso modo, le posizioni dei rack o i numeri dei modelli di appliance possono cambiare se si spostano le apparecchiature o si aggiorna l'hardware.

Esempi di nomi visualizzati

Si supponga che il sistema StorageGRID disponga di tre data center e di nodi di tipi diversi in ciascun data center. I nomi visualizzati potrebbero essere semplici come questi:

- **Griglia**: `StorageGRID Deployment`
- **Primo sito**: `Data Center 1`

    - `dc1-adm1`
    - `dc1-s1`
    - `dc1-s2`
    - `dc1-s3`
    - `dc1-gw1`
- **Secondo sito**: `Data Center 2`
    - `dc2-adm2`
    - `dc2-s1`
    - `dc2-s2`
    - `dc2-s3`
- **Terzo sito**: `Data Center 3`
    - `dc3-s1`
    - `dc3-s2`
    - `dc3-s3`

Aggiungere o aggiornare i nomi visualizzati

È possibile utilizzare questa procedura per aggiungere o aggiornare i nomi di visualizzazione utilizzati per la griglia, i siti e i nodi. È possibile rinominare un singolo elemento, più elementi o anche tutti gli elementi contemporaneamente. La definizione o l'aggiornamento di un nome visualizzato non influisce in alcun modo sulle operazioni StorageGRID.

Prima di iniziare

- Da **Primary Admin Node**, hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

> È possibile aggiungere o aggiornare i nomi visualizzati da un nodo di amministrazione non primario, ma è necessario accedere al nodo di amministrazione primario per scaricare un pacchetto di ripristino.

- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.
- Hai compreso i requisiti e le Best practice per i nomi visualizzati. Vedere "Rinomina griglia, siti e nodi: Panoramica".

Come rinominare la griglia, i siti o i nodi

È possibile rinominare il sistema StorageGRID, uno o più siti o uno o più nodi.

È possibile utilizzare un nome visualizzato precedentemente utilizzato da un nodo diverso, purché il nome non sia un nome visualizzato o un nome di sistema duplicati.

Selezionare gli elementi da rinominare

Per iniziare, selezionare gli elementi che si desidera rinominare.

Fasi

1. Selezionare **MANUTENZIONE** > **attività** > **Rinomina griglia, siti e nodi**.
2. Per il passo **Select Names**, selezionare gli elementi che si desidera rinominare.

Elemento da modificare	Istruzioni
Nomi di tutto (o quasi tutto) nel sistema	a. Selezionare **Seleziona tutto**. b. Se si desidera, deselezionare gli elementi che non si desidera rinominare.
Nome della griglia	Selezionare la casella di controllo della griglia.
Nome di un sito e di alcuni o di tutti i suoi nodi	a. Selezionare la casella di controllo nell'intestazione della tabella per il sito. b. Facoltativamente, deselezionare i nodi che non si desidera rinominare.
Nome di un sito	Selezionare la casella di controllo del sito.
Nome di un nodo	Selezionare la casella di controllo del nodo.

3. Selezionare **continua**.
4. Esaminare la tabella, che include gli elementi selezionati.
   - La colonna **Nome visualizzato** mostra il nome corrente di ciascun elemento. Se l'elemento non è mai stato rinominato, il nome visualizzato corrisponde al nome del sistema.
   - La colonna **Nome sistema** mostra il nome immesso per ciascun elemento durante l'installazione. I nomi di sistema vengono utilizzati per le operazioni StorageGRID interne e non possono essere modificati. Ad esempio, il nome di sistema di un nodo potrebbe essere il nome host.
   - La colonna **Type** indica il tipo di elemento: Grid, Site o il tipo di nodo specifico.

Proporre nuovi nomi

Per il passo **proporre nuovi nomi**, è possibile immettere un nome visualizzato per ciascun elemento singolarmente oppure rinominare gli elementi in blocco.

Rinominare gli elementi singolarmente

Seguire questa procedura per inserire un nome visualizzato per ciascun elemento che si desidera rinominare.

Fasi

1. Nel campo **Display name** (Nome visualizzato), immettere un nome visualizzato per ciascun elemento dell'elenco.

   Vedere "Rinomina griglia, siti e nodi: Panoramica" per conoscere i requisiti di naming.

2. Per rimuovere gli elementi che non si desidera rinominare, selezionare ✕ Nella colonna **Rimuovi dall'elenco**.

   Se non si intende proporre un nuovo nome per un elemento, è necessario rimuoverlo dalla tabella.

3. Una volta proposti nuovi nomi per tutti gli elementi della tabella, selezionare **Rinomina**.

   Viene visualizzato un messaggio di successo. I nuovi nomi visualizzati vengono ora utilizzati in Grid Manager.

Rinominare gli elementi in blocco

Utilizzare lo strumento di ridenominazione in blocco se i nomi degli elementi condividono una stringa comune che si desidera sostituire con una stringa diversa.

Fasi

1. Per il passo **proporre nuovi nomi**, selezionare **Usa lo strumento di ridenominazione in blocco**.

   L'anteprima **Rename (Rinomina)** include tutti gli elementi visualizzati per il passo **Proponi nuovi nomi**. È possibile utilizzare l'anteprima per visualizzare l'aspetto dei nomi visualizzati dopo la sostituzione di una stringa condivisa.

2. Nel campo **existing string**, immettere la stringa condivisa che si desidera sostituire. Ad esempio, se la stringa che si desidera sostituire è `Data-Center-1`, Immettere **Data-Center-1**.

   Durante la digitazione, il testo viene evidenziato ovunque si trovi nei nomi a sinistra.

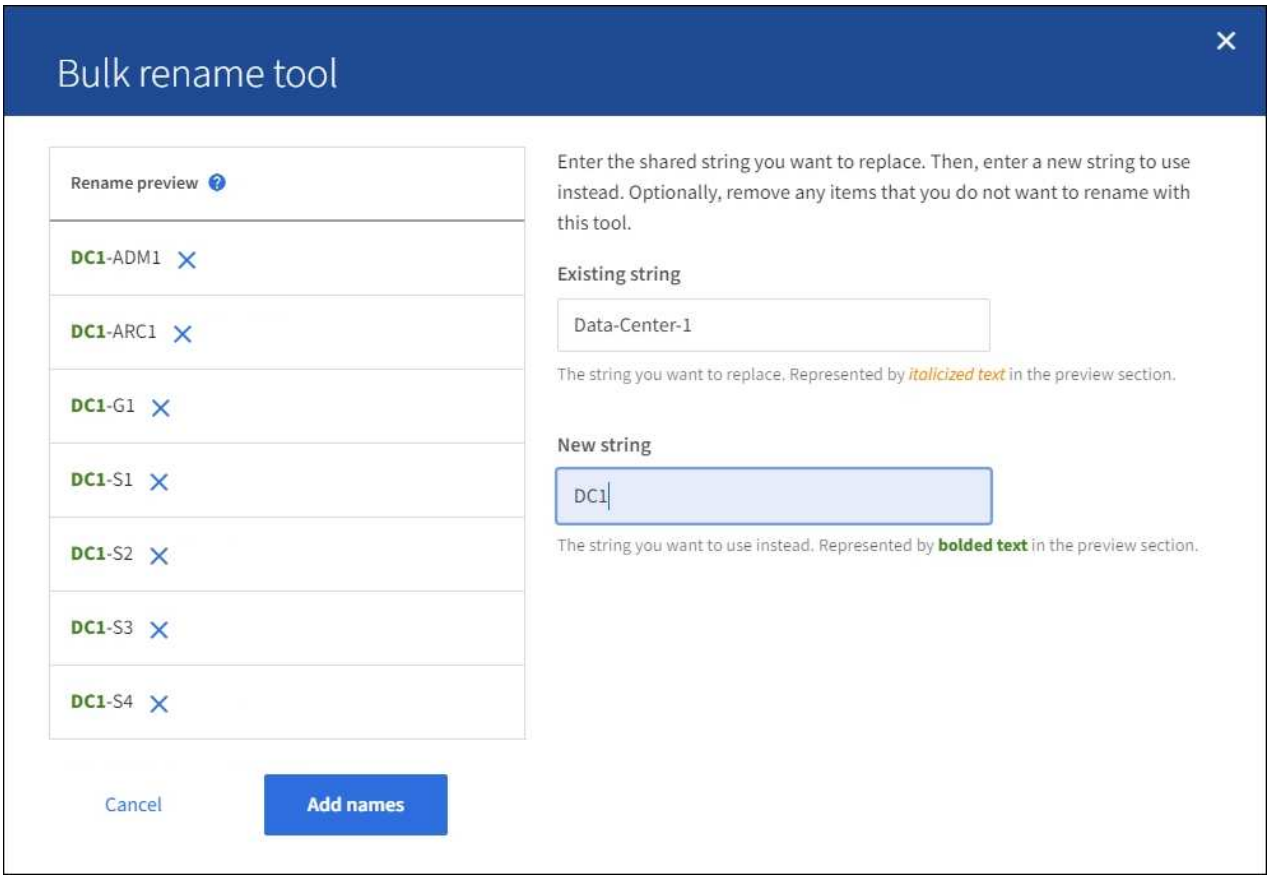
3. Selezionare ✕ per rimuovere gli elementi che non si desidera rinominare con questo strumento.

   Ad esempio, si supponga di voler rinominare tutti i nodi che contengono la stringa `Data-Center-1`, ma non si desidera rinominare `Data-Center-1` sito stesso. Selezionare ✕ per rimuovere il sito dall'anteprima di ridenominazione.

4. Nel campo **New string** (Nuova stringa), immettere la stringa sostitutiva che si desidera utilizzare. Ad esempio, inserire **DC1**.

   Vedere "Rinomina griglia, siti e nodi: Panoramica" per conoscere i requisiti di naming.

   Quando si inserisce la stringa di sostituzione, i nomi a sinistra vengono aggiornati, in modo da verificare che i nuovi nomi siano corretti.



5. Una volta soddisfatti dei nomi visualizzati nell'anteprima, selezionare **Aggiungi nomi** per aggiungere i nomi alla tabella per il passo **proporre nuovi nomi**.
6. Apportare eventuali modifiche aggiuntive richieste oppure selezionare ✕ per rimuovere gli elementi che non si desidera rinominare.
7. Quando si è pronti a rinominare tutti gli elementi della tabella, selezionare **Rinomina**.

   Viene visualizzato un messaggio di successo. I nuovi nomi visualizzati vengono ora utilizzati in Grid Manager.

Scarica il pacchetto di ripristino

Una volta terminata la ridenominazione degli elementi, scaricare e salvare un nuovo pacchetto di ripristino. I nuovi nomi visualizzati per gli elementi rinominati sono inclusi in `Passwords.txt` file.

Fasi

1. Inserire la passphrase di provisioning.
2. Selezionare **Download Recovery Package** (Scarica pacchetto di ripristino).

   Il download viene avviato immediatamente.

3. Al termine del download, aprire `Passwords.txt` per visualizzare il nome del server per tutti i nodi e i nomi visualizzati per tutti i nodi rinominati.
4. Copiare il `sgws-recovery-package-id-revision.zip` archiviare in due posizioni sicure, sicure e separate.

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

5. Selezionare **fine** per tornare al primo passaggio.

Riportare i nomi visualizzati ai nomi di sistema

È possibile ripristinare il nome di sistema originale di una griglia, di un sito o di un nodo rinominato. Quando si ripristina il nome di sistema di un elemento, le pagine di Grid Manager e altre posizioni StorageGRID non mostrano più un **Nome visualizzato** per quell'elemento. Viene visualizzato solo il nome di sistema dell'elemento.

Fasi

1. Selezionare **MANUTENZIONE** > **attività** > **Rinomina griglia, siti e nodi**.
2. Per il passo **Select Names**, selezionare gli elementi che si desidera ripristinare ai nomi di sistema.
3. Selezionare **continua**.
4. Per il passo **proporre nuovi nomi**, ripristinare i nomi visualizzati in nomi di sistema singolarmente o in blocco.

Ripristinare i nomi di sistema singolarmente

a. Copiare il nome di sistema originale di ciascun elemento e incollarlo nel campo **Display name** (Nome visualizzato) oppure selezionare ✕ per rimuovere gli elementi che non si desidera ripristinare.

   Per ripristinare un nome visualizzato, il nome del sistema deve essere visualizzato nel campo **Nome visualizzato**, ma il nome non fa distinzione tra maiuscole e minuscole.

b. Selezionare **Rinomina**.

   Viene visualizzato un messaggio di successo. I nomi visualizzati per questi elementi non vengono più utilizzati.

Ripristinare i nomi di sistema in blocco

a. Per il passo **proporre nuovi nomi**, selezionare **Usa lo strumento di ridenominazione in blocco**.
b. Nel campo **existing string**, immettere la stringa del nome da sostituire.
c. Nel campo **New string**, immettere la stringa del nome di sistema che si desidera utilizzare.
d. Selezionare **Aggiungi nomi** per aggiungere i nomi alla tabella per il passo **proporre nuovi nomi**.
e. Verificare che ogni voce nel campo **Display name** corrisponda al nome nel campo **System name**. Apportare modifiche o selezionare ✕ per rimuovere gli elementi che non si desidera ripristinare.

   Per ripristinare un nome visualizzato, il nome del sistema deve essere visualizzato nel campo **Nome visualizzato**, ma il nome non fa distinzione tra maiuscole e minuscole.

f. Selezionare **Rinomina**.

   Viene visualizzato un messaggio di successo. I nomi visualizzati per questi elementi non vengono più utilizzati.

5. Scaricare e salvare un nuovo pacchetto di ripristino.

   I nomi visualizzati per gli elementi ripristinati non sono più inclusi in `Passwords.txt` file.

Procedure dei nodi

Procedure dei nodi: Panoramica

Potrebbe essere necessario eseguire procedure di manutenzione relative a specifici nodi di rete o servizi di nodi.

Procedure di Server Manager

Server Manager viene eseguito su ogni nodo grid per supervisionare l'avvio e l'arresto dei servizi e per garantire che i servizi si uniscano e abbandonino correttamente il sistema StorageGRID. Server Manager monitora inoltre i servizi su ogni nodo grid e tenta automaticamente di riavviare tutti i servizi che segnalano gli errori.

Per eseguire le procedure di Server Manager, in genere è necessario accedere alla riga di comando del nodo.

> L'accesso a Server Manager deve essere effettuato solo se il supporto tecnico lo ha richiesto.

> Al termine dell'operazione con Server Manager, chiudere la sessione corrente della shell dei comandi e disconnettersi. Inserire: `exit`

Procedure di riavvio, spegnimento e alimentazione del nodo

Queste procedure vengono utilizzate per riavviare uno o più nodi, per arrestare e riavviare i nodi o per spegnere e riaccendere i nodi.

Procedure di rimappamento delle porte

È possibile utilizzare le procedure di rimappamento delle porte per rimuovere i rimappamenti delle porte da un nodo, ad esempio, se si desidera configurare un endpoint di bilanciamento del carico utilizzando una porta precedentemente rimappata.

Procedure di Server Manager

Visualizzare lo stato e la versione di Server Manager

Per ciascun nodo Grid, è possibile visualizzare lo stato e la versione correnti di Server Manager in esecuzione su tale nodo Grid. È inoltre possibile ottenere lo stato corrente di tutti i servizi in esecuzione su quel nodo della griglia.

Prima di iniziare

Hai il `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Visualizzare lo stato corrente di Server Manager in esecuzione sul nodo grid: **`service servermanager status`**

   Viene riportato lo stato corrente di Server Manager in esecuzione sul nodo grid (in esecuzione o meno). Se lo stato di Server Manager è `running`, l'ora in cui è stato eseguito dall'ultimo avvio. Ad esempio:

   ```
   servermanager running for 1d, 13h, 0m, 30s
   ```

3. Visualizzare la versione corrente di Server Manager in esecuzione su un nodo Grid: **`service`**

servermanager version

Viene visualizzata la versione corrente. Ad esempio:

```
11.1.0-20180425.1905.39c9493
```

4. Disconnettersi dalla shell dei comandi: **exit**

Visualizzare lo stato corrente di tutti i servizi

È possibile visualizzare lo stato corrente di tutti i servizi in esecuzione su un nodo Grid in qualsiasi momento.

Prima di iniziare

Hai il `Passwords.txt` file.

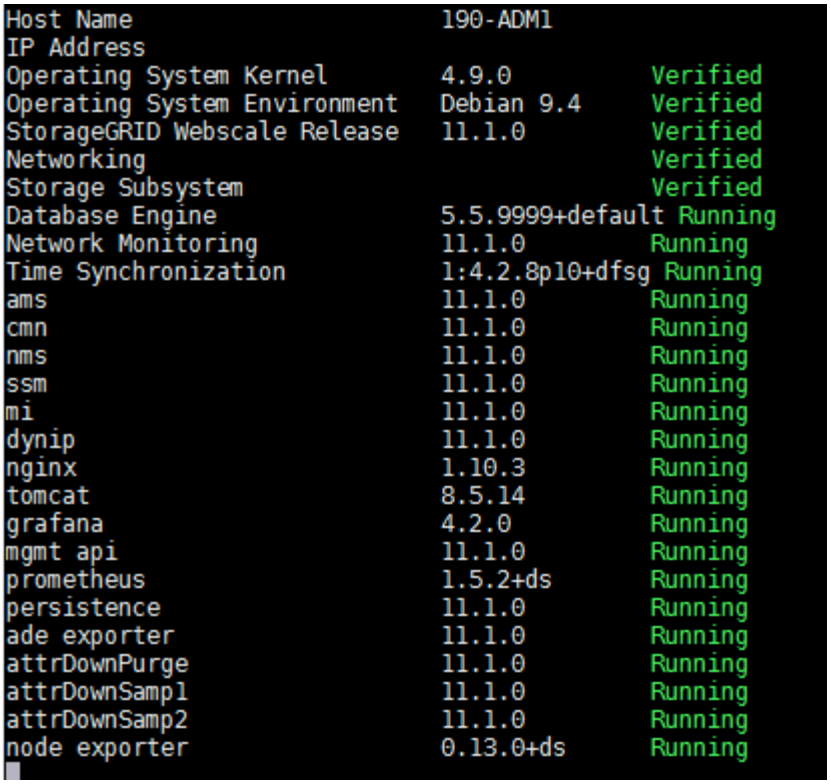
Fasi

1. Accedere al nodo Grid:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo grid: `storagegrid-status`

   Ad esempio, l'output per il nodo di amministrazione primario mostra lo stato corrente dei servizi AMS, CMN e NMS in esecuzione. Questo output viene aggiornato immediatamente se lo stato di un servizio cambia.



3. Tornare alla riga di comando, premere **Ctrl**+**C**.
4. Se si desidera, visualizzare un report statico per tutti i servizi in esecuzione sul nodo Grid: `/usr/local/servermanager/reader.rb`

   Questo report include le stesse informazioni del report continuamente aggiornato, ma non viene aggiornato se lo stato di un servizio cambia.

5. Disconnettersi dalla shell dei comandi: `exit`

Avviare Server Manager e tutti i servizi

Potrebbe essere necessario avviare Server Manager, che avvia anche tutti i servizi sul nodo Grid.

Prima di iniziare

Hai il `Passwords.txt` file.

A proposito di questa attività

L'avvio di Server Manager su un nodo grid in cui è già in esecuzione comporta il riavvio di Server Manager e di tutti i servizi sul nodo grid.

Fasi

1. Accedere al nodo Grid:

   a. Immettere il seguente comando: `ssh admin@`*`grid_node_IP`*

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Avviare Server Manager: `service servermanager start`
3. Disconnettersi dalla shell dei comandi: `exit`

Riavviare Server Manager e tutti i servizi

Potrebbe essere necessario riavviare il server manager e tutti i servizi in esecuzione su un nodo grid.

Prima di iniziare

Hai il `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Riavviare Server Manager e tutti i servizi sul nodo grid: `service servermanager restart`

   Server Manager e tutti i servizi sul nodo grid vengono arrestati e quindi riavviati.

   > Utilizzando il `restart` il comando è identico a quello utilizzato da `stop` seguito dal comando `start` comando.

3. Disconnettersi dalla shell dei comandi: `exit`

Arrestare Server Manager e tutti i servizi

Server Manager è progettato per essere eseguito in qualsiasi momento, ma potrebbe essere necessario interrompere Server Manager e tutti i servizi in esecuzione su un nodo grid.

Prima di iniziare

Hai il `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

c. Immettere il seguente comando per passare a root: `su -`

d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Arrestare Server Manager e tutti i servizi in esecuzione sul nodo grid: `service servermanager stop`

   Server Manager e tutti i servizi in esecuzione sul nodo grid vengono terminati senza problemi. L'arresto dei servizi può richiedere fino a 15 minuti.

3. Disconnettersi dalla shell dei comandi: `exit`

Visualizzare lo stato corrente del servizio

È possibile visualizzare lo stato corrente di un servizio in esecuzione su un nodo Grid in qualsiasi momento.

Prima di iniziare

Hai il `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Visualizzare lo stato corrente di un servizio in esecuzione su un nodo griglia: `**service *servicename* status**` Viene riportato lo stato corrente del servizio richiesto in esecuzione sul nodo della griglia (in esecuzione o meno). Ad esempio:

   ```
   cmn running for 1d, 14h, 21m, 2s
   ```

3. Disconnettersi dalla shell dei comandi: **`exit`**

Interrompere il servizio

Alcune procedure di manutenzione richiedono l'interruzione di un singolo servizio mantenendo in esecuzione altri servizi sul nodo grid. Interrompere i singoli servizi solo quando richiesto da una procedura di manutenzione.

Prima di iniziare

Hai il `Passwords.txt` file.

A proposito di questa attività

Quando si utilizza questa procedura per "arrestare amministrativamente" un servizio, Server Manager non riavvia automaticamente il servizio. È necessario avviare il servizio singolo manualmente o riavviare Server Manager.

Se è necessario arrestare il servizio LDR su un nodo di storage, tenere presente che potrebbe essere necessario un po' di tempo per arrestare il servizio in presenza di connessioni attive.

Fasi

1. Accedere al nodo Grid:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
2. Interruzione di un singolo servizio: `service servicename stop`

   Ad esempio:

   ```
   service ldr stop
   ```

   L'interruzione dei servizi può richiedere fino a 11 minuti.
3. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

"Forzare l'interruzione del servizio"

Forzare l'interruzione del servizio

Se è necessario interrompere immediatamente un servizio, è possibile utilizzare `force-stop` comando.

Prima di iniziare

Hai il `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Forzare manualmente l'interruzione del servizio: `service servicename force-stop`

   Ad esempio:

   ```
   service ldr force-stop
   ```

   Il sistema attende 30 secondi prima di terminare il servizio.

3. Disconnettersi dalla shell dei comandi: `exit`

Avviare o riavviare il servizio

Potrebbe essere necessario avviare un servizio che è stato arrestato oppure arrestare e riavviare un servizio.

Prima di iniziare

Hai il `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Decidere quale comando emettere, in base al fatto che il servizio sia attualmente in esecuzione o interrotto.

   - Se il servizio è attualmente arrestato, utilizzare `start` comando per avviare il servizio manualmente: `service servicename start`

     Ad esempio:

     ```
     service ldr start
     ```

   - Se il servizio è in esecuzione, utilizzare `restart` comando per arrestare e riavviare il servizio: `service servicename restart`

     Ad esempio:

```
service ldr restart
```

+

Utilizzando il `restart` il comando è identico a quello utilizzato da `stop` seguito dal comando `start` comando. È possibile che si verifici problemi `restart` anche se il servizio è attualmente arrestato.

3. Disconnettersi dalla shell dei comandi: `exit`

Utilizzare un file DoNotStart

Se si eseguono diverse procedure di manutenzione o configurazione sotto la direzione del supporto tecnico, potrebbe essere richiesto di utilizzare un file DoNotStart per impedire l'avvio dei servizi all'avvio o al riavvio di Server Manager.

Aggiungere o rimuovere un file DoNotStart solo se richiesto dal supporto tecnico.

Per impedire l'avvio di un servizio, inserire un file DoNotStart nella directory del servizio che si desidera impedire l'avvio. All'avvio, Server Manager cerca il file DoNotStart. Se il file è presente, non è possibile avviare il servizio (e i servizi da esso dipendenti). Quando il file DoNotStart viene rimosso, il servizio precedentemente interrotto viene avviato al successivo avvio o riavvio di Server Manager. I servizi non vengono avviati automaticamente quando il file DoNotStart viene rimosso.

Il modo più efficiente per impedire il riavvio di tutti i servizi consiste nell'impedire l'avvio del servizio NTP. Tutti i servizi dipendono dal servizio NTP e non possono essere eseguiti se il servizio NTP non è in esecuzione.

Aggiungere il file DoNotStart per il servizio

È possibile impedire l'avvio di un singolo servizio aggiungendo un file DoNotStart alla directory del servizio su un nodo Grid.

Prima di iniziare

Hai il `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Aggiunta di un file DoNotStart: `touch /etc/sv/service/DoNotStart`

   dove `service` indica il nome del servizio che non può essere avviato. Ad esempio,

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   Viene creato un file DoNotStart. Non è necessario alcun contenuto di file.

Al riavvio di Server Manager o del nodo grid, Server Manager viene riavviato, ma il servizio non viene attivato.

3. Disconnettersi dalla shell dei comandi: `exit`

Rimuovere il file DoNotStart per l'assistenza

Quando si rimuove un file DoNotStart che impedisce l'avvio di un servizio, è necessario avviarlo.

Prima di iniziare

Hai il `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Rimuovere il file DoNotStart dalla directory di servizio: `rm /etc/sv/service/DoNotStart`

   dove `service` è il nome del servizio. Ad esempio,

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. Avviare il servizio: `service servicename start`
4. Disconnettersi dalla shell dei comandi: `exit`

Risolvere i problemi di Server Manager

Se si verifica un problema durante l'utilizzo di Server Manager, controllare il file di log.

I messaggi di errore relativi a Server Manager vengono acquisiti nel file di log di Server Manager, che si trova all'indirizzo: `/var/local/log/servermanager.log`

Controllare questo file per i messaggi di errore relativi agli errori. Se necessario, inoltrare il problema al supporto tecnico. Potrebbe essere richiesto di inoltrare i file di registro al supporto tecnico.

Servizio con stato di errore

Se si rileva che un servizio è entrato in uno stato di errore, tentare di riavviare il servizio.

Prima di iniziare

Hai il `Passwords.txt` file.

A proposito di questa attività

Server Manager monitora i servizi e riavvia quelli che si sono arrestati inaspettatamente. Se un servizio non riesce, Server Manager tenta di riavviarlo. Se si verificano tre tentativi non riusciti di avvio di un servizio entro cinque minuti, il servizio entra in uno stato di errore. Server Manager non tenta un altro riavvio.

Fasi

1. Accedere al nodo Grid:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Confermare lo stato di errore del servizio: `service servicename status`

   Ad esempio:

   ```
   service ldr status
   ```

   Se il servizio si trova in uno stato di errore, viene visualizzato il seguente messaggio: `servicename in error state`. Ad esempio:

   ```
   ldr in error state
   ```

   > Se lo stato del servizio è `disabled`, consultare le istruzioni per "Rimozione di un file DoNotStart per un servizio".

3. Tentare di rimuovere lo stato di errore riavviando il servizio: `service servicename restart`

   Se il servizio non viene riavviato, contattare il supporto tecnico.

4. Disconnettersi dalla shell dei comandi: `exit`

Procedure di riavvio, spegnimento e alimentazione

Eseguire un riavvio a rotazione

È possibile eseguire un riavvio in sequenza per riavviare più nodi grid senza causare un'interruzione del servizio.

Prima di iniziare

- Si è effettuato l'accesso al Grid Manager sul nodo amministrativo principale e si sta utilizzando un "browser web supportato".

  > Per eseguire questa procedura, è necessario aver effettuato l'accesso al nodo amministrativo primario.

- Hai il "Autorizzazione di manutenzione o di accesso root".

A proposito di questa attività

Utilizzare questa procedura se è necessario riavviare più nodi contemporaneamente. Ad esempio, è possibile utilizzare questa procedura dopo aver modificato la modalità FIPS per le griglie "Criteri di sicurezza TLS e SSH". Quando la modalità FIPS cambia, è necessario riavviare tutti i nodi per rendere effettiva la modifica.

È possibile riavviare un solo nodo "Riavviare il nodo dalla scheda Tasks (attività)".

Quando StorageGRID riavvia i nodi della griglia, emette il `reboot` su ogni nodo, che causa l'arresto e il riavvio del nodo. Tutti i servizi vengono riavviati automaticamente.

- Il riavvio di un nodo VMware riavvia la macchina virtuale.
- Il riavvio di un nodo Linux riavvia il contenitore.
- Il riavvio di un nodo dell'appliance StorageGRID riavvia il controller di elaborazione.

La procedura di riavvio in sequenza può riavviare più nodi contemporaneamente, con le seguenti eccezioni:

- Due nodi dello stesso tipo non verranno riavviati contemporaneamente.
- I nodi gateway e i nodi amministrativi non verranno riavviati contemporaneamente.
- I nodi storage e i nodi archivio non verranno riavviati contemporaneamente.

Al contrario, questi nodi vengono riavviati in sequenza per garantire che i gruppi di ha, i dati degli oggetti e i servizi dei nodi critici rimangano sempre disponibili.

Quando si riavvia il nodo amministrativo primario, il browser perde temporaneamente l'accesso al Grid Manager, quindi non è più possibile monitorare la procedura. Per questo motivo, il nodo amministrativo primario viene riavviato per ultimo.

Eseguire un riavvio a rotazione

Selezionare i nodi che si desidera riavviare, rivedere le selezioni, avviare la procedura di riavvio e monitorare l'avanzamento.

Selezionare nodi

Come primo passo, accedere alla pagina di riavvio in sequenza e selezionare i nodi che si desidera riavviare.

Fasi

1. Selezionare **MANUTENZIONE** > **attività** > **riavvio in sequenza**.
2. Esaminare le icone di stato della connessione e di avviso nella colonna **Nome nodo**.

   Non è possibile riavviare un nodo se è disconnesso dalla griglia. Le caselle di controllo sono disattivate per i nodi con queste icone: oppure .

3. Se in un nodo sono presenti avvisi attivi, esaminare l'elenco degli avvisi nella colonna **Riepilogo avvisi**.

   Per visualizzare tutti gli avvisi correnti per un nodo, è anche possibile selezionare **Nodi › scheda Panoramica**.

4. Facoltativamente, eseguire le azioni consigliate per risolvere eventuali avvisi correnti.
5. Facoltativamente, se tutti i nodi sono connessi e si desidera riavviarli tutti, selezionare la casella di controllo nell'intestazione della tabella e selezionare **Seleziona tutto**. In caso contrario, selezionare ciascun nodo che si desidera riavviare.

   È possibile utilizzare le opzioni di filtro della tabella per visualizzare i sottogruppi di nodi. Ad esempio, è possibile visualizzare e selezionare solo nodi di archiviazione o tutti i nodi di un determinato sito.

6. Selezionare **Rivedi selezione**.

Selezione di revisione

In questo passaggio, è possibile determinare il tempo necessario per la procedura di riavvio totale e confermare di aver selezionato i nodi corretti.

1. Nella pagina di selezione Revisione, esaminare il Riepilogo, che indica il numero di nodi che verranno riavviati e il tempo totale stimato per il riavvio di tutti i nodi.
2. Se si desidera, per rimuovere un nodo specifico dall'elenco di riavvio, selezionare **Rimuovi**.
3. In alternativa, per aggiungere altri nodi, selezionare **passaggio precedente**, selezionare i nodi aggiuntivi e selezionare **selezione revisione**.
4. Quando si è pronti ad avviare la procedura di riavvio in sequenza per tutti i nodi selezionati, selezionare **Reboot Node** (Riavvia nodi).
5. Se si è scelto di riavviare il nodo amministrativo primario, leggere il messaggio informativo e selezionare **Sì**.

> Il nodo amministrativo primario sarà l'ultimo nodo da riavviare. Durante il riavvio di questo nodo, la connessione del browser andrà persa. Quando il nodo amministrativo primario è nuovamente disponibile, è necessario ricaricare la pagina di riavvio in sequenza.

Monitorare un riavvio continuo

Durante l'esecuzione della procedura di riavvio in sequenza, è possibile monitorarla dal nodo amministrativo principale.

Fasi

1. Esaminare lo stato di avanzamento generale dell'operazione, che include le seguenti informazioni:
   - Numero di nodi riavviati
   - Numero di nodi in corso di riavvio
   - Numero di nodi che devono ancora essere riavviati
2. Esaminare la tabella per ciascun tipo di nodo.

   Le tabelle forniscono una barra di avanzamento dell'operazione su ciascun nodo e mostrano la fase di riavvio per quel nodo, che può essere una delle seguenti:

   - In attesa del riavvio
   - Interruzione dei servizi
   - Riavvio del sistema in corso
   - Avvio dei servizi

- Riavvio completato

Interrompere la procedura di riavvio in sequenza

È possibile interrompere la procedura di riavvio in sequenza dal nodo amministrativo primario. Quando si arresta la procedura, qualsiasi nodo che abbia lo stato "arresto dei servizi", "riavvio del sistema" o "avvio dei servizi" completerà l'operazione di riavvio. Tuttavia, questi nodi non saranno più registrati come parte della procedura.

Fasi

1. Selezionare **MANUTENZIONE** > **attività** > **riavvio in sequenza**.
2. Dal passaggio **Monitor reboot** (riavvio monitor), selezionare **Stop reboot procedure** (Interrompi procedura di riavvio).

Riavviare il nodo della griglia dalla scheda attività

È possibile riavviare un singolo nodo della griglia dalla scheda attività della pagina nodi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.
- Se si sta riavviando il nodo amministrativo primario o qualsiasi nodo di storage, sono state esaminate le seguenti considerazioni:
  - Quando si riavvia il nodo amministrativo primario, il browser perde temporaneamente l'accesso al Grid Manager.
  - Se si riavviano due o più nodi di archiviazione in un determinato sito, potrebbe non essere possibile accedere a determinati oggetti per la durata del riavvio. Questo problema può verificarsi se una regola ILM utilizza l'opzione di acquisizione **Dual Commit** (o una regola specifica **Balanced** e non è possibile creare immediatamente tutte le copie richieste). In questo caso, StorageGRID assegna gli oggetti appena acquisiti a due nodi storage nello stesso sito e valuta l'ILM in un secondo momento.
  - Per garantire l'accesso a tutti gli oggetti durante il riavvio di un nodo di storage, interrompere l'acquisizione di oggetti in un sito per circa un'ora prima di riavviare il nodo.

A proposito di questa attività

Quando StorageGRID riavvia un nodo griglia, emette il `reboot` comando sul nodo, che causa l'arresto e il riavvio del nodo. Tutti i servizi vengono riavviati automaticamente.

- Il riavvio di un nodo VMware riavvia la macchina virtuale.
- Il riavvio di un nodo Linux riavvia il contenitore.
- Il riavvio di un nodo dell'appliance StorageGRID riavvia il controller di elaborazione.

> Se è necessario riavviare più di un nodo, è possibile utilizzare "procedura di riavvio in sequenza".

Fasi

1. Selezionare **NODI**.
2. Selezionare il nodo della griglia che si desidera riavviare.

3. Selezionare la scheda **Tasks**.
4. Selezionare **Reboot** (Riavvia).

   Viene visualizzata una finestra di dialogo di conferma. Se si sta riavviando il nodo di amministrazione primario, la finestra di dialogo di conferma ricorda che la connessione del browser a Grid Manager viene temporaneamente persa quando i servizi vengono arrestati.

5. Inserire la passphrase di provisioning e selezionare **OK**.
6. Attendere il riavvio del nodo.

   L'arresto dei servizi potrebbe richiedere del tempo.

   Quando il nodo viene riavviato, viene visualizzata l'icona grigia (amministrativamente giù) per il nodo nella pagina nodi. Quando tutti i servizi sono stati riavviati e il nodo è collegato correttamente alla griglia, la pagina dei nodi dovrebbe visualizzare lo stato normale (nessuna icona a sinistra del nome del nodo), indicando che non sono attivi avvisi e che il nodo è connesso alla griglia.

Riavviare il nodo Grid dalla shell dei comandi

Se è necessario monitorare più da vicino l'operazione di riavvio o se non si riesce ad accedere a Grid Manager, è possibile accedere al nodo Grid ed eseguire il comando di riavvio di Server Manager dalla shell dei comandi.

Prima di iniziare

Hai il `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Facoltativamente, interrompere i servizi: `service servermanager stop`

   L'interruzione dei servizi è un passaggio facoltativo, ma consigliato. L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto prima di riavviare il nodo nella fase successiva.

3. Riavviare il nodo Grid: `reboot`
4. Disconnettersi dalla shell dei comandi: `exit`

Chiudere il nodo della griglia

È possibile chiudere un nodo Grid dalla shell dei comandi del nodo.

Prima di iniziare

- Hai il `Passwords.txt` file.

A proposito di questa attività

Prima di eseguire questa procedura, esaminare le seguenti considerazioni:

- In generale, non è necessario spegnere più di un nodo alla volta per evitare interruzioni.
- Non spegnere un nodo durante una procedura di manutenzione, a meno che non venga espressamente richiesto dalla documentazione o dal supporto tecnico.
- Il processo di shutdown si basa sulla posizione in cui è installato il nodo, come segue:
  - L'arresto di un nodo VMware arresta la macchina virtuale.
  - L'arresto di un nodo Linux arresta il container.
  - L'arresto di un nodo appliance StorageGRID arresta il controller di calcolo.
- Se si prevede di chiudere più di un nodo di storage in un sito, interrompere l'acquisizione di oggetti in quel sito per circa un'ora prima di spegnere i nodi.

  Se una regola ILM utilizza l'opzione di acquisizione **doppio commit** (o se una regola utilizza l'opzione **bilanciato** e non è possibile creare immediatamente tutte le copie richieste), StorageGRID commuta immediatamente gli oggetti appena acquisiti su due nodi di storage sullo stesso sito e valuta ILM in un secondo momento. Se più di un nodo di storage in un sito viene arrestato, potrebbe non essere possibile accedere agli oggetti appena acquisiti per la durata della chiusura. Anche le operazioni di scrittura potrebbero non riuscire se nel sito rimangono disponibili troppi nodi di storage. Vedere "Gestire gli oggetti con ILM".

Fasi

1. Accedere al nodo Grid:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Arrestare tutti i servizi: `service servermanager stop`

   L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto.

3. Se il nodo è in esecuzione su una macchina virtuale VMware o si tratta di un nodo appliance, eseguire il comando shutdown: `shutdown -h now`

   Eseguire questa operazione indipendentemente dal risultato dell' `service servermanager stop` comando.

   > Dopo aver eseguito il `shutdown -h now` su un nodo appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

   Per l'appliance, questo comando spegne il controller, ma l'appliance è ancora accesa. Completare la fase successiva.

4. Se si sta spegnendo un nodo appliance, seguire la procedura relativa all'appliance.

SG6160

a. Spegnere il controller di storage SG6100-CN.
b. Attendere lo spegnimento del LED di alimentazione blu sul controller di archiviazione SG6100-CN.

SGF6112

a. Spegnere l'apparecchio.
b. Attendere che il LED di alimentazione blu si spenga.

SG6000

a. Attendere che il LED verde cache Active (cache attiva) sul retro dei controller dello storage si spenga.

   Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

b. Spegnere l'apparecchio e attendere che il LED di alimentazione blu si spenga.

SG5800

a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

   Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

b. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
c. Confermare che tutte le operazioni sono state completate prima di passare alla fase successiva.
d. Spegnere entrambi gli interruttori di alimentazione sul ripiano del controller e attendere lo spegnimento di tutti i LED sul ripiano del controller.

SG5700

a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

   Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

b. Spegnere l'apparecchio e attendere che il LED e il display a sette segmenti si interrompano.

SG100 o SG1000

a. Spegnere l'apparecchio.
b. Attendere che il LED di alimentazione blu si spenga.

Spegnere l'host

Prima di spegnere un host, è necessario interrompere i servizi su tutti i nodi della rete su tale host.

Fasi

1. Accedere al nodo Grid:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Arrestare tutti i servizi in esecuzione sul nodo: `service servermanager stop`

   L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto.

3. Ripetere i passaggi 1 e 2 per ciascun nodo dell'host.
4. Se si dispone di un host Linux:

   a. Accedere al sistema operativo host.

   b. Arrestare il nodo: `storagegrid node stop`

   c. Arrestare il sistema operativo host.

5. Se il nodo è in esecuzione su una macchina virtuale VMware o si tratta di un nodo appliance, eseguire il comando shutdown: `shutdown -h now`

   Eseguire questa operazione indipendentemente dal risultato dell' `service servermanager stop` comando.

   > Dopo aver eseguito il `shutdown -h now` su un nodo appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

   Per l'appliance, questo comando spegne il controller, ma l'appliance è ancora accesa. Completare la fase successiva.

6. Se si sta spegnendo un nodo appliance, seguire la procedura relativa all'appliance.

SG6160

a. Spegnere il controller di storage SG6100-CN.

b. Attendere lo spegnimento del LED di alimentazione blu sul controller di archiviazione SG6100-CN.

SGF6112

a. Spegnere l'apparecchio.

b. Attendere che il LED di alimentazione blu si spenga.

SG6000

a. Attendere che il LED verde cache Active (cache attiva) sul retro dei controller dello storage si spenga.

   Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

b. Spegnere l'apparecchio e attendere che il LED di alimentazione blu si spenga.

SG5800

a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

   Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

b. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.

c. Confermare che tutte le operazioni sono state completate prima di passare alla fase successiva.

d. Spegnere entrambi gli interruttori di alimentazione sul ripiano del controller e attendere lo spegnimento di tutti i LED sul ripiano del controller.

SG5700

a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

   Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

b. Spegnere l'apparecchio e attendere che il LED e il display a sette segmenti si interrompano.

SG110 o SG1100

a. Spegnere l'apparecchio.

b. Attendere che il LED di alimentazione blu si spenga.

SG100 o SG1000

a. Spegnere l'apparecchio.

b. Attendere che il LED di alimentazione blu si spenga.

7. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

"Appliance di storage SGF6112 e SG6160"

"Appliance di storage SG6000"

"SG5800 appliance di storage"

"SG5700 appliance di storage"

"Appliance per i servizi SG110 e SG1100"

"Appliance di servizi SG100 e SG1000"

Spegnere e riaccendere tutti i nodi della rete

Potrebbe essere necessario spegnere l'intero sistema StorageGRID, ad esempio, se si sta spostando un data center. Questi passaggi forniscono una panoramica di alto livello della sequenza consigliata per l'esecuzione di uno shutdown e di un startup controllati.

Quando si spengono tutti i nodi di un sito o di una griglia, non sarà possibile accedere agli oggetti acquisiti mentre i nodi di storage sono offline.

Arrestare i servizi e chiudere i nodi di rete

Prima di spegnere un sistema StorageGRID, è necessario arrestare tutti i servizi in esecuzione su ciascun nodo di rete e quindi arrestare tutte le macchine virtuali VMware, i motori di container e le appliance StorageGRID.

A proposito di questa attività

Arrestare prima i servizi sui nodi Admin e Gateway, quindi arrestare i servizi sui nodi Storage.

Questo approccio consente di utilizzare l'Admin Node primario per monitorare lo stato degli altri nodi della griglia il più a lungo possibile.

> Se un singolo host include più di un nodo di griglia, non spegnere l'host fino a quando non sono stati arrestati tutti i nodi su tale host. Se l'host include il nodo di amministrazione primario, arrestare l'host per ultimo.

> Se necessario, è possibile "Migrare i nodi da un host Linux a un altro" per eseguire la manutenzione degli host senza influire sulle funzionalità o sulla disponibilità del grid.

Fasi

1. Impedire a tutte le applicazioni client di accedere alla griglia.
2. Accedi a ciascun nodo gateway:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

3. Arresta tutti i servizi in esecuzione sul nodo: `service servermanager stop`

   L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto.

4. Ripetere i due passaggi precedenti per arrestare i servizi su tutti i nodi di storage, i nodi di archivio e i nodi di amministrazione non primari.

   È possibile interrompere i servizi su questi nodi in qualsiasi ordine.

   > Se si esegue il `service servermanager stop` Per arrestare i servizi su un nodo di storage dell'appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

5. Per il nodo di amministrazione principale, ripetere i passaggi per accesso al nodo e. interruzione di tutti i servizi sul nodo.
6. Per i nodi in esecuzione su host Linux:
   a. Accedere al sistema operativo host.
   b. Arrestare il nodo: `storagegrid node stop`
   c. Arrestare il sistema operativo host.
7. Per i nodi in esecuzione sulle macchine virtuali VMware e per i nodi di storage dell'appliance, eseguire il comando shutdown: `shutdown -h now`

   Eseguire questa operazione indipendentemente dal risultato dell' `service servermanager stop` comando.

   Per l'appliance, questo comando arresta il controller di calcolo, ma l'appliance è ancora accesa. Completare la fase successiva.

8. Se si dispone di nodi appliance, seguire la procedura relativa all'appliance.

SG110 o SG1100

a. Spegnere l'apparecchio.

b. Attendere che il LED di alimentazione blu si spenga.

SG100 o SG1000

a. Spegnere l'apparecchio.

b. Attendere che il LED di alimentazione blu si spenga.

SG6160

a. Spegnere il controller di storage SG6100-CN.

b. Attendere lo spegnimento del LED di alimentazione blu sul controller di archiviazione SG6100-CN.

SGF6112

a. Spegnere l'apparecchio.

b. Attendere che il LED di alimentazione blu si spenga.

SG6000

a. Attendere che il LED verde cache Active (cache attiva) sul retro dei controller dello storage si spenga.

   Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

b. Spegnere l'apparecchio e attendere che il LED di alimentazione blu si spenga.

SG5800

a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

   Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

b. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.

c. Confermare che tutte le operazioni sono state completate prima di passare alla fase successiva.

d. Spegnere entrambi gli interruttori di alimentazione sul ripiano del controller e attendere lo spegnimento di tutti i LED sul ripiano del controller.

SG5700

a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

   Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

b. Spegnere l'apparecchio e attendere che il LED e il display a sette segmenti si interrompano.

9. Se necessario, disconnettersi dalla shell dei comandi: `exit`

La griglia StorageGRID è stata chiusa.

Avviare i nodi della griglia

> Se l'intero grid è stato spento per più di 15 giorni, è necessario contattare il supporto tecnico prima di avviare qualsiasi grid node. Non tentare di eseguire le procedure di ripristino che ricostruiscono i dati Cassandra. Ciò potrebbe causare la perdita di dati.

Se possibile, accendere i nodi della rete in questo ordine:

- Prima di tutto, alimentare i nodi di amministrazione.
- Alimentare per ultimo i nodi gateway.

> Se un host include più nodi di rete, i nodi torneranno automaticamente in linea all'accensione dell'host.

Fasi

1. Accendere gli host per il nodo di amministrazione primario e tutti i nodi di amministrazione non primari.

   > Non sarà possibile accedere ai nodi di amministrazione fino a quando i nodi di storage non saranno stati riavviati.

2. Accendere gli host per tutti i nodi di archiviazione e i nodi di storage.

   È possibile accendere questi nodi in qualsiasi ordine.

3. Accendere gli host per tutti i nodi gateway.
4. Accedi a Grid Manager.
5. Selezionare **NODI** e monitorare lo stato dei nodi della griglia. Verificare che non siano presenti icone di avviso accanto ai nomi dei nodi.

Informazioni correlate

- "Appliance di storage SGF6112 e SG6160"
- "Appliance per i servizi SG110 e SG1100"
- "Appliance di servizi SG100 e SG1000"
- "Appliance di storage SG6000"
- "SG5800 appliance di storage"
- "SG5700 appliance di storage"

Procedure di rimappamento delle porte

Rimuovere i rimap delle porte

Se si desidera configurare un endpoint per il servizio Load Balancer e si desidera utilizzare una porta che è già stata configurata come porta mappata di un remap di porta, è necessario prima rimuovere il remap di porta esistente, altrimenti l'endpoint non sarà efficace. È necessario eseguire uno script su ciascun nodo Admin e nodo gateway che

dispone di porte remapped in conflitto per rimuovere tutti i remap delle porte del nodo.

A proposito di questa attività

Questa procedura rimuove tutti i rimap delle porte. Se hai bisogno di conservare alcuni rimaps, contatta il supporto tecnico.

Per informazioni sulla configurazione degli endpoint del bilanciamento del carico, vedere "Configurazione degli endpoint del bilanciamento del carico".

> Se il remap della porta fornisce l'accesso al client, riconfigurare il client in modo che utilizzi una porta diversa come endpoint del bilanciamento del carico per evitare la perdita di servizio. In caso contrario, la rimozione del mapping delle porte causerà la perdita dell'accesso al client e dovrebbe essere pianificata in modo appropriato.

> Questa procedura non funziona per un sistema StorageGRID implementato come container su host bare metal. Consultare le istruzioni per "rimozione dei rimaps delle porte sugli host bare metal".

Fasi

1. Accedere al nodo.
   a. Immettere il seguente comando: `ssh -p 8022 admin@node_IP`

      La porta 8022 è la porta SSH del sistema operativo di base, mentre la porta 22 è la porta SSH del motore dei container che esegue StorageGRID.

   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Eseguire il seguente script: `remove-port-remap.sh`
3. Riavviare il nodo: `reboot`
4. Disconnettersi dalla shell dei comandi: `exit`
5. Ripetere questi passaggi su ogni nodo Admin e nodo gateway con porte remapped in conflitto.

Rimuovere i rimaps delle porte sugli host bare metal

Se si desidera configurare un endpoint per il servizio Load Balancer e si desidera utilizzare una porta che è già stata configurata come porta mappata di un remap di porta, è necessario prima rimuovere il remap di porta esistente, altrimenti l'endpoint non sarà efficace.

A proposito di questa attività

Se si esegue StorageGRID su host bare metal, seguire questa procedura invece della procedura generale per rimuovere i rimaps delle porte. È necessario modificare il file di configurazione del nodo per ogni nodo Admin e nodo gateway che ha porte remapped in conflitto per rimuovere tutti i remap delle porte del nodo e riavviare il nodo.

Questa procedura rimuove tutti i rimap delle porte. Se hai bisogno di conservare alcuni rimaps, contatta il supporto tecnico.

Per informazioni sulla configurazione degli endpoint del bilanciamento del carico, vedere le istruzioni per l'amministrazione di StorageGRID.

Questa procedura può causare una perdita temporanea del servizio quando i nodi vengono riavviati.

Fasi

1. Accedere all'host che supporta il nodo. Accedere come root o con un account che dispone dell'autorizzazione sudo.
2. Eseguire il seguente comando per disattivare temporaneamente il nodo: `sudo storagegrid node stop node-name`
3. Utilizzando un editor di testo come vim o pico, modificare il file di configurazione del nodo per il nodo.

   Il file di configurazione del nodo è disponibile all'indirizzo `/etc/storagegrid/nodes/node-name.conf`.

4. Individuare la sezione del file di configurazione del nodo che contiene i rimap delle porte.

   Vedere le ultime due righe nell'esempio seguente.

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. Modificare LE voci PORT_REMAP e PORT_REMAP_INBOUND per rimuovere i rimap delle porte.

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. Eseguire il seguente comando per convalidare le modifiche apportate al file di configurazione del nodo per il nodo: `sudo storagegrid node validate node-name`

   Risolvere eventuali errori o avvisi prima di passare alla fase successiva.

7. Eseguire il seguente comando per riavviare il nodo senza i rimaps delle porte: `sudo storagegrid node start node-name`
8. Accedere al nodo come admin utilizzando la password elencata in `Passwords.txt` file.
9. Verificare che i servizi vengano avviati correttamente.
   a. Visualizzare un elenco degli stati di tutti i servizi sul server:`sudo storagegrid-status`

      Lo stato viene aggiornato automaticamente.

b. Attendere che tutti i servizi abbiano lo stato di in esecuzione o verificato.

c. Uscire dalla schermata di stato: `Ctrl+C`

10. Ripetere questi passaggi su ogni nodo Admin e nodo gateway con porte remapped in conflitto.

Procedure di rete

Aggiornare le subnet per Grid Network

StorageGRID mantiene un elenco delle subnet di rete utilizzate per comunicare tra i nodi della griglia sulla rete (eth0). Queste voci includono le subnet utilizzate per la rete griglia da ciascun sito nel sistema StorageGRID, nonché le subnet utilizzate per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway della rete griglia. Quando si aggiungono nodi griglia o un nuovo sito in un'espansione, potrebbe essere necessario aggiornare o aggiungere sottoreti alla rete Grid.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.
- Si dispone degli indirizzi di rete, in notazione CIDR, delle subnet che si desidera configurare.

A proposito di questa attività

Se si sta eseguendo un'attività di espansione che include l'aggiunta di una nuova subnet, è necessario aggiungere una nuova subnet all'elenco delle subnet Grid Network prima di avviare la procedura di espansione. In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e riavviare l'espansione.

Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete di amministrazione o la rete client di alcun nodo:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Ad esempio, non utilizzare i seguenti intervalli di subnet per la rete Grid, la rete amministrativa o la rete client di alcun nodo:

- 192.168.130.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 198.51.100.2 e 198.51.100.4

Aggiungere una subnet

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **rete griglia**.
2. Selezionare **Aggiungi un'altra subnet** per aggiungere una nuova subnet nella notazione CIDR.

   Ad esempio, immettere `10.96.104.0/22`.

3. Inserire la passphrase di provisioning e selezionare **Save** (Salva).
4. Attendere che le modifiche vengano applicate, quindi scaricare un nuovo pacchetto di ripristino.
   a. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.
   b. Immettere la **Provisioning Passphrase**.

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. Viene inoltre utilizzato per ripristinare il nodo di amministrazione primario.

Le subnet specificate vengono configurate automaticamente per il sistema StorageGRID.

Modificare una subnet

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **rete griglia**.
2. Selezionare la subnet che si desidera modificare e apportare le modifiche necessarie.
3. Inserire la passphrase di provisioning e selezionare **Save** (Salva).
4. Selezionare **Sì** nella finestra di dialogo di conferma.

5. Attendere che le modifiche vengano applicate, quindi scaricare un nuovo pacchetto di ripristino.
   a. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.
   b. Immettere la **Provisioning Passphrase**.

Eliminare una subnet

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **rete griglia**.
2. Selezionare l'icona di eliminazione ✕ accanto alla subnet.
3. Inserire la passphrase di provisioning e selezionare **Save** (Salva).
4. Selezionare **Sì** nella finestra di dialogo di conferma.
5. Attendere che le modifiche vengano applicate, quindi scaricare un nuovo pacchetto di ripristino.
   a. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.
   b. Immettere la **Provisioning Passphrase**.

Configurare gli indirizzi IP

Configure IP addresses (Configura indirizzi IP): Panoramica

È possibile eseguire la configurazione di rete configurando gli indirizzi IP per i nodi della griglia utilizzando lo strumento Change IP (Modifica IP).

È necessario utilizzare lo strumento Change IP per apportare la maggior parte delle modifiche alla configurazione di rete impostata inizialmente durante l'implementazione della griglia. Le modifiche manuali che utilizzano i comandi e i file di rete Linux standard potrebbero non propagarsi a tutti i servizi StorageGRID e non persistere tra gli aggiornamenti, i riavvii o le procedure di ripristino dei nodi.

> La procedura di modifica dell'IP può essere una procedura di interruzione. Alcune parti della griglia potrebbero non essere disponibili fino a quando non viene applicata la nuova configurazione.

> Se si apportano modifiche solo all'elenco subnet di rete griglia, utilizzare Grid Manager per aggiungere o modificare la configurazione di rete. In caso contrario, utilizzare lo strumento Change IP se Grid Manager non è accessibile a causa di un problema di configurazione di rete o se si stanno eseguendo contemporaneamente modifiche al routing Grid Network e altre modifiche di rete.

> Se si desidera modificare l'indirizzo IP Grid Network per tutti i nodi della griglia, utilizzare "procedura speciale per le modifiche a livello di griglia".

Interfacce Ethernet

L'indirizzo IP assegnato a eth0 è sempre l'indirizzo IP Grid Network del nodo Grid. L'indirizzo IP assegnato a eth1 è sempre l'indirizzo IP Admin Network del nodo della griglia. L'indirizzo IP assegnato a eth2 è sempre l'indirizzo IP della rete client del nodo della griglia.

Si noti che su alcune piattaforme, come le appliance StorageGRID, eth0, eth1 ed eth2 potrebbero essere interfacce aggregate composte da bridge o legami subordinati di interfacce fisiche o VLAN. Su queste

piattaforme, la scheda **SSM** > **Resources** potrebbe visualizzare l'indirizzo IP Grid, Admin e Client Network assegnato ad altre interfacce oltre a eth0, eth1 o eth2.

DHCP

È possibile configurare DHCP solo durante la fase di implementazione. Impossibile impostare DHCP durante la configurazione. Se si desidera modificare gli indirizzi IP, le subnet mask e i gateway predefiniti per un nodo griglia, è necessario utilizzare le procedure di modifica dell'indirizzo IP. Utilizzando lo strumento Change IP, gli indirizzi DHCP diventano statici.

Gruppi ad alta disponibilità (ha)

- Se un'interfaccia di rete client è contenuta in un gruppo ha, non è possibile modificare l'indirizzo IP di rete client per tale interfaccia con un indirizzo esterno alla subnet configurata per il gruppo ha.
- Non è possibile modificare l'indirizzo IP della rete client con il valore di un indirizzo IP virtuale esistente assegnato a un gruppo ha configurato sull'interfaccia di rete client.
- Se un'interfaccia di rete Grid è contenuta in un gruppo ha, non è possibile modificare l'indirizzo IP della rete Grid per tale interfaccia con un indirizzo esterno alla subnet configurata per il gruppo ha.
- Non è possibile modificare l'indirizzo IP Grid Network con il valore di un indirizzo IP virtuale esistente assegnato a un gruppo ha configurato sull'interfaccia Grid Network.

Modificare la configurazione di rete del nodo

È possibile modificare la configurazione di rete di uno o più nodi utilizzando lo strumento Change IP. È possibile modificare la configurazione di Grid Network o aggiungere, modificare o rimuovere le reti Admin o Client.

Prima di iniziare

Hai il `Passwords.txt` file.

A proposito di questa attività

Linux: se si aggiunge un nodo Grid alla rete di amministrazione o alla rete client per la prima volta e non si è precedentemente configurato ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET nel file di configurazione del nodo, è necessario farlo ora.

Consultare le istruzioni di installazione di StorageGRID per il sistema operativo Linux in uso:

- "Installare StorageGRID su Red Hat Enterprise Linux"
- "Installare StorageGRID su Ubuntu o Debian"

Appliance: sulle appliance StorageGRID, se il client o la rete amministrativa non sono stati configurati nel programma di installazione dell'appliance StorageGRID durante l'installazione iniziale, la rete non può essere aggiunta utilizzando solo il tool Cambia IP. Innanzitutto, è necessario "impostare l'apparecchio in modalità di manutenzione", Configurare i collegamenti, ripristinare la normale modalità operativa dell'appliance, quindi utilizzare lo strumento Change IP per modificare la configurazione di rete. Vedere "procedura per la configurazione dei collegamenti di rete".

È possibile modificare l'indirizzo IP, la subnet mask, il gateway o il valore MTU per uno o più nodi su qualsiasi rete.

È inoltre possibile aggiungere o rimuovere un nodo da una rete client o da una rete amministrativa:

- È possibile aggiungere un nodo a una rete client o a una rete amministrativa aggiungendo un indirizzo IP/subnet mask su tale rete al nodo.
- È possibile rimuovere un nodo da una rete client o da una rete amministrativa eliminando l'indirizzo IP/subnet mask del nodo sulla rete.

  I nodi non possono essere rimossi dalla Grid Network.

> Non è consentito lo swap degli indirizzi IP. Se è necessario scambiare indirizzi IP tra nodi di rete, è necessario utilizzare un indirizzo IP intermedio temporaneo.

> Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID e si sta modificando l'indirizzo IP di un nodo di amministrazione, tenere presente che qualsiasi trust della parte che si basa configurato utilizzando l'indirizzo IP del nodo di amministrazione (invece del nome di dominio completo, come consigliato) non sarà valido. Non sarà più possibile accedere al nodo. Subito dopo aver modificato l'indirizzo IP, è necessario aggiornare o riconfigurare il trust della parte di supporto del nodo in Active Directory Federation Services (ad FS) con il nuovo indirizzo IP. Consultare le istruzioni per "Configurazione di SSO".

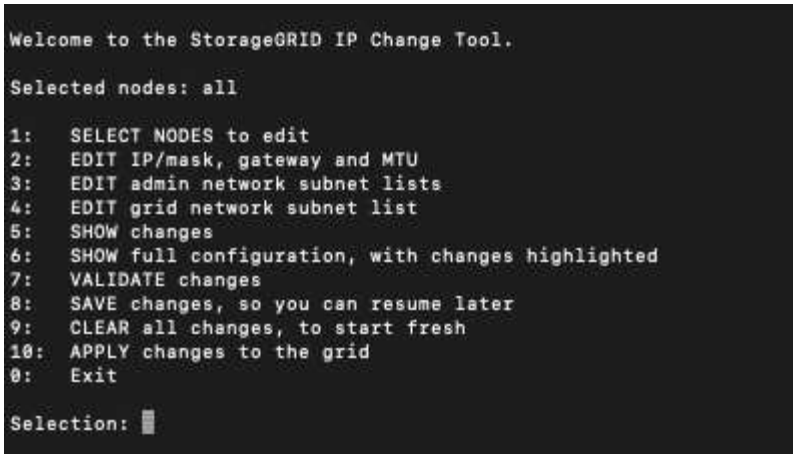
> Le modifiche apportate alla rete utilizzando lo strumento Cambia IP vengono propagate al firmware del programma di installazione delle appliance StorageGRID. In questo modo, se il software StorageGRID viene reinstallato su un'appliance o se un'appliance viene messa in modalità di manutenzione, la configurazione di rete sarà corretta.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
2. Avviare lo strumento Change IP immettendo il seguente comando: `change-ip`
3. Inserire la passphrase di provisioning quando richiesto.

   Viene visualizzato il menu principale.



4. Se si desidera, selezionare **1** per scegliere i nodi da aggiornare. Quindi selezionare una delle seguenti opzioni:

   - **1**: Nodo singolo — selezionare per nome
   - **2**: Nodo singolo — selezionare per sito, quindi per nome
   - **3**: Nodo singolo — selezionare in base all'IP corrente
   - **4**: Tutti i nodi di un sito
   - **5**: Tutti i nodi della griglia

   Nota: se si desidera aggiornare tutti i nodi, lasciare selezionato "tutti".

   Una volta effettuata la selezione, viene visualizzato il menu principale, con il campo **Selected Nodes** (nodi selezionati) aggiornato per riflettere la scelta. Tutte le azioni successive vengono eseguite solo sui nodi visualizzati.

5. Nel menu principale, selezionare l'opzione **2** per modificare le informazioni relative a IP/mask, gateway e MTU per i nodi selezionati.
   a. Selezionare la rete in cui si desidera apportare le modifiche:

      - **1**: Rete di rete
      - **2**: Rete amministrativa
      - **3**: Rete client
      - **4**: Tutte le reti

      Dopo aver effettuato la selezione, il prompt mostra il nome del nodo, il nome della rete (Grid, Admin o Client), il tipo di dati (IP/mask, gateway o MTU) e il valore corrente.

      Se si modificano l'indirizzo IP, la lunghezza del prefisso, il gateway o la MTU di un'interfaccia configurata con DHCP, l'interfaccia diventa statica. Quando si sceglie di modificare un'interfaccia configurata da DHCP, viene visualizzato un avviso per informare l'utente che l'interfaccia passerà a static (statica).

      Interfacce configurate come `fixed` impossibile modificare.

   b. Per impostare un nuovo valore, immetterlo nel formato indicato per il valore corrente.
   c. Per lasciare invariato il valore corrente, premere **Invio**.

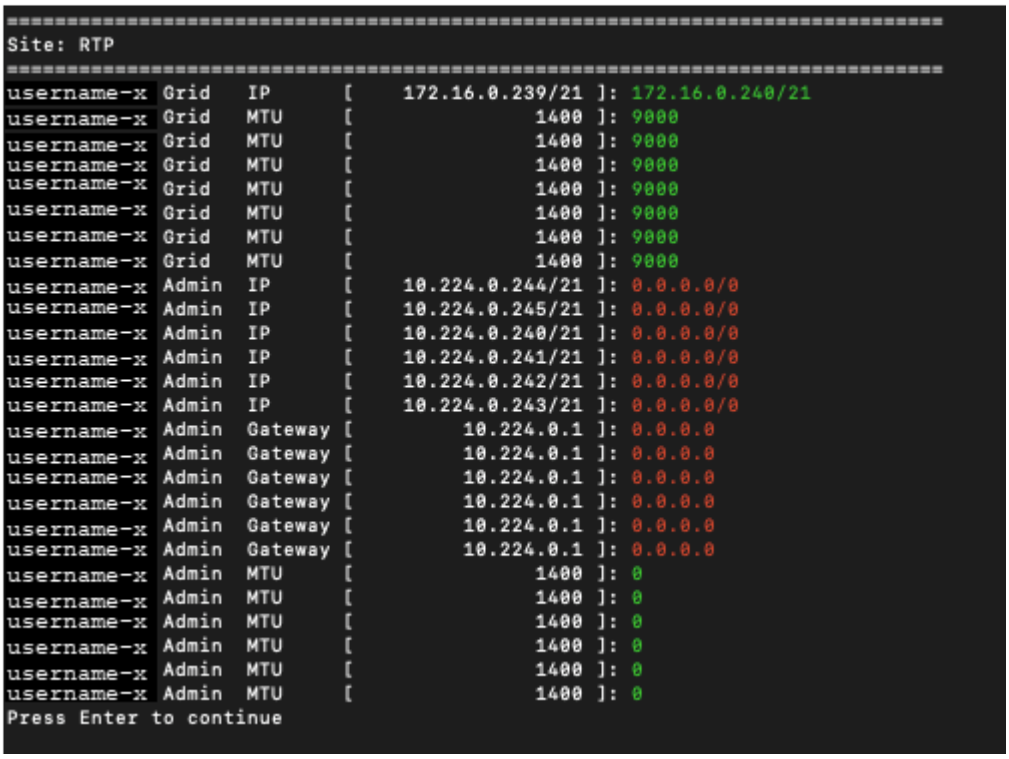
d. Se il tipo di dati è `IP/mask`, È possibile eliminare la rete Admin o Client dal nodo immettendo **d** o **0.0.0.0/0**.

e. Dopo aver modificato tutti i nodi che si desidera modificare, immettere **q** per tornare al menu principale.

   Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.

6. Per rivedere le modifiche, selezionare una delle seguenti opzioni:

   - **5**: Mostra le modifiche nell'output isolato per mostrare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'output di esempio:



   - **6**: Mostra le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni).

> Alcune interfacce della riga di comando potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough. La corretta visualizzazione dipende dal client terminale che supporta le sequenze di escape VT100 necessarie.

7. Selezionare l'opzione **7** per convalidare tutte le modifiche.

   Questa convalida garantisce che le regole per le reti Grid, Admin e Client, come ad esempio l'utilizzo di sottoreti sovrapposte, non vengano violate.

   In questo esempio, la convalida ha restituito errori.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

In questo esempio, la convalida è stata superata.

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

Press Enter to continue
```

8. Dopo il superamento della convalida, scegliere una delle seguenti opzioni:
   - **8**: Salva le modifiche non applicate.

     Questa opzione consente di uscire dallo strumento Change IP e di avviarlo di nuovo in un secondo momento, senza perdere alcuna modifica non applicata.

   - **10**: Applicare la nuova configurazione di rete.
9. Se è stata selezionata l'opzione **10**, scegliere una delle seguenti opzioni:
   - **Apply**: Applica le modifiche immediatamente e riavvia automaticamente ogni nodo, se necessario.

     Se la nuova configurazione di rete non richiede modifiche fisiche, selezionare **Apply** (Applica) per applicare le modifiche immediatamente. I nodi verranno riavviati automaticamente, se necessario. Verranno visualizzati i nodi che devono essere riavviati.

   - **Fase**: Applicare le modifiche al successivo riavvio manuale dei nodi.

     Se è necessario apportare modifiche alla configurazione di rete fisica o virtuale per il funzionamento della nuova configurazione di rete, utilizzare l'opzione **stage**, arrestare i nodi interessati, apportare le necessarie modifiche fisiche di rete e riavviare i nodi interessati. Se si seleziona **Apply** (Applica) senza apportare prima queste modifiche alla rete, le modifiche non vengono eseguite correttamente.

     > Se si utilizza l'opzione **stage**, è necessario riavviare il nodo il prima possibile dopo lo staging per ridurre al minimo le interruzioni.

   - **CANCEL**: Non apportare modifiche alla rete in questo momento.

     Se non si è a conoscenza del fatto che le modifiche proposte richiedono il riavvio dei nodi, è possibile posticipare le modifiche per ridurre al minimo l'impatto sull'utente. Selezionando **CANCEL** si torna al menu principale e si conservano le modifiche in modo da poterle applicare in un secondo momento.

     Quando si seleziona **Apply** o **Stage**, viene generato un nuovo file di configurazione di rete, viene eseguito il provisioning e i nodi vengono aggiornati con nuove informazioni di lavoro.

     Durante il provisioning, l'output visualizza lo stato man mano che vengono applicati gli aggiornamenti.

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

Una volta applicate o apportate le modifiche, viene generato un nuovo pacchetto di ripristino in seguito alla modifica della configurazione della griglia.

10. Se si seleziona **fase**, seguire questi passaggi al termine del provisioning:

    a. Apportare le modifiche di rete fisiche o virtuali richieste.

       Modifiche fisiche alla rete: Apportare le modifiche fisiche necessarie alla rete, spegnendo il nodo in modo sicuro, se necessario.

    Linux: Se si aggiunge il nodo a una rete amministrativa o a una rete client per la prima volta, assicurarsi di aver aggiunto l'interfaccia come descritto in "Linux: Aggiunta di interfacce al nodo esistente".

    a. Riavviare i nodi interessati.

11. Selezionare **0** per uscire dallo strumento Change IP una volta completate le modifiche.
12. Scarica un nuovo pacchetto di ripristino da Grid Manager.
    a. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.
    b. Inserire la passphrase di provisioning.

Aggiungere o modificare gli elenchi di subnet nella rete amministrativa

È possibile aggiungere, eliminare o modificare le subnet nell'elenco subnet di rete amministrativa di uno o più nodi.

Prima di iniziare

- Hai il `Passwords.txt` file.

È possibile aggiungere, eliminare o modificare le subnet in tutti i nodi dell'elenco subnet di rete amministrativa.

Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete di amministrazione o la rete client di alcun nodo:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Ad esempio, non utilizzare i seguenti intervalli di subnet per la rete Grid, la rete amministrativa o la rete client di alcun nodo:

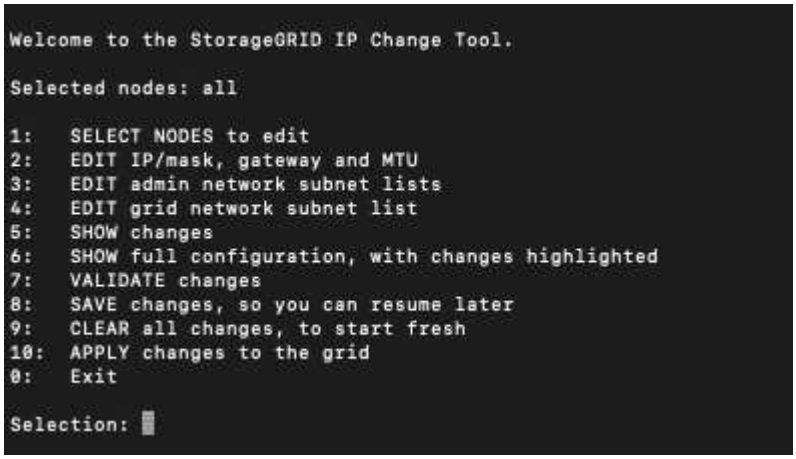
- 192.168.130.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 198.51.100.2 e 198.51.100.4

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
2. Avviare lo strumento Change IP immettendo il seguente comando: `change-ip`
3. Inserire la passphrase di provisioning quando richiesto.

   Viene visualizzato il menu principale.



4. Facoltativamente, limitare le reti/nodi su cui vengono eseguite le operazioni. Scegliere una delle seguenti opzioni:
   - Selezionare i nodi da modificare scegliendo **1**, se si desidera filtrare su nodi specifici su cui eseguire l'operazione. Selezionare una delle seguenti opzioni:
     - **1**: Nodo singolo (selezionare per nome)
     - **2**: Nodo singolo (selezionare per sito, quindi per nome)
     - **3**: Nodo singolo (selezionato in base all'IP corrente)
     - **4**: Tutti i nodi di un sito
     - **5**: Tutti i nodi della griglia
     - **0**: Torna indietro
   - Consenti a "tutto" di rimanere selezionato.
     Una volta effettuata la selezione, viene visualizzata la schermata del menu principale. Il campo Selected Nodes (nodi selezionati) riflette la nuova selezione e ora tutte le operazioni selezionate verranno eseguite solo su questo elemento.
5. Nel menu principale, selezionare l'opzione per modificare le subnet per la rete amministrativa (opzione **3**).
6. Scegliere una delle seguenti opzioni:
   - Per aggiungere una subnet, immettere il seguente comando: `add CIDR`
   - Per eliminare una subnet, immettere il seguente comando: `del CIDR`
   - Impostare l'elenco delle subnet immettendo questo comando: `set CIDR`

   Per tutti i comandi, è possibile inserire più indirizzi utilizzando questo formato: `add CIDR, CIDR`

   Esempio: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   È possibile ridurre la quantità di digitazione richiesta utilizzando la "freccia su" per richiamare i valori digitati in precedenza al prompt di immissione corrente, quindi modificarli se necessario.

   L'esempio riportato di seguito mostra l'aggiunta di subnet all'elenco subnet di rete amministrativa:

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. Una volta pronti, inserire **q** per tornare alla schermata del menu principale. Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.

> Se è stata selezionata una delle modalità di selezione dei nodi "all" nel passaggio 2, premere **Invio** (senza **q**) per passare al nodo successivo nell'elenco.

8. Scegliere una delle seguenti opzioni:

   - Selezionare l'opzione **5** per visualizzare le modifiche nell'output isolato in modo da visualizzare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'esempio riportato di seguito:

```
=====================================================================
Site: Data Center 1
=====================================================================
DC1-ADM1-105-154 Admin  Subnets                    add 172.17.0.0/16
                                                   del 172.16.0.0/16
                              [      172.14.0.0/16 ]
                              [      172.15.0.0/16 ]
                              [      172.17.0.0/16 ]
                              [      172.19.0.0/16 ]
                              [      172.20.0.0/16 ]
                              [      172.21.0.0/16 ]
Press Enter to continue
```

   - Selezionare l'opzione **6** per visualizzare le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni).
     Nota: alcuni emulatori di terminali potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough.

     Quando si tenta di modificare l'elenco delle subnet, viene visualizzato il seguente messaggio:

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't reachable using default StorageGRID routing, but are reachable
using a different interface and gateway. Making and applying changes
to the subnet list will make all automatically applied subnets
persistent. If you don't want that to happen, delete the unwanted
subnets before applying changes. If you know that all /32 subnets in
the list were added intentionally, you can ignore this caution.
```

     Se non sono state assegnate in modo specifico le subnet NTP e DNS dei server a una rete, StorageGRID crea automaticamente un percorso host (/32) per la connessione. Se, ad esempio, si preferisce un percorso /16 o /24 per la connessione in uscita a un server DNS o NTP, eliminare il percorso /32 creato automaticamente e aggiungere i percorsi desiderati. Se non si elimina la route host creata automaticamente, questa verrà persistente dopo l'applicazione di eventuali modifiche all'elenco delle subnet.

Sebbene sia possibile utilizzare questi percorsi host rilevati automaticamente, in generale è necessario configurare manualmente i percorsi DNS e NTP per garantire la connettività.

9. Selezionare l'opzione **7** per convalidare tutte le modifiche in fasi.

   Questa convalida garantisce il rispetto delle regole per le reti Grid, Admin e Client, ad esempio l'utilizzo di sottoreti sovrapposte.

10. Se si desidera, selezionare l'opzione **8** per salvare tutte le modifiche in più fasi e tornare in seguito per continuare ad apportare le modifiche.

    Questa opzione consente di uscire dallo strumento Change IP e di avviarlo di nuovo in un secondo momento, senza perdere alcuna modifica non applicata.

11. Effettuare una delle seguenti operazioni:
    - Selezionare l'opzione **9** se si desidera annullare tutte le modifiche senza salvare o applicare la nuova configurazione di rete.
    - Selezionare l'opzione **10** se si desidera applicare le modifiche e fornire la nuova configurazione di rete. Durante il provisioning, l'output visualizza lo stato quando vengono applicati gli aggiornamenti, come mostrato nell'output di esempio seguente:

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

12. Scarica un nuovo pacchetto di ripristino da Grid Manager.
    a. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.
    b. Inserire la passphrase di provisioning.

Aggiungere o modificare gli elenchi di subnet su Grid Network

È possibile utilizzare lo strumento Change IP per aggiungere o modificare le subnet nella rete griglia.

Prima di iniziare

- Hai il `Passwords.txt` file.

È possibile aggiungere, eliminare o modificare le subnet nell'elenco subnet di rete griglia. Le modifiche influiscono sul routing su tutti i nodi della griglia.

Se si apportano modifiche solo all'elenco subnet di rete griglia, utilizzare Grid Manager per aggiungere o modificare la configurazione di rete. In caso contrario, utilizzare lo strumento Change IP se Grid Manager non è accessibile a causa di un problema di configurazione di rete o se si stanno eseguendo contemporaneamente modifiche al routing Grid Network e altre modifiche di rete.

Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete di amministrazione o la rete client di alcun nodo:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Ad esempio, non utilizzare i seguenti intervalli di subnet per la rete Grid, la rete amministrativa o la rete client di alcun nodo:

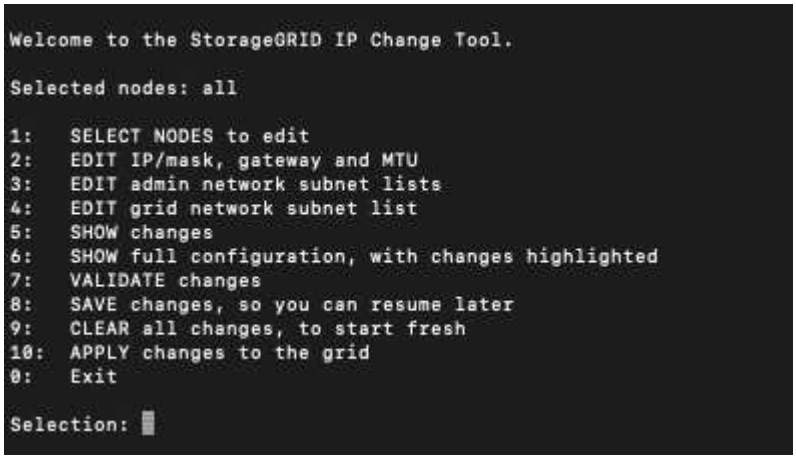
- 192.168.130.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 198.51.100.2 e 198.51.100.4

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
2. Avviare lo strumento Change IP immettendo il seguente comando: `change-ip`
3. Inserire la passphrase di provisioning quando richiesto.

   Viene visualizzato il menu principale.



4. Nel menu principale, selezionare l'opzione per modificare le subnet per Grid Network (opzione **4**).

   Le modifiche apportate all'elenco di subnet di rete griglia sono a livello di griglia.

5. Scegliere una delle seguenti opzioni:

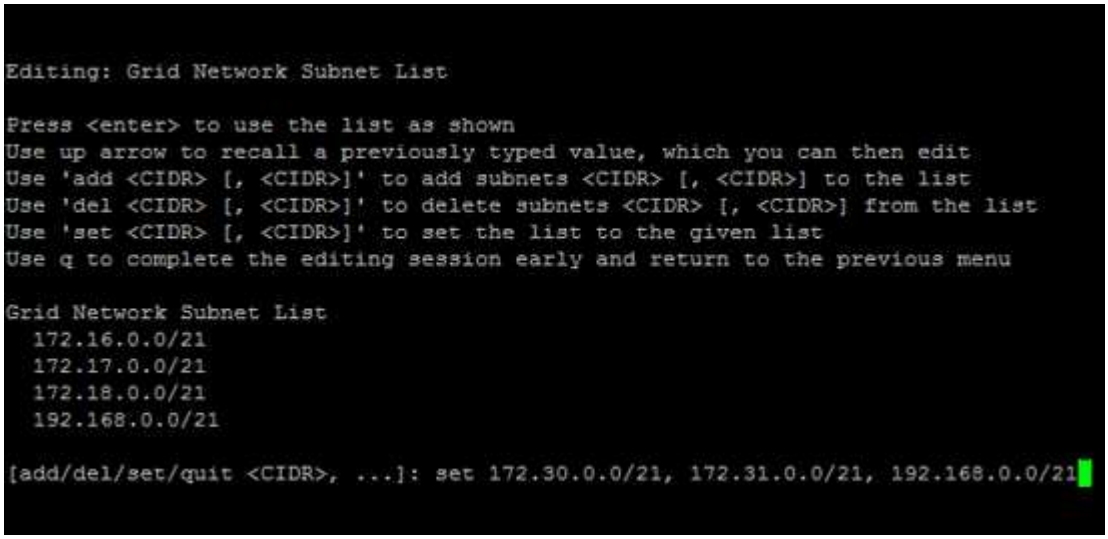
   - Per aggiungere una subnet, immettere il seguente comando: `add CIDR`
   - Per eliminare una subnet, immettere il seguente comando: `del CIDR`
   - Impostare l'elenco delle subnet immettendo questo comando: `set CIDR`

   Per tutti i comandi, è possibile inserire più indirizzi utilizzando questo formato: `add CIDR, CIDR`

   Esempio: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

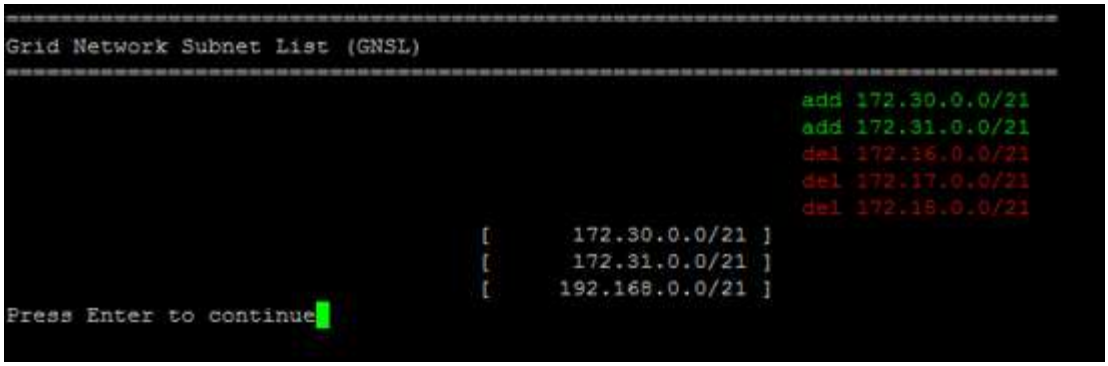
   È possibile ridurre la quantità di digitazione richiesta utilizzando la "freccia su" per richiamare i valori digitati in precedenza al prompt di immissione corrente, quindi modificarli se necessario.

   L'input di esempio riportato di seguito mostra l'impostazione delle subnet per l'elenco di subnet di rete griglia:



6. Una volta pronti, inserire **q** per tornare alla schermata del menu principale. Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.
7. Scegliere una delle seguenti opzioni:

   - Selezionare l'opzione **5** per visualizzare le modifiche nell'output isolato in modo da visualizzare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'esempio riportato di seguito:



- Selezionare l'opzione **6** per visualizzare le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni).

> Alcune interfacce della riga di comando potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough.

8. Selezionare l'opzione **7** per convalidare tutte le modifiche in fasi.

   Questa convalida garantisce il rispetto delle regole per le reti Grid, Admin e Client, ad esempio l'utilizzo di sottoreti sovrapposte.

9. Se si desidera, selezionare l'opzione **8** per salvare tutte le modifiche in più fasi e tornare in seguito per continuare ad apportare le modifiche.

   Questa opzione consente di uscire dallo strumento Change IP e di avviarlo di nuovo in un secondo momento, senza perdere alcuna modifica non applicata.

10. Effettuare una delle seguenti operazioni:
    - Selezionare l'opzione **9** se si desidera annullare tutte le modifiche senza salvare o applicare la nuova configurazione di rete.
    - Selezionare l'opzione **10** se si desidera applicare le modifiche e fornire la nuova configurazione di rete. Durante il provisioning, l'output visualizza lo stato quando vengono applicati gli aggiornamenti, come mostrato nell'output di esempio seguente:

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

11. Se è stata selezionata l'opzione **10** quando si apportano modifiche alla rete griglia, selezionare una delle seguenti opzioni:
    - **Apply**: Applica le modifiche immediatamente e riavvia automaticamente ogni nodo, se necessario.

      Se la nuova configurazione di rete funziona contemporaneamente alla vecchia configurazione di rete senza modifiche esterne, è possibile utilizzare l'opzione **Apply** per una modifica della configurazione completamente automatica.

- **Fase**: Applicare le modifiche al successivo riavvio dei nodi.

  Se è necessario apportare modifiche alla configurazione di rete fisica o virtuale per il funzionamento della nuova configurazione di rete, utilizzare l'opzione **stage**, arrestare i nodi interessati, apportare le necessarie modifiche fisiche di rete e riavviare i nodi interessati.

  > Se si utilizza l'opzione **stage**, riavviare il nodo il prima possibile dopo lo staging per ridurre al minimo le interruzioni.

- **CANCEL**: Non apportare modifiche alla rete in questo momento.

  Se non si è a conoscenza del fatto che le modifiche proposte richiedono il riavvio dei nodi, è possibile posticipare le modifiche per ridurre al minimo l'impatto sull'utente. Selezionando **CANCEL** si torna al menu principale e si conservano le modifiche in modo da poterle applicare in un secondo momento.

Una volta applicate o apportate le modifiche, viene generato un nuovo pacchetto di ripristino in seguito alla modifica della configurazione della griglia.

12. Se la configurazione viene interrotta a causa di errori, sono disponibili le seguenti opzioni:
    - Per terminare la procedura di modifica dell'indirizzo IP e tornare al menu principale, immettere **a**.
    - Per riprovare l'operazione non riuscita, immettere **r**.
    - Per passare all'operazione successiva, immettere **c**.

      L'operazione non riuscita può essere rieseguita in un secondo momento selezionando l'opzione **10** (Applica modifiche) dal menu principale. La procedura di modifica dell'IP non sarà completa fino a quando tutte le operazioni non saranno state completate correttamente.

    - Se è stato necessario intervenire manualmente (ad esempio per riavviare un nodo) e si è certi che l'azione che lo strumento ritiene non sia riuscita sia stata completata correttamente, immettere **f** per contrassegnarla come riuscita e passare all'operazione successiva.
13. Scarica un nuovo pacchetto di ripristino da Grid Manager.
    a. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.
    b. Inserire la passphrase di provisioning.

    > 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.

Modificare gli indirizzi IP per tutti i nodi nella griglia

Se è necessario modificare l'indirizzo IP Grid Network per tutti i nodi della griglia, seguire questa procedura speciale. Non è possibile modificare l'IP Grid Network a livello di griglia utilizzando la procedura per modificare i singoli nodi.

Prima di iniziare

- Hai il `Passwords.txt` file.

Per garantire che la griglia venga avviata correttamente, è necessario apportare tutte le modifiche contemporaneamente.

Questa procedura si applica solo alla rete di rete. Non è possibile utilizzare questa procedura per modificare gli indirizzi IP nelle reti Admin o Client.

Se si desidera modificare gli indirizzi IP e la MTU per i nodi di un solo sito, seguire la "Modificare la configurazione di rete del nodo" istruzioni.

Fasi

1. Pianificare in anticipo le modifiche da apportare al di fuori dello strumento Change IP, ad esempio le modifiche a DNS o NTP, e le modifiche alla configurazione SSO (Single Sign-on), se utilizzata.

   Se i server NTP esistenti non sono accessibili alla griglia dei nuovi indirizzi IP, aggiungere i nuovi server NTP prima di eseguire la procedura di modifica dell'ip.

   Se i server DNS esistenti non sono accessibili alla griglia dei nuovi indirizzi IP, aggiungere i nuovi server DNS prima di eseguire la procedura di modifica dell'indirizzo ip.

   Se SSO è attivato per il sistema StorageGRID e i trust di qualsiasi parte che si basa sono configurati utilizzando gli indirizzi IP del nodo di amministrazione (invece di nomi di dominio completi, come consigliato), è necessario essere pronti ad aggiornare o riconfigurare i trust di tali parti in Active Directory Federation Services (ad FS) Subito dopo aver modificato gli indirizzi IP. Vedere "Configurare il single sign-on".

   Se necessario, aggiungere la nuova subnet per i nuovi indirizzi IP.

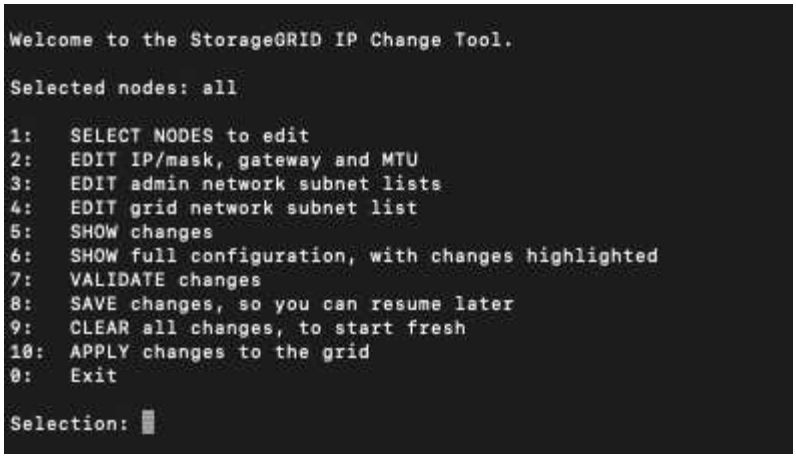
2. Accedere al nodo di amministrazione principale:

   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

3. Avviare lo strumento Change IP immettendo il seguente comando: `change-ip`
4. Inserire la passphrase di provisioning quando richiesto.

   Viene visualizzato il menu principale. Per impostazione predefinita, il `Selected nodes` il campo è impostato su `all`.



5. Nel menu principale, selezionare **2** per modificare le informazioni relative a IP/subnet mask, gateway e MTU per tutti i nodi.

   a. Selezionare **1** per apportare modifiche alla rete griglia.

      Una volta effettuata la selezione, il prompt visualizza i nomi dei nodi, il nome della rete di griglia, il tipo di dati (IP/mask, Gateway o MTU), e valori correnti.

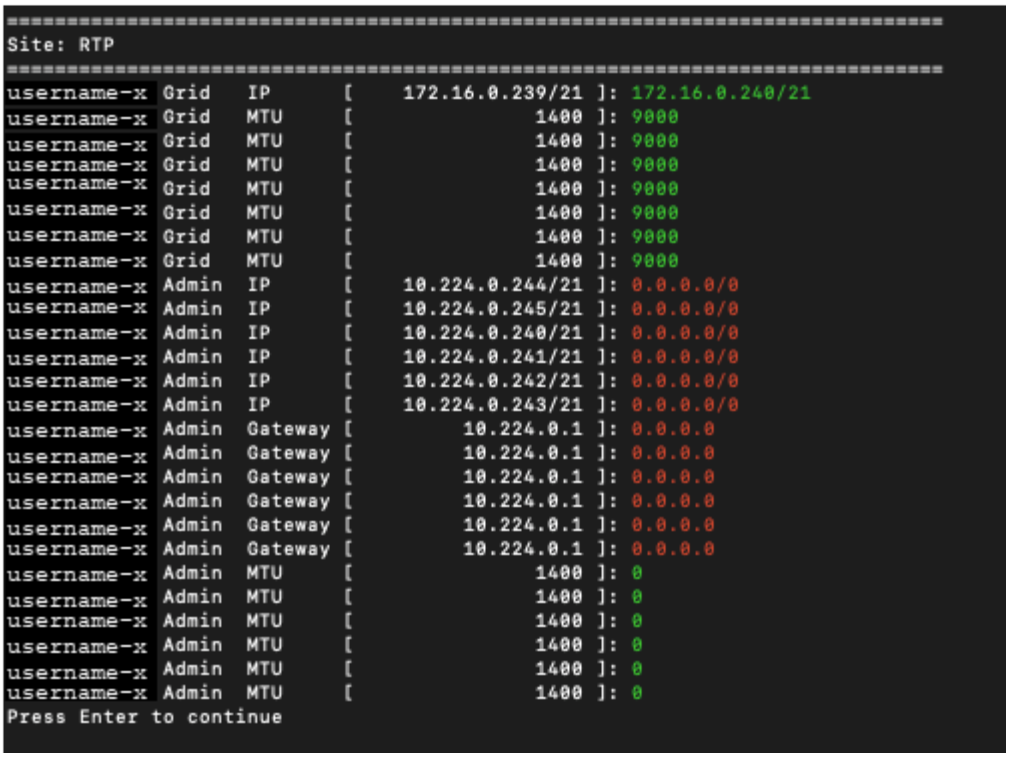
      Se si modificano l'indirizzo IP, la lunghezza del prefisso, il gateway o la MTU di un'interfaccia configurata con DHCP, l'interfaccia diventa statica. Viene visualizzato un avviso prima di ogni interfaccia configurata da DHCP.

   Interfacce configurate come `fixed` impossibile modificare.

   a. Per impostare un nuovo valore, immetterlo nel formato indicato per il valore corrente.
   b. Dopo aver modificato tutti i nodi che si desidera modificare, immettere **q** per tornare al menu principale.

      Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.

6. Per rivedere le modifiche, selezionare una delle seguenti opzioni:
   - **5**: Mostra le modifiche nell'output isolato per mostrare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'output di esempio:



- **6**: Mostra le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni).

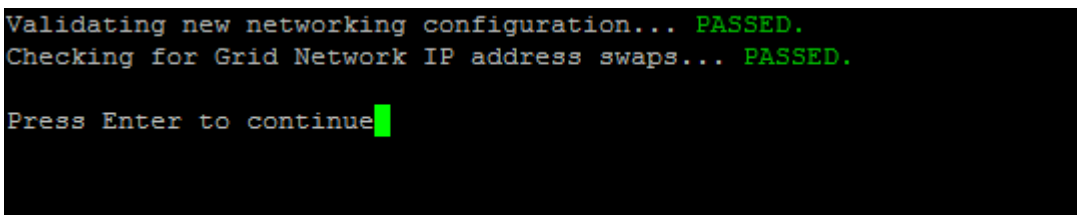
> Alcune interfacce della riga di comando potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough. La corretta visualizzazione dipende dal client terminale che supporta le sequenze di escape VT100 necessarie.

7. Selezionare l'opzione **7** per convalidare tutte le modifiche.

   Questa convalida garantisce che le regole per Grid Network, come ad esempio il non utilizzo di sottoreti sovrapposte, non vengano violate.

   In questo esempio, la convalida ha restituito errori.

   In questo esempio, la convalida è stata superata.



8. Dopo il superamento della convalida, selezionare **10** per applicare la nuova configurazione di rete.
9. Selezionare **stage** per applicare le modifiche al successivo riavvio dei nodi.

> Selezionare **stage**. Non eseguire un rolling restart, manualmente o selezionando **Apply** invece di **stage**; la griglia non si avvierà correttamente.

10. Una volta completate le modifiche, selezionare **0** per uscire dallo strumento Change IP.
11. Arrestare tutti i nodi contemporaneamente.

> L'intera griglia deve essere chiusa, in modo che tutti i nodi siano spenti contemporaneamente.

12. Apportare le modifiche di rete fisiche o virtuali richieste.
13. Verificare che tutti i nodi della griglia non siano attivi.
14. Accendere tutti i nodi.
15. Dopo l'avvio della griglia:
    a. Se sono stati aggiunti nuovi server NTP, eliminare i vecchi valori del server NTP.
    b. Se sono stati aggiunti nuovi server DNS, eliminare i valori dei server DNS precedenti.
16. Scarica il nuovo pacchetto di ripristino da Grid Manager.
    a. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**.
    b. Inserire la passphrase di provisioning.

Informazioni correlate

- "Aggiungere o modificare gli elenchi di subnet su Grid Network"
- "Chiudere il nodo della griglia"

Aggiungere interfacce al nodo esistente

Linux: Aggiunta di interfacce Admin o Client a un nodo esistente

Seguire questa procedura per aggiungere un'interfaccia sulla rete di amministrazione o sulla rete client a un nodo Linux dopo l'installazione.

Se NON sono stati configurati ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET nel file di configurazione del nodo sull'host Linux durante l'installazione, utilizzare questa procedura per aggiungere l'interfaccia. Per ulteriori informazioni sul file di configurazione del nodo, consultare le istruzioni relative al sistema operativo Linux in uso:

- "Installare StorageGRID su Red Hat Enterprise Linux"
- "Installare StorageGRID su Ubuntu o Debian"

Questa procedura viene eseguita sul server Linux che ospita il nodo che richiede la nuova assegnazione di rete, non all'interno del nodo. Questa procedura aggiunge l'interfaccia solo al nodo; si verifica un errore di convalida se si tenta di specificare altri parametri di rete.

Per fornire le informazioni di indirizzamento, è necessario utilizzare lo strumento Change IP (Modifica IP). Vedere "Modificare la configurazione di rete del nodo".

Fasi

1. Accedere al server Linux che ospita il nodo.
2. Modificare il file di configurazione del nodo: `/etc/storagegrid/nodes/node-name.conf`.

   Non specificare altri parametri di rete, altrimenti si verificherà un errore di convalida.

   a. Aggiungere una voce per la nuova destinazione di rete. Ad esempio:

      ```
      CLIENT_NETWORK_TARGET = bond0.3206
      ```

   b. Facoltativo: Aggiungere una voce per l'indirizzo MAC. Ad esempio:

      ```
      CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
      ```

3. Eseguire il comando node validate:

   ```
   sudo storagegrid node validate node-name
   ```

4. Risolvere tutti gli errori di convalida.
5. Eseguire il comando node reload:

   ```
   sudo storagegrid node reload node-name
   ```

Linux: Aggiunta di interfacce di accesso o trunk a un nodo

È possibile aggiungere trunk o interfacce di accesso supplementari a un nodo Linux dopo averlo installato. Le interfacce aggiunte vengono visualizzate nella pagina delle interfacce VLAN e nella pagina dei gruppi ha.

Prima di iniziare

- Hai accesso alle istruzioni per l'installazione di StorageGRID sulla tua piattaforma Linux.
  - "Installare StorageGRID su Red Hat Enterprise Linux"
  - "Installare StorageGRID su Ubuntu o Debian"
- Hai il `Passwords.txt` file.
- Lo hai fatto "autorizzazioni di accesso specifiche".

Non tentare di aggiungere interfacce a un nodo mentre è attiva una procedura di aggiornamento, ripristino o espansione del software.

A proposito di questa attività

Seguire questa procedura per aggiungere una o più interfacce aggiuntive a un nodo Linux dopo l'installazione del nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (ha).

Se si aggiunge un'interfaccia di linea, è necessario configurare un'interfaccia VLAN in StorageGRID. Se si aggiunge un'interfaccia di accesso, è possibile aggiungerla direttamente a un gruppo ha; non è necessario configurare un'interfaccia VLAN.

Il nodo non è disponibile per un breve periodo di tempo quando si aggiungono interfacce. Eseguire questa procedura su un nodo alla volta.

Fasi

1. Accedere al server Linux che ospita il nodo.
2. Utilizzando un editor di testo come vim o pico, modificare il file di configurazione del nodo:

   `/etc/storagegrid/nodes/node-name.conf`

3. Aggiungere una voce al file per specificare il nome e, facoltativamente, la descrizione di ogni interfaccia aggiuntiva che si desidera aggiungere al nodo. USA questo formato.

   `INTERFACE_TARGET_nnnn=value`

   Per *nnnn*, specificare un numero univoco per ciascuno di essi `INTERFACE_TARGET` voce da aggiungere.

   Per *valore*, specificare il nome dell'interfaccia fisica sull'host bare-metal. Quindi, facoltativamente, aggiungere una virgola e fornire una descrizione dell'interfaccia, che viene visualizzata nella pagina delle interfacce VLAN e nella pagina dei gruppi ha.

   Ad esempio:

   `INTERFACE_TARGET_0001=ens256, Trunk`

   > Non specificare altri parametri di rete, altrimenti si verificherà un errore di convalida.

4. Eseguire il seguente comando per convalidare le modifiche apportate al file di configurazione del nodo:

   `sudo storagegrid node validate node-name`

   Risolvere eventuali errori o avvisi prima di passare alla fase successiva.

5. Eseguire il seguente comando per aggiornare la configurazione del nodo:

   `sudo storagegrid node reload node-name`

Al termine

- Se sono state aggiunte una o più interfacce di linea, passare a. "Configurare le interfacce VLAN" Per configurare una o più interfacce VLAN per ogni nuova interfaccia principale.
- Se sono state aggiunte una o più interfacce di accesso, visitare il sito "configurare i gruppi ad alta disponibilità" Per aggiungere le nuove interfacce direttamente ai gruppi ha.

VMware: Aggiunta di interfacce di accesso o trunk a un nodo

Una volta installato il nodo, è possibile aggiungere un trunk o un'interfaccia di accesso a un nodo VM. Le interfacce aggiunte vengono visualizzate nella pagina delle interfacce VLAN e nella pagina dei gruppi ha.

Prima di iniziare

- È possibile accedere alle istruzioni per "Installazione di StorageGRID sulla piattaforma VMware".

- Si dispone di macchine virtuali VMware con nodo di amministrazione e nodo di gateway.
- Si dispone di una subnet di rete che non viene utilizzata come rete, amministratore o rete client.
- Hai il `Passwords.txt` file.
- Lo hai fatto "autorizzazioni di accesso specifiche".

> Non tentare di aggiungere interfacce a un nodo mentre è attiva una procedura di aggiornamento, ripristino o espansione del software.

A proposito di questa attività

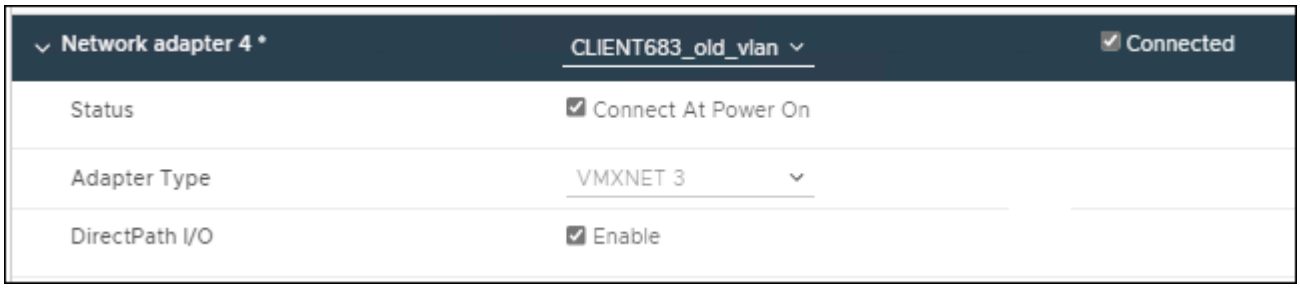
Seguire questa procedura per aggiungere una o più interfacce aggiuntive a un nodo VMware dopo l'installazione del nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (ha).

Se si aggiunge un'interfaccia di linea, è necessario configurare un'interfaccia VLAN in StorageGRID. Se si aggiunge un'interfaccia di accesso, è possibile aggiungerla direttamente a un gruppo ha; non è necessario configurare un'interfaccia VLAN.

Il nodo potrebbe non essere disponibile per un breve periodo di tempo quando si aggiungono interfacce.

Fasi

1. In vCenter, aggiungere una nuova scheda di rete (tipo VMXNET3) a un nodo di amministrazione e a una macchina virtuale del nodo gateway. Selezionare le caselle di controllo **connesso** e **Connetti all'accensione**.



2. Utilizzare SSH per accedere al nodo di amministrazione o al nodo gateway.
3. Utilizzare `ip link show` per confermare il rilevamento della nuova interfaccia di rete ens256.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Al termine

- Se sono state aggiunte una o più interfacce di linea, passare a. "Configurare le interfacce VLAN" Per configurare una o più interfacce VLAN per ogni nuova interfaccia principale.
- Se sono state aggiunte una o più interfacce di accesso, visitare il sito "configurare i gruppi ad alta disponibilità" Per aggiungere le nuove interfacce direttamente ai gruppi ha.

Configurare i server DNS

È possibile aggiungere, aggiornare e rimuovere i server DNS, in modo da poter utilizzare i nomi host FQDN (Fully Qualified Domain Name) anziché gli indirizzi IP.

Per utilizzare FQDN (Fully Qualified Domain Name) invece degli indirizzi IP quando si specificano i nomi host per le destinazioni esterne, specificare l'indirizzo IP di ciascun server DNS da utilizzare. Queste voci vengono utilizzate per AutoSupport, e-mail di avviso, notifiche SNMP, endpoint dei servizi della piattaforma, pool di storage cloud, e molto altro ancora.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone degli indirizzi IP dei server DNS da configurare.

A proposito di questa attività

Per garantire il corretto funzionamento, specificare due o tre server DNS. Se si specificano più di tre, è possibile che ne vengano utilizzati solo tre a causa delle limitazioni del sistema operativo note su alcune piattaforme. Se nel proprio ambiente sono presenti restrizioni di routing, è possibile "Personalizzare l'elenco dei server DNS" Per i singoli nodi (in genere tutti i nodi di un sito) di utilizzare un set diverso di un massimo di tre server DNS.

Se possibile, utilizzare i server DNS a cui ciascun sito può accedere localmente per garantire che un sito islanded possa risolvere i FQDN per le destinazioni esterne.

Aggiungere un server DNS

Per aggiungere un server DNS, procedere come segue.

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **Server DNS**.
2. Selezionare **Aggiungi un altro server** per aggiungere un server DNS.
3. Selezionare **Salva**.

Modificare un server DNS

Per modificare un server DNS, procedere come segue.

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **Server DNS**.
2. Selezionare l'indirizzo IP del nome del server che si desidera modificare e apportare le modifiche necessarie.
3. Selezionare **Salva**.

Eliminare un server DNS

Per eliminare un indirizzo IP di un server DNS, procedere come segue.

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **Server DNS**.
2. Selezionare l'icona di eliminazione ✕ Accanto all'indirizzo IP.
3. Selezionare **Salva**.

Modificare la configurazione DNS per un nodo griglia singolo

Invece di configurare il DNS a livello globale per l'intera implementazione, è possibile eseguire uno script per configurare il DNS in modo diverso per ciascun nodo della griglia.

In generale, utilizzare l'opzione **MANUTENZIONE** > **rete** > **server DNS** in Grid Manager per configurare i server DNS. Utilizzare il seguente script solo se è necessario utilizzare server DNS diversi per nodi griglia diversi.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

   e. Aggiungere la chiave privata SSH all'agente SSH. Inserire: `ssh-add`

f. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

2. Accedi al nodo che desideri aggiornare con una configurazione DNS personalizzata: `ssh node_IP_address`

3. Eseguire lo script di installazione del DNS: `setup_resolv.rb.`

   Lo script risponde con l'elenco dei comandi supportati.

```
Tool to modify external name servers

available commands:
  add search <domain>
              add a specified domain to search list
              e.g.> add search netapp.com
  remove search <domain>
              remove a specified domain from list
              e.g.> remove search netapp.com
  add nameserver <ip>
              add a specified IP address to the name server list
              e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
              remove a specified IP address from list
              e.g.> remove nameserver 192.0.2.65
  remove nameserver all
              remove all nameservers from list
  save        write configuration to disk and quit
  abort       quit without saving changes
  help        display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. Aggiungere l'indirizzo IPv4 di un server che fornisce il servizio dei nomi di dominio per la rete: `add <nameserver IP_address>`

5. Ripetere il `add nameserver` comando per aggiungere i server dei nomi.

6. Seguire le istruzioni richieste per altri comandi.
7. Salvare le modifiche e uscire dall'applicazione: `save`
8. chiudere la shell dei comandi sul server: `exit`
9. Per ciascun nodo della griglia, ripetere i passi da accesso al nodo attraverso chiudere la shell dei comandi.
10. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire: `ssh-add -D`

Gestire i server NTP

È possibile aggiungere, aggiornare o rimuovere server NTP (Network Time Protocol) per garantire che i dati siano sincronizzati in modo accurato tra i nodi della griglia nel sistema StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.
- Si dispone degli indirizzi IPv4 dei server NTP da configurare.

Utilizzo di NTP da parte di StorageGRID

Il sistema StorageGRID utilizza il protocollo NTP (Network Time Protocol) per sincronizzare l'ora tra tutti i nodi della griglia.

In ogni sito, ad almeno due nodi nel sistema StorageGRID viene assegnato il ruolo NTP primario. Si sincronizzano con un minimo consigliato di quattro e un massimo di sei sorgenti di tempo esterne e tra loro. Ogni nodo del sistema StorageGRID che non è un nodo NTP primario agisce come client NTP e si sincronizza con questi nodi NTP primari.

I server NTP esterni si connettono ai nodi ai quali sono stati precedentemente assegnati ruoli NTP primari. Per questo motivo, si consiglia di specificare almeno due nodi con ruoli NTP primari.

Linee guida del server NTP

Segui queste linee guida per proteggerti dai problemi di tempistica:

- I server NTP esterni si connettono ai nodi ai quali sono stati precedentemente assegnati ruoli NTP primari. Per questo motivo, si consiglia di specificare almeno due nodi con ruoli NTP primari.
- Assicurarsi che almeno due nodi di ciascun sito possano accedere ad almeno quattro origini NTP esterne. Se solo un nodo di un sito può raggiungere le origini NTP, si verificheranno problemi di tempistica se tale nodo non funziona. Inoltre, la designazione di due nodi per sito come origini NTP primarie garantisce tempi precisi se un sito viene isolato dal resto della rete.
- I server NTP esterni specificati devono utilizzare il protocollo NTP. È necessario specificare i riferimenti al server NTP di strato 3 o superiore per evitare problemi di deriva del tempo.

> Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Windows Time (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Time sulle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'utilizzo in ambienti ad alta precisione, incluso StorageGRID. Per ulteriori informazioni, vedere "Supportare il limite per configurare il servizio Time di Windows per ambienti ad alta precisione".

Configurare i server NTP

Per aggiungere, aggiornare o rimuovere i server NTP, procedere come segue.

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **server NTP**.
2. Nella sezione Server, aggiungere, aggiornare o rimuovere le voci del server NTP, secondo necessità.

   È necessario includere almeno quattro server NTP ed è possibile specificare fino a sei server.

3. Inserire la passphrase di provisioning per il sistema StorageGRID, quindi selezionare **Salva**.

   La pagina viene disattivata fino al completamento degli aggiornamenti della configurazione.

> Se tutti i server NTP non superano il test di connessione dopo aver salvato i nuovi server NTP, non procedere. Contattare il supporto tecnico.

Risolvere i problemi del server NTP

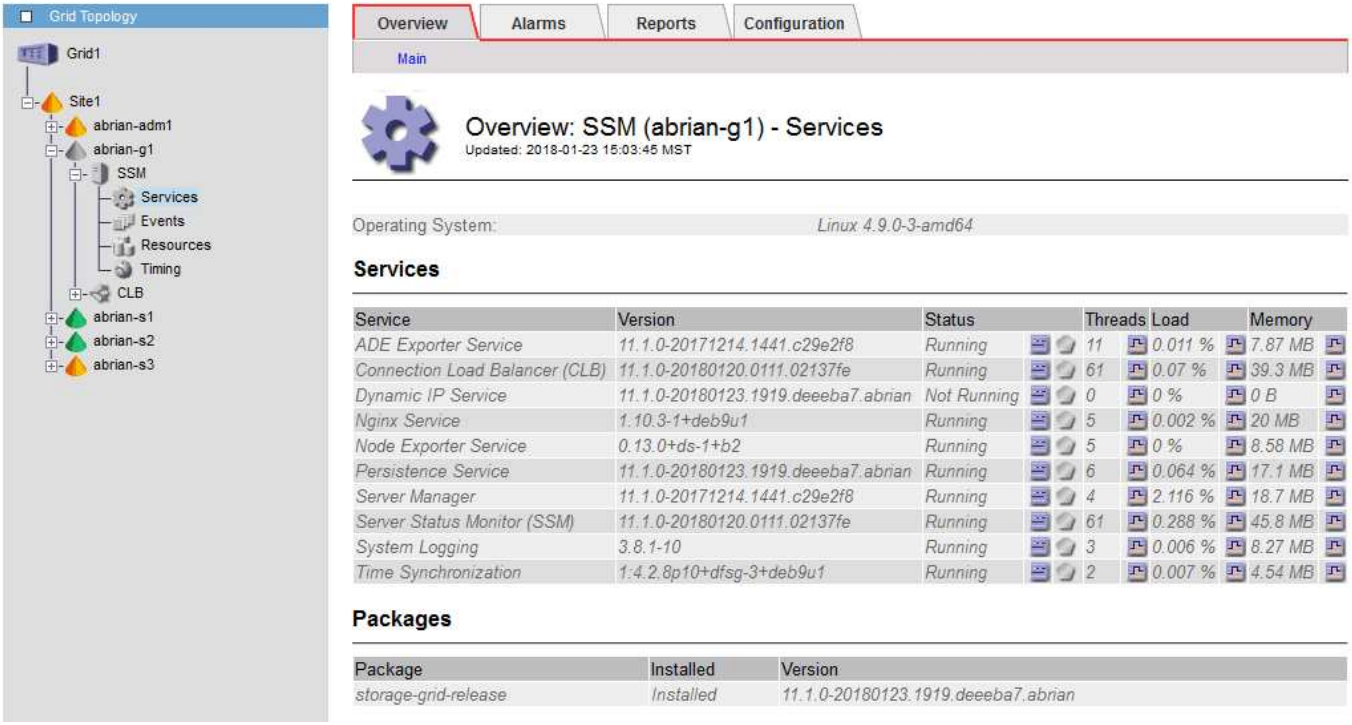
In caso di problemi con la stabilità o la disponibilità dei server NTP originariamente specificati durante l'installazione, è possibile aggiornare l'elenco delle origini NTP esterne utilizzate dal sistema StorageGRID aggiungendo server aggiuntivi o aggiornando o rimuovendo i server esistenti.

Ripristinare la connettività di rete per i nodi isolati

In alcuni casi, ad esempio in caso di modifica dell'indirizzo IP a livello di sito o di griglia, uno o più gruppi di nodi potrebbero non essere in grado di contattare il resto della griglia.

A proposito di questa attività

In Grid Manager (**SUPPORT** > **Tools** > **Grid topology**), se un nodo è grigio o se un nodo è blu con molti dei suoi servizi che mostrano uno stato diverso da quello in esecuzione, è necessario verificare l'isolamento del nodo.



Di seguito sono riportate alcune delle conseguenze derivanti dall'utilizzo di nodi isolati:

- Se sono isolati più nodi, potrebbe non essere possibile accedere a Grid Manager o accedervi.
- Se si isolano più nodi, i valori di utilizzo dello storage e di quota mostrati nella dashboard per il tenant Manager potrebbero essere obsoleti. I totali verranno aggiornati al ripristino della connettività di rete.

Per risolvere il problema di isolamento, eseguire un'utilità della riga di comando su ciascun nodo isolato o su un nodo di un gruppo (tutti i nodi di una subnet che non contiene il nodo di amministrazione primario) isolato dalla griglia. L'utility fornisce ai nodi l'indirizzo IP di un nodo non isolato nella griglia, che consente al nodo isolato o al gruppo di nodi di contattare nuovamente l'intera griglia.

Se il sistema mDNS (multicast domain name system) è disattivato nelle reti, potrebbe essere necessario eseguire l'utility della riga di comando su ciascun nodo isolato.

Fasi

1. Accedere al nodo e controllare `/var/local/log/dynip.log` per i messaggi di isolamento.

   Ad esempio:

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action might be required.
   ```

   Se si utilizza la console VMware, viene visualizzato un messaggio che indica che il nodo potrebbe essere isolato.

   Nelle implementazioni Linux, i messaggi di isolamento vengono visualizzati in `/var/log/storagegrid/node/<nodename>.log` file.

2. Se i messaggi di isolamento sono ricorrenti e persistenti, eseguire il seguente comando:

   `add_node_ip.py <address>`

   dove `<address>` È l'indirizzo IP di un nodo remoto connesso alla rete.

```
# /usr/sbin/add_node_ip.py  10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. Verificare quanto segue per ciascun nodo precedentemente isolato:
   - I servizi del nodo sono stati avviati.
   - Lo stato del servizio IP dinamico è "in esecuzione" dopo l'esecuzione di `storagegrid-status` comando.
   - Nell'albero topologia griglia, il nodo non appare più disconnesso dal resto della griglia.

> Se si esegue `add_node_ip.py` il comando non risolve il problema, potrebbero essere presenti altri problemi di rete che devono essere risolti.

Procedure host e middleware

Linux: Migrazione del nodo grid al nuovo host

È possibile migrare uno o più nodi StorageGRID da un host Linux (l' *host di origine*) a un altro host Linux (l' *host di destinazione*) per eseguire la manutenzione dell'host senza influire sulla funzionalità o sulla disponibilità del grid.

Ad esempio, è possibile migrare un nodo per eseguire l'applicazione di patch e il riavvio del sistema operativo.

Prima di iniziare

- Hai pianificato l'implementazione di StorageGRID per includere il supporto per la migrazione.
  - "Requisiti di migrazione dei container dei nodi per Red Hat Enterprise Linux"
  - "Requisiti di migrazione dei container di nodi per Ubuntu o Debian"
- L'host di destinazione è già pronto per l'uso con StorageGRID.
- Lo storage condiviso viene utilizzato per tutti i volumi di storage per nodo
- Le interfacce di rete hanno nomi coerenti tra gli host.

In un'implementazione in produzione, non eseguire più di un nodo di storage su un singolo host. L'utilizzo di un host dedicato per ciascun nodo di storage fornisce un dominio di errore isolato.

Sullo stesso host è possibile implementare altri tipi di nodi, come ad esempio i nodi Admin o Gateway. Tuttavia, se si dispone di più nodi dello stesso tipo (ad esempio due nodi gateway), non installare tutte le istanze sullo stesso host.

Esportare il nodo dall'host di origine

Come primo passo, chiudere il nodo grid ed esportarlo dall'host Linux di origine.

Eseguire i seguenti comandi sul *host di origine*.

Fasi

1. Ottenere lo stato di tutti i nodi attualmente in esecuzione sull'host di origine.

   ```
   sudo storagegrid node status all
   ```

   Output di esempio:

   ```
   Name Config-State Run-State
   DC1-ADM1 Configured Running
   DC1-ARC1 Configured Running
   DC1-GW1 Configured Running
   DC1-S1 Configured Running
   DC1-S2 Configured Running
   DC1-S3 Configured Running
   ```

2. Identificare il nome del nodo che si desidera migrare e interromperlo se il relativo stato di esecuzione è in esecuzione.

   ```
   sudo storagegrid node stop DC1-S3
   ```

   Output di esempio:

   ```
   Stopping node DC1-S3
   Waiting up to 630 seconds for node shutdown
   ```

3. Esportare il nodo dall'host di origine.

   ```
   sudo storagegrid node export DC1-S3
   ```

   Output di esempio:

   ```
   Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
   Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
   want to import it again.
   ```

4. Prendere nota di `import` comando suggerito nell'output.

   Questo comando verrà eseguito sull'host di destinazione nel passaggio successivo.

Nodo di importazione sull'host di destinazione

Dopo aver esportato il nodo dall'host di origine, importare e convalidare il nodo sull'host di destinazione. La convalida conferma che il nodo ha accesso agli stessi dispositivi di storage a blocchi e di interfaccia di rete dell'host di origine.

Eseguire i seguenti comandi sul *host di destinazione*.

Fasi

1. Importare il nodo sull'host di destinazione.

   ```
   sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
   ```

   Output di esempio:

   ```
   Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
   You should run 'storagegrid node validate DC1-S3'
   ```

2. Convalidare la configurazione del nodo sul nuovo host.

   ```
   sudo storagegrid node validate DC1-S3
   ```

   Output di esempio:

   ```
   Confirming existence of node DC1-S3... PASSED
   Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
   DC1-S3... PASSED
   Checking for duplication of unique values... PASSED
   ```

3. Se si verificano errori di convalida, risolverli prima di avviare il nodo migrato.

   Per informazioni sulla risoluzione dei problemi, consultare le istruzioni di installazione di StorageGRID per il sistema operativo Linux in uso.

   - "Installare StorageGRID su Red Hat Enterprise Linux"
   - "Installare StorageGRID su Ubuntu o Debian"

Avvia nodo migrato

Dopo aver validato il nodo migrato, avviarlo eseguendo un comando sul *host di destinazione*.

Fasi

1. Avviare il nodo sul nuovo host.

   ```
   sudo storagegrid node start DC1-S3
   ```

2. Accedere a Grid Manager e verificare che lo stato del nodo sia verde senza alcun avviso.

   Verificare che lo stato del nodo sia verde per garantire che il nodo migrato sia stato riavviato completamente e ricongiungesso alla griglia. Se lo stato non è verde, non migrare nodi aggiuntivi in modo da non avere più di un nodo fuori servizio.

3. Se non si riesce ad accedere a Grid Manager, attendere 10 minuti, quindi eseguire il seguente comando:

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

   Verificare che il nodo migrato abbia uno stato di esecuzione in esecuzione.

Manutenzione del nodo di archiviazione per il middleware TSM

I nodi di archiviazione possono essere configurati per essere utilizzati come destinazione su nastro tramite un server middleware TSM o il cloud tramite l'API S3. Una volta completata la configurazione, non è possibile modificare la destinazione di un nodo di archiviazione.

Se il server che ospita il nodo di archiviazione non funziona, sostituire il server e seguire la procedura di ripristino appropriata.

Guasto ai dispositivi storage di archiviazione

Se si determina la presenza di un guasto nel dispositivo di storage di archiviazione a cui il nodo di archiviazione sta accedendo tramite TSM, impostare il nodo di archiviazione offline per limitare il numero di allarmi visualizzati nel sistema StorageGRID. È quindi possibile utilizzare gli strumenti di amministrazione del server TSM o del dispositivo di storage, o entrambi, per diagnosticare e risolvere ulteriormente il problema.

Portare il componente di destinazione offline

Prima di eseguire qualsiasi manutenzione del server middleware TSM che potrebbe rendere il server non disponibile per il nodo di archiviazione, portare il componente di destinazione offline per limitare il numero di allarmi che vengono attivati se il server middleware TSM diventa non disponibile.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare **nodo archivio** > **ARC** > **destinazione** > **Configurazione** > **principale**.
3. Impostare il valore di Tivoli Storage Manager state su **Offline** e fare clic su **Apply Changes** (Applica modifiche).
4. Una volta completata la manutenzione, modificare il valore di Tivoli Storage Manager state (Stato di Tivoli Storage Manager) su **Online** e fare clic su **Apply Changes** (Applica modifiche).

Strumenti di amministrazione di Tivoli Storage Manager

Lo strumento dsmadmc è la console amministrativa per il server middleware TSM installato sul nodo di archiviazione. È possibile accedere allo strumento digitando `dsmadmc` nella riga di comando del server. Accedere alla console di amministrazione utilizzando lo stesso nome utente e la stessa password configurati

per il servizio ARC.

Il `tsmquery.rb` lo script è stato creato per generare informazioni sullo stato da dsmacmc in un formato più leggibile. È possibile eseguire questo script immettendo il seguente comando nella riga di comando del nodo di archiviazione: `/usr/local/arc/tsmquery.rb status`

Per ulteriori informazioni sulla console di amministrazione di TSM dsmadmc, consultare *Tivoli Storage Manager for Linux: Administrator's Reference*.

Oggetto permanentemente non disponibile

Quando il nodo di archiviazione richiede un oggetto dal server Tivoli Storage Manager (TSM) e il recupero non riesce, il nodo di archiviazione riprova la richiesta dopo un intervallo di 10 secondi. Se l'oggetto non è permanentemente disponibile (ad esempio, perché l'oggetto è corrotto su nastro), l'API TSM non può indicare questo al nodo di archiviazione, quindi il nodo di archiviazione continua a riprovare la richiesta.

Quando si verifica questa situazione, viene attivato un allarme e il valore continua ad aumentare. Per visualizzare l'allarme, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi, selezionare **Archive Node** > **ARC** > **Retrieve** > **Request Failures**.

Se l'oggetto non è permanentemente disponibile, è necessario identificarlo e quindi annullare manualmente la richiesta del nodo di archiviazione come descritto nella procedura, Determinare se gli oggetti non sono permanentemente disponibili.

Il recupero può anche avere esito negativo se l'oggetto non è temporaneamente disponibile. In questo caso, le richieste di recupero successive dovrebbero avere successo.

Se il sistema StorageGRID è configurato per utilizzare una regola ILM che crea una singola copia a oggetti e tale copia non può essere recuperata, l'oggetto viene perso e non può essere recuperato. Tuttavia, è comunque necessario seguire la procedura per determinare se l'oggetto non è permanentemente disponibile per "ripulire" il sistema StorageGRID, per annullare la richiesta del nodo di archiviazione e per eliminare i metadati per l'oggetto perso.

Determinare se gli oggetti non sono permanentemente disponibili

È possibile determinare se gli oggetti non sono permanentemente disponibili effettuando una richiesta utilizzando la console di amministrazione di TSM.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai il `Passwords.txt` file.
- Si dispone dell'indirizzo IP di un nodo amministratore.

A proposito di questa attività

Questo esempio viene fornito a scopo informativo. Questa procedura non consente di identificare tutte le condizioni di errore che potrebbero causare oggetti o volumi su nastro non disponibili. Per informazioni sull'amministrazione di TSM, consultare la documentazione di TSM Server.

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.

2. Identificare l'oggetto o gli oggetti che non possono essere recuperati dal nodo di archiviazione:

   a. Accedere alla directory contenente i file di log di controllo: `cd /var/local/log`

      Il file di log di audit attivo è denominato audit.log. Una volta al giorno, il attivo `audit.log` il file viene salvato e viene visualizzato un nuovo `audit.log` il file viene avviato. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`. Dopo un giorno, il file salvato viene compresso e rinominato, nel formato `yyyy-mm-dd.txt.gz`, che conserva la data originale.

   b. Cercare nel file di log di audit pertinente i messaggi che indicano che non è stato possibile recuperare un oggetto archiviato. Ad esempio, immettere: `grep ARCE audit.log | less -n`

      Quando un oggetto non può essere recuperato da un nodo di archiviazione, il messaggio di audit ARCE (fine recupero oggetto di archiviazione) visualizza ARUN (middleware di archiviazione non disponibile) o GERR (errore generale) nel campo dei risultati. La seguente riga di esempio del registro di controllo mostra che il messaggio ARCE è terminato con il risultato ARUN per CBID 498D8A1F681F05B3.

      ```
      [AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
      ):ARUN][AVER(UI32):7]
      [ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
      MID(FC32):ARCI]
      [ATID(UI64):4560349751312520631]]
      ```

      Per ulteriori informazioni, consultare le istruzioni relative ai messaggi di audit.

   c. Registrare il CBID di ciascun oggetto che ha avuto un errore di richiesta.

      È inoltre possibile registrare le seguenti informazioni aggiuntive utilizzate dal TSM per identificare gli oggetti salvati dal nodo di archiviazione:

      - **Nome spazio file**: Equivalente all'ID nodo archivio. Per trovare l'ID nodo archivio, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi, selezionare **nodo archivio** > **ARC** > **destinazione** > **Panoramica**.
      - **High Level Name**: Equivalente all'ID del volume assegnato all'oggetto dal nodo di archiviazione. L'ID del volume assume la forma di una data (ad esempio, `20091127`), e viene registrato come VLID dell'oggetto nei messaggi di audit dell'archivio.
      - **Nome livello basso**: Equivalente al CBID assegnato a un oggetto dal sistema StorageGRID.

   d. Disconnettersi dalla shell dei comandi: `exit`

3. Controllare il server TSM per verificare se gli oggetti identificati al punto 2 non sono permanentemente disponibili:

   a. Accedere alla console di amministrazione del server TSM: `dsmadmc`

      Utilizzare il nome utente amministrativo e la password configurati per il servizio ARC. Immettere il nome utente e la password in Grid Manager. Per visualizzare il nome utente, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi, selezionare **Archive Node** > **ARC** > **Target** > **Configuration**.)

   b. Determinare se l'oggetto non è permanentemente disponibile.

Ad esempio, è possibile cercare nel registro attività TSM un errore di integrità dei dati per quell'oggetto. Nell'esempio seguente viene illustrata una ricerca nel registro delle attività per il giorno precedente di un oggetto con CBID `498D8A1F681F05B3`.

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

A seconda della natura dell'errore, il CBID potrebbe non essere registrato nel log delle attività del TSM. Potrebbe essere necessario cercare altri errori TSM nel registro durante il periodo di errore della richiesta.

c. Se un intero nastro non è disponibile in modo permanente, identificare i CBID per tutti gli oggetti memorizzati su quel volume: `query content TSM_Volume_Name`

dove `TSM_Volume_Name` È il nome TSM del nastro non disponibile. Di seguito viene riportato un esempio dell'output di questo comando:

```
 > query content TSM-Volume-Name
Node Name     Type Filespace  FSID Client's Name for File Name
------------- ---- ---------- ---- --------------------------
DEV-ARC-20    Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

Il `Client's Name for File Name` È uguale all'ID del volume del nodo di archivio (o TSM "nome di livello alto") seguito dal CBID dell'oggetto (o TSM "nome di livello basso"). Ovvero, il `Client's Name for File Name` prende la forma `/Archive Node volume ID /CBID`. Nella prima riga dell'output di esempio, il `Client's Name for File Name` è `/20081201/ C1D172940E6C7E12`.

Ricordate anche che il `Filespace` È l'ID del nodo del nodo di archiviazione.

Per annullare la richiesta di recupero, sono necessari il CBID di ciascun oggetto memorizzato nel volume e l'ID del nodo del nodo di archiviazione.

4. Per ogni oggetto non disponibile in modo permanente, annullare la richiesta di recupero ed emettere un comando per informare il sistema StorageGRID che la copia dell'oggetto è stata persa:

> Utilizzare la console ADE con cautela. Se la console non viene utilizzata correttamente, è possibile interrompere le operazioni di sistema e danneggiare i dati. Immettere i comandi con attenzione e utilizzare solo i comandi descritti in questa procedura.

a. Se non si è già connessi al nodo di archiviazione, effettuare l'accesso come segue:

i. Immettere il seguente comando: `ssh admin@grid_node_IP`

ii. Immettere la password elencata in `Passwords.txt` file.

iii. Immettere il seguente comando per passare a root: `su -`

iv. Immettere la password elencata in `Passwords.txt` file.

b. Accedere alla console ADE del servizio ARC: `telnet localhost 1409`

c. Annullare la richiesta per l'oggetto: `/proc/BRTR/cancel -c CBID`

dove `CBID` È l'identificatore dell'oggetto che non può essere recuperato dal TSM.

Se le sole copie dell'oggetto sono su nastro, la richiesta di "recupero in blocco" viene annullata con un messaggio, "1 richieste annullate". Se nel sistema sono presenti copie dell'oggetto, il recupero dell'oggetto viene elaborato da un altro modulo, quindi la risposta al messaggio è "0 richieste annullate".

d. Eseguire un comando per notificare al sistema StorageGRID che una copia dell'oggetto è stata persa e che è necessario eseguire un'altra copia: `/proc/CMSI/Object_Lost CBID node_ID`

dove `CBID` È l'identificatore dell'oggetto che non può essere recuperato dal server TSM, e. `node_ID` È l'ID nodo del nodo di archiviazione in cui il recupero non è riuscito.

Immettere un comando separato per ogni copia di oggetto persa: L'immissione di un intervallo di CBID non è supportata.

Nella maggior parte dei casi, il sistema StorageGRID inizia immediatamente a creare copie aggiuntive dei dati degli oggetti per garantire che venga rispettato il criterio ILM del sistema.

Tuttavia, se la regola ILM dell'oggetto specifica che è stata eseguita una sola copia e che tale copia è stata persa, l'oggetto non può essere recuperato. In questo caso, eseguire il `Object_Lost` Il comando rimuove i metadati dell'oggetto perso dal sistema StorageGRID.

Quando il `Object_Lost` il comando viene completato correttamente e viene visualizzato il seguente messaggio:

```
CLOC_LOST_ANS returned result 'SUCS'
```

+

> Il `/proc/CMSI/Object_Lost` Il comando è valido solo per gli oggetti persi memorizzati nei nodi di archiviazione.

a. Uscire dalla console ADE: `exit`

b. Disconnettersi dal nodo di archiviazione: `exit`

5. Reimpostare il valore di Request Failures (errori richiesta) nel sistema StorageGRID:

a. Accedere a **nodo archivio** > **ARC** > **Recupera** > **Configurazione** e selezionare **Reset Request Failure Count**.

b. Fare clic su **Applica modifiche**.

Informazioni correlate

"Amministrare StorageGRID"

"Esaminare i registri di audit"

VMware: Configurare la macchina virtuale per il riavvio automatico

Se la macchina virtuale non si riavvia dopo il riavvio di VMware vSphere Hypervisor, potrebbe essere necessario configurare la macchina virtuale per il riavvio automatico.

Eseguire questa procedura se si nota che una macchina virtuale non si riavvia durante il ripristino di un nodo di griglia o l'esecuzione di un'altra procedura di manutenzione.

Fasi

1. Nell'albero di VMware vSphere Client, selezionare la macchina virtuale non avviata.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Power on** (accensione).
3. Configurare VMware vSphere Hypervisor per riavviare automaticamente la macchina virtuale in futuro.

Recovery o sostituzione dei nodi

Procedure di ripristino del nodo Grid: Panoramica

In caso di guasto di un nodo Grid, è possibile ripristinarlo sostituendo il server fisico o virtuale guasto, reinstallando il software StorageGRID e ripristinando i dati ripristinabili.

I nodi Grid possono non funzionare se un guasto hardware, virtualizzazione, sistema operativo o software rende il nodo inutilizzabile o inaffidabile. Esistono diversi tipi di errore che possono attivare la necessità di ripristinare un nodo di rete.

I passaggi per il ripristino di un nodo di rete variano a seconda della piattaforma in cui è ospitato il nodo di rete e del tipo di nodo di rete. 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 Grid Manager per configurare il nodo sostitutivo e ripristinare i dati del nodo.

> In caso di guasto di un intero sito StorageGRID, contattare il supporto tecnico. Il supporto tecnico collaborerà con te per sviluppare ed eseguire un piano di ripristino del sito che massimizzi la quantità di dati recuperati e soddisfi i tuoi obiettivi di business. Vedere "Come il supporto tecnico recupera un sito".

Avvertenze e considerazioni per il ripristino del nodo grid

In caso di guasto di un nodo della griglia, è necessario ripristinarlo il prima possibile. Prima di iniziare, è necessario esaminare tutti gli avvisi e le considerazioni per il ripristino del nodo.

> StorageGRID è un sistema distribuito composto da più nodi che lavorano l'uno con l'altro. Non utilizzare le snapshot dei dischi per ripristinare i nodi della griglia. Fare invece riferimento alle procedure di ripristino e manutenzione per ciascun tipo di nodo.

Di seguito sono riportati alcuni dei motivi per cui è stato eseguito il ripristino di un nodo Grid guasto il prima possibile:

- Un nodo Grid guasto può ridurre la ridondanza dei dati di sistema e dei dati a oggetti, lasciando l'utente vulnerabile al rischio di perdita permanente dei dati in caso di guasto di un altro nodo.
- Un nodo Grid guasto può influire sull'efficienza delle operazioni giornaliere da-a-.
- Un nodo Grid guasto può ridurre la capacità di monitorare le operazioni del sistema.
- Un nodo Grid guasto può causare un errore del server interno 500 se sono in vigore regole ILM rigide.
- Se un nodo di rete non viene recuperato tempestivamente, i tempi di ripristino potrebbero aumentare. Ad esempio, potrebbero svilupparsi code che devono essere cancellate prima del completamento del ripristino.

Seguire sempre la procedura di ripristino per il tipo specifico di nodo della griglia che si sta ripristinando. Le procedure di recovery variano per i nodi di amministrazione primari o non primari, i nodi gateway, i nodi di archivio, i nodi appliance e i nodi storage.

Condizioni preliminari per il ripristino dei nodi di rete

Quando si ripristinano i nodi della griglia, si presume che siano presenti tutte le seguenti condizioni:

- L'hardware fisico o virtuale guasto è stato sostituito e configurato.
- La versione del programma di installazione dell'appliance StorageGRID installata sull'appliance sostitutiva corrisponde alla versione software del sistema StorageGRID, come descritto in "Verificare e aggiornare la versione del programma di installazione dell'appliance StorageGRID".
- Se si sta ripristinando un nodo Grid diverso dal nodo Admin primario, esiste una connessione tra il nodo Grid da ripristinare e il nodo Admin primario.

Ordine di recovery del nodo in caso di guasto di un server che ospita più di un nodo griglia

Se un server che ospita più di un nodo di rete si guasta, è possibile ripristinare i nodi in qualsiasi ordine. Tuttavia, se il server guasto ospita il nodo di amministrazione primario, è necessario ripristinare prima tale nodo. Il ripristino del nodo di amministrazione primario impedisce prima agli altri ripristini del nodo di interrompere l'attesa di contattare il nodo di amministrazione primario.

Indirizzi IP per i nodi ripristinati

Non tentare di ripristinare un nodo utilizzando un indirizzo IP attualmente assegnato a un altro nodo. Quando si implementa il nuovo nodo, utilizzare l'indirizzo IP corrente del nodo guasto o un indirizzo IP inutilizzato.

Se si utilizza un nuovo indirizzo IP per implementare il nuovo nodo e ripristinarlo, il nuovo indirizzo IP continuerà a essere utilizzato per il nodo recuperato. Se si desidera ripristinare l'indirizzo IP originale, utilizzare lo strumento Cambia IP al termine del ripristino.

Raccogliere i materiali necessari per il ripristino dei nodi grid

Prima di eseguire le procedure di manutenzione, assicurarsi di disporre dei materiali necessari per ripristinare un nodo della griglia guasto.

Elemento	Note
Archivio di installazione di StorageGRID	Se è necessario ripristinare un nodo Grid, è necessario Scaricare i file di installazione di StorageGRID per la tua piattaforma. **Nota:** non è necessario scaricare i file se si stanno ripristinando volumi di storage guasti su un nodo di storage.
Laptop di assistenza	Il laptop di assistenza deve disporre di quanto segue: • Porta di rete • Client SSH (ad esempio, putty) • "Browser Web supportato"

Elemento	Note
Pacchetto di ripristino `.zip` file	Ottenere una copia del pacchetto di ripristino più recente `.zip` file: `sgws-recovery-package-id-revision.zip` Il contenuto di `.zip` i file vengono aggiornati ogni volta che si modifica il sistema. Dopo aver apportato tali modifiche, viene richiesto di memorizzare la versione più recente del pacchetto di ripristino in una posizione sicura. Utilizzare la copia più recente per eseguire il ripristino in caso di errori della griglia. Se il nodo di amministrazione primario funziona normalmente, è possibile scaricare il pacchetto di ripristino da Grid Manager. Selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino**. Se non è possibile accedere a Grid Manager, è possibile trovare copie crittografate del pacchetto di ripristino su alcuni nodi di storage che contengono il servizio ADC. Su ciascun nodo di storage, esaminare questa posizione per il pacchetto di ripristino: `/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg` Utilizzare il pacchetto di ripristino con il numero di revisione più alto.
`Passwords.txt` file	Contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando. Incluso nel pacchetto di ripristino.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non si trova in `Passwords.txt` file.
Documentazione aggiornata per la piattaforma	Per la documentazione, visitare il sito Web del vendor della piattaforma. Per le versioni correnti supportate della piattaforma, consultare "Tool di matrice di interoperabilità NetApp".

Scaricare ed estrarre i file di installazione di StorageGRID

Scaricare il software ed estrarre i file, a meno che non si trovino "Ripristino dei volumi di storage guasti in un nodo di storage".

È necessario utilizzare la versione di StorageGRID attualmente in esecuzione sulla griglia.

Fasi

1. Determinare la versione del software attualmente installata. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **About** (informazioni su).
2. Accedere alla "Pagina dei download NetApp per StorageGRID".
3. Selezionare la versione di StorageGRID attualmente in esecuzione nella griglia.

   Le versioni del software StorageGRID hanno questo formato: `11.x.y`.

4. Accedi con il nome utente e la password del tuo account NetApp.
5. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).
6. Nella colonna **Installa StorageGRID** della pagina di download, selezionare `.tgz` oppure `.zip` file per la tua piattaforma.

   La versione mostrata nel file di archivio dell'installazione deve corrispondere alla versione del software attualmente installato.

   Utilizzare `.zip` Se si utilizza Windows.

Piattaforma	Archivio di installazione

Red Hat Enterprise Linux	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`

Ubuntu o Debian o appliance	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

7. Scaricare ed estrarre il file di archivio.
8. Segui la procedura appropriata per la tua piattaforma per scegliere i file di cui hai bisogno, in base alla piattaforma e ai nodi grid da ripristinare.

   I percorsi elencati nella fase per ciascuna piattaforma sono relativi alla directory di primo livello installata dal file di archivio.

9. Se si sta ripristinando un "Sistema Red Hat Enterprise Linux", selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Pacchetto RPM per l'installazione delle immagini del nodo StorageGRID sui vostri host RHEL.
	Pacchetto RPM per l'installazione del servizio host StorageGRID sugli host RHEL.

Percorso e nome del file	Descrizione
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per il ping federate.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di ruolo e playbook Ansible per la configurazione degli host RHEL per l'implementazione dei container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Script di supporto chiamato dal compagno `storagegrid-ssoauth-azure.py` Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta ripristinando un "Ubuntu o sistema Debian", selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Un file di licenza NetApp non in produzione che è possibile utilizzare per le implementazioni di test e proof of concept.
	PACCHETTO DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.
	Checksum MD5 per il file `/debs/storagegrid-webscale-images-version-SHA.deb`.
	PACCHETTO DEB per l'installazione del servizio host StorageGRID su host Ubuntu o Debian.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per il ping federate.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di manuale e ruolo Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.

Percorso e nome del file	Descrizione
	Script di supporto chiamato dal compagno `storagegrid-ssoauth-azure.py` Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta ripristinando un "Sistema VMware", selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid.
	Il file di modello Open Virtualization Format (`.ovf`) e il file manifest (`.mf`) Per l'implementazione del nodo di amministrazione primario.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi amministrativi non primari.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi di archiviazione.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi gateway.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi di storage basati su macchine virtuali.
Tool di scripting per la distribuzione	Descrizione

Percorso e nome del file	Descrizione
	Uno script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.
	Un file di configurazione di esempio da utilizzare con `deploy-vsphere-ovftool.sh` script.
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando è attivato il Single Sign-on (SSO). È anche possibile utilizzare questo script per il ping federate.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Script di supporto chiamato dal compagno `storagegrid-ssoauth-azure.py` Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta ripristinando un sistema basato su appliance StorageGRID, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	PACCHETTO DEB per l'installazione delle immagini del nodo StorageGRID sulle appliance.
	Checksum MD5 per il file `/debs/storagegridwebscale-images-version-SHA.deb`.

Per l'installazione dell'appliance, questi file sono necessari solo se è necessario evitare il traffico di rete. L'appliance può scaricare i file richiesti dal nodo di amministrazione principale.

Selezionare la procedura di ripristino del nodo

Selezionare la procedura di ripristino corretta per il tipo di nodo che ha avuto esito negativo.

Nodo della griglia	Procedura di recovery
Più di un nodo di storage	Contattare il supporto tecnico. Se più di un nodo di storage si è guastato, il supporto tecnico deve fornire assistenza per il ripristino per evitare incoerenze del database che potrebbero causare la perdita di dati. Potrebbe essere necessaria una procedura di ripristino del sito. "Come il supporto tecnico recupera un sito"
Un singolo nodo di storage	La procedura di recovery di Storage Node dipende dal tipo e dalla durata dell'errore. "Ripristino da guasti del nodo di storage"
Nodo Admin	La procedura Admin Node (nodo amministratore) dipende dalla necessità di ripristinare il nodo amministratore primario o un nodo amministratore non primario. "Ripristino da errori del nodo di amministrazione"
Nodo gateway	"Ripristino da guasti del nodo gateway".
Nodo di archiviazione	"Ripristino da errori del nodo di archiviazione".

Se un server che ospita più di un nodo di rete si guasta, è possibile ripristinare i nodi in qualsiasi ordine. Tuttavia, se il server guasto ospita il nodo di amministrazione primario, è necessario ripristinare prima tale nodo. Il ripristino del nodo di amministrazione primario impedisce prima agli altri ripristini del nodo di interrompere l'attesa di contattare il nodo di amministrazione primario.

Ripristino da guasti del nodo di storage

Recovery from Storage Node Failures: Panoramica

La procedura per il ripristino di un nodo di storage guasto dipende dal tipo di guasto e dal tipo di nodo di storage guasto.

Utilizzare questa tabella per selezionare la procedura di ripristino per un nodo di storage guasto.

Problema	Azione	Note
• Si è verificato un errore in più di un nodo di storage. • Un secondo nodo di storage si è guastato meno di 15 giorni dopo un guasto o un ripristino di un nodo di storage. Questo include il caso in cui un nodo di storage si guasta mentre il ripristino di un altro nodo di storage è ancora in corso.	Contattare il supporto tecnico.	Il ripristino di più di un nodo di storage (o di più nodi di storage entro 15 giorni) potrebbe influire sull'integrità del database Cassandra, causando la perdita di dati. Il supporto tecnico può determinare quando è sicuro iniziare il ripristino di un secondo nodo di storage. **Nota**: Se più di un nodo di storage che contiene il servizio ADC si guasta in un sito, si perdono le richieste di servizio della piattaforma in sospeso per quel sito.
Si è verificato un errore in più di un nodo di storage in un sito o in un intero sito.	Contattare il supporto tecnico. Potrebbe essere necessario eseguire una procedura di ripristino del sito.	Il supporto tecnico valuterà la tua situazione e svilupperà un piano di recovery. Vedere "Come il supporto tecnico recupera un sito".
Un nodo di storage è stato offline per più di 15 giorni.	"Recovery Storage Node Down per più di 15 giorni"	Questa procedura è necessaria per garantire l'integrità del database Cassandra.
Si è verificato un errore in un nodo di storage dell'appliance.	"Ripristinare il nodo storage dell'appliance"	La procedura di ripristino per i nodi di storage dell'appliance è la stessa per tutti i guasti.
Uno o più volumi di storage sono guasti, ma il disco di sistema è intatto	" Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto"	Questa procedura viene utilizzata per i nodi di storage basati su software.
Il disco di sistema è guasto.	"Ripristino in caso di guasto al disco di sistema"	La procedura di sostituzione del nodo dipende dalla piattaforma di implementazione e dal fatto che anche i volumi di storage abbiano avuto un guasto.

Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "riparazione Cassandra". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

Recovery Storage Node Down per più di 15 giorni

Se un singolo nodo di storage è stato offline e non connesso ad altri nodi di storage per più di 15 giorni, è necessario ricostruire Cassandra sul nodo.

Prima di iniziare

- È stato verificato che non è in corso la decommissionamento di un nodo di storage oppure che la procedura di decommissionamento del nodo è stata sospesa. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **smantellamento**).
- Hai verificato che non è in corso un'espansione. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **espansione**).

A proposito di questa attività

I nodi di storage dispongono di un database Cassandra che include metadati a oggetti. Se un nodo di storage non è stato in grado di comunicare con altri nodi di storage per più di 15 giorni, StorageGRID presume che il database Cassandra del nodo sia obsoleta. Il nodo di storage non può ricongiungersi alla griglia fino a quando Cassandra non viene ricostruita utilizzando le informazioni provenienti da altri nodi di storage.

Utilizzare questa procedura per ricostruire Cassandra solo se un singolo nodo di storage non è attivo. Contattare il supporto tecnico se altri nodi di storage sono offline o se Cassandra è stato ricostruito su un altro nodo di storage negli ultimi 15 giorni; ad esempio, Cassandra potrebbe essere stato ricostruito come parte delle procedure per ripristinare i volumi di storage guasti o per ripristinare un nodo di storage guasto.

Se più di un nodo di storage si è guastato (o non è in linea), contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

Se si tratta del secondo guasto del nodo di storage in meno di 15 giorni dopo un guasto o un ripristino del nodo di storage, contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

Se più di un nodo di storage in un sito si è guastato, potrebbe essere necessaria una procedura di ripristino del sito. Vedere "Come il supporto tecnico recupera un sito".

Fasi

1. Se necessario, accendere il nodo di storage che deve essere ripristinato.
2. Accedere al nodo Grid:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.+

> Se non si riesce ad accedere al nodo Grid, il disco di sistema potrebbe non essere intatto. Passare alla procedura per "ripristino in caso di guasto al disco di sistema".

3. Eseguire i seguenti controlli sul nodo di storage:

   a. Eseguire questo comando: `nodetool status`

      L'output deve essere `Connection refused`

   b. In Grid Manager, selezionare **SUPPORT** > **Tools** > **Grid topology**.

   c. Selezionare ***Site*** > **Storage Node** > **SSM** > **Services**. Verificare che venga visualizzato il servizio Cassandra `Not Running`.

   d. Selezionare **Storage Node** > **SSM** > **Resources**. Verificare che non vi sia stato di errore nella sezione Volumes (volumi).

   e. Eseguire questo comando: `grep -i Cassandra /var/local/log/servermanager.log`

      Nell'output dovrebbe essere visualizzato il seguente messaggio:

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

4. Eseguire questo comando e monitorare l'output dello script: `check-cassandra-rebuild`

   - Se il servizio Cassandra in base al volume 0 è in esecuzione, viene richiesto di interromperlo. Immettere: **Y**

     > Se il servizio Cassandra è già stato arrestato, non viene richiesto. Il servizio Cassandra viene arrestato solo per il volume 0.

   - Esaminare gli avvisi nello script. Se non sono applicabili, confermare che si desidera ricostruire Cassandra. Immettere: **Y**

     > Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "riparazione Cassandra". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

5. Al termine della ricostruzione, eseguire i seguenti controlli:

   a. In Grid Manager, selezionare **SUPPORT** > **Tools** > **Grid topology**.

   b. Selezionare ***Site*** > **Reupered Storage Node** > **SSM** > **Services**.

   c. Verificare che tutti i servizi siano in esecuzione.

   d. Selezionare **DDS** > **Data Store**.

   e. Verificare che lo stato **Data Store** sia "Up" e lo stato **Data Store** sia "Normal" (normale).

Ripristinare il nodo storage dell'appliance

Avvisi per il ripristino dei nodi di archiviazione dell'appliance

La procedura per il ripristino di un nodo di storage dell'appliance StorageGRID guasto è la stessa, sia che si stia ripristinando dalla perdita del disco di sistema che dalla perdita dei soli volumi di storage.

> Se più di un nodo di storage si è guastato (o non è in linea), contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

> Se si tratta del secondo guasto del nodo di storage in meno di 15 giorni dopo un guasto o un ripristino del nodo di storage, contattare il supporto tecnico. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni può causare la perdita di dati.

> Se più di un nodo di storage in un sito si è guastato, potrebbe essere necessaria una procedura di ripristino del sito. Vedere "Come il supporto tecnico recupera un sito".

> Se le regole ILM sono configurate in modo da memorizzare una sola copia replicata e la copia esiste su un volume di storage che ha avuto esito negativo, non sarà possibile ripristinare l'oggetto.

> Se si verifica un allarme Services: Status - Cassandra (SVST) durante il ripristino, vedere "Ripristinare i volumi di storage guasti e ricostruire il database Cassandra". Dopo la ricostruzione di Cassandra, gli allarmi devono essere disattivati. Se gli allarmi non vengono disattivati, contattare il supporto tecnico.

> Per le procedure di manutenzione dell'hardware, ad esempio le istruzioni per la sostituzione di un controller o la reinstallazione di SANtricity OS, consultare la "istruzioni di manutenzione per l'apparecchio di stoccaggio".

Preparare l'appliance Storage Node per la reinstallazione

Quando si ripristina un nodo di storage dell'appliance, è necessario prima preparare l'appliance per la reinstallazione del software StorageGRID.

Fasi

1. Accedere al nodo di storage guasto:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Preparare il nodo di storage dell'appliance per l'installazione del software StorageGRID. `sgareinstall`

3. Quando viene richiesto di continuare, immettere: `y`

   L'apparecchio si riavvia e la sessione SSH termina. In genere, il programma di installazione dell'appliance StorageGRID richiede circa 5 minuti, anche se in alcuni casi potrebbe essere necessario attendere fino a 30 minuti.

   > Non tentare di accelerare il riavvio spegnendo e riaccendendo o ripristinando l'apparecchio. È possibile interrompere gli aggiornamenti automatici di BIOS, BMC o altri aggiornamenti del firmware.

   Il nodo di storage dell'appliance StorageGRID viene ripristinato e i dati sul nodo di storage non sono più accessibili. Gli indirizzi IP configurati durante il processo di installazione originale devono rimanere intatti; tuttavia, si consiglia di confermarli al termine della procedura.

   Dopo aver eseguito il `sgareinstall` Comando, tutti gli account, le password e le chiavi SSH forniti da StorageGRID vengono rimossi e vengono generate nuove chiavi host.

Avviare l'installazione dell'appliance StorageGRID

Per installare StorageGRID su un nodo di storage dell'appliance, utilizzare il programma di installazione dell'appliance StorageGRID, incluso nell'appliance.

Prima di iniziare

- L'appliance è stata installata in un rack, collegata alla rete e accesa.
- I collegamenti di rete e gli indirizzi IP sono stati configurati per l'appliance mediante il programma di installazione dell'appliance StorageGRID.
- Si conosce l'indirizzo IP del nodo di amministrazione principale per la griglia StorageGRID.
- Tutte le subnet della rete griglia elencate nella pagina di configurazione IP del programma di installazione dell'appliance StorageGRID sono state definite nell'elenco delle subnet della rete griglia nel nodo di amministrazione principale.
- Queste attività preliminari sono state completate seguendo le istruzioni di installazione dell'appliance di storage. Vedere "Avvio rapido per l'installazione dell'hardware".
- Si sta utilizzando un "browser web supportato".
- Conosci uno degli indirizzi IP assegnati al controller di calcolo nell'appliance. È possibile utilizzare l'indirizzo IP per Admin Network (porta di gestione 1 sul controller), Grid Network o Client Network.

A proposito di questa attività

Per installare StorageGRID su un nodo di storage dell'appliance:

- Specificare o confermare l'indirizzo IP del nodo di amministrazione primario e il nome host (nome di sistema) del nodo.
- Avviare l'installazione e attendere la configurazione dei volumi e l'installazione del software.
- Durante il processo, l'installazione viene interrotta. Per riprendere l'installazione, è necessario accedere a Grid Manager e configurare il nodo di storage in sospeso come sostituzione del nodo guasto.
- Una volta configurato il nodo, il processo di installazione dell'appliance viene completato e l'appliance viene riavviata.

Fasi

1. Aprire un browser e inserire uno degli indirizzi IP del controller di calcolo nell'appliance.

   `https://Controller_IP:8443`

   Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.

2. Nella sezione Primary Admin Node Connection (connessione nodo amministratore primario), determinare se è necessario specificare l'indirizzo IP per il nodo amministratore primario.

   Il programma di installazione dell'appliance StorageGRID è in grado di rilevare automaticamente questo indirizzo IP, presupponendo che il nodo amministratore primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente nella stessa sottorete.

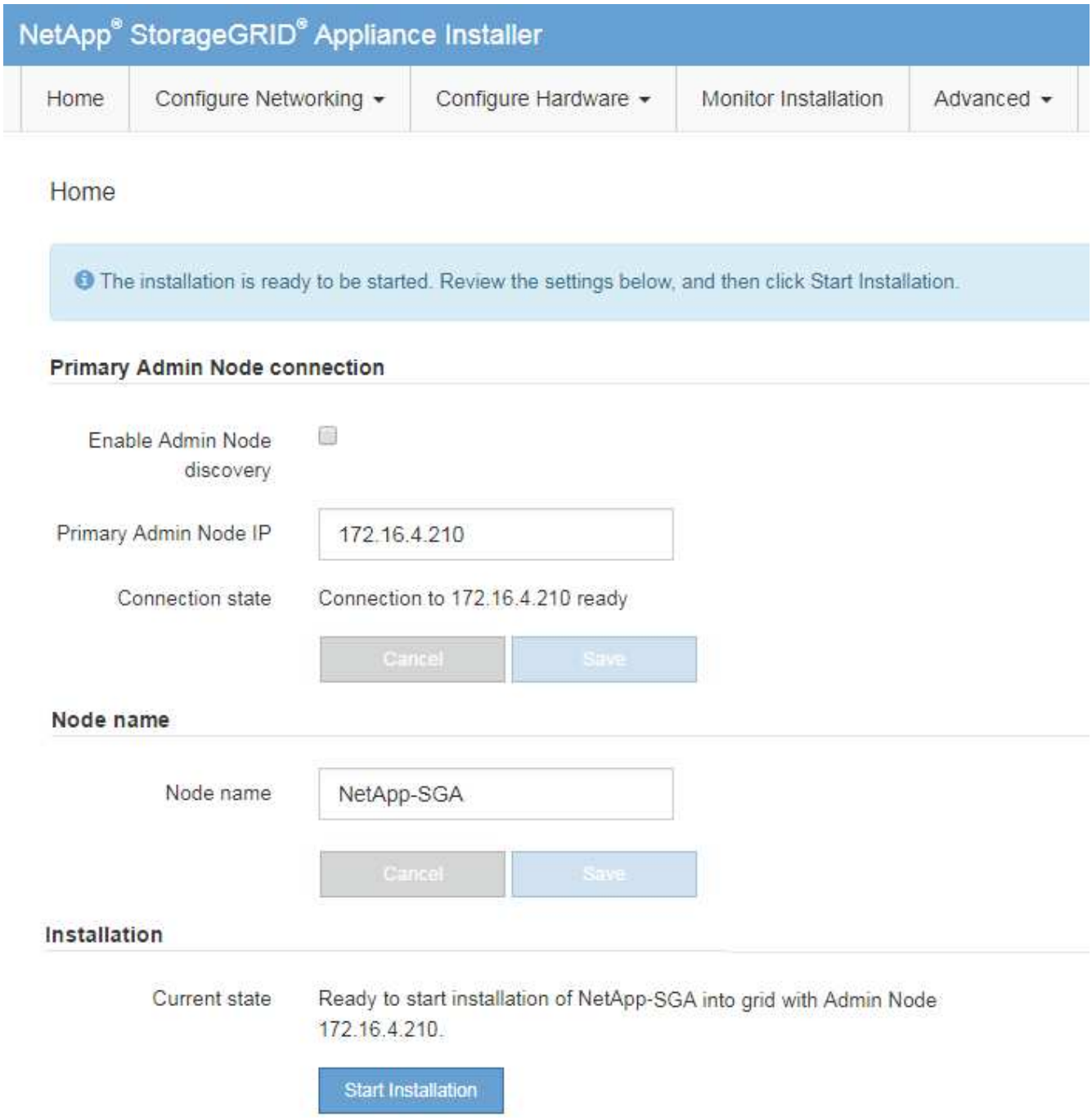
3. Se questo indirizzo IP non viene visualizzato o se è necessario modificarlo, specificare l'indirizzo:

Opzione	Fasi
Immissione manuale dell'IP	a. Deselezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Inserire l'indirizzo IP manualmente. c. Fare clic su **Save** (Salva). d. Attendere che lo stato della connessione del nuovo indirizzo IP diventi "pronto".
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Dall'elenco degli indirizzi IP rilevati, selezionare il nodo di amministrazione principale per la griglia in cui verrà implementato il nodo di storage dell'appliance. c. Fare clic su **Save** (Salva). d. Attendere che lo stato della connessione del nuovo indirizzo IP diventi "pronto".

4. Nel campo **Node Name** (Nome nodo), immettere lo stesso nome host (nome di sistema) utilizzato per il nodo che si sta ripristinando e fare clic su **Save** (Salva).
5. Nella sezione Installazione, verificare che lo stato corrente sia "Pronto per avviare l'installazione di *node name* Nella griglia con nodo di amministrazione primario `*admin_ip*`" e che il pulsante **Avvia installazione** sia abilitato.

   Se il pulsante **Avvia installazione** non è attivato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per istruzioni, consultare le istruzioni di manutenzione dell'apparecchio.

6. Dalla home page del programma di installazione dell'appliance StorageGRID, fare clic su **Avvia installazione**.



Lo stato corrente cambia in "Installazione in corso" e viene visualizzata la pagina Installazione monitor.

Per accedere manualmente alla pagina Installazione monitor, fare clic su **Installazione monitor** dalla barra dei menu. Vedere "Installazione dell'appliance di monitoraggio".

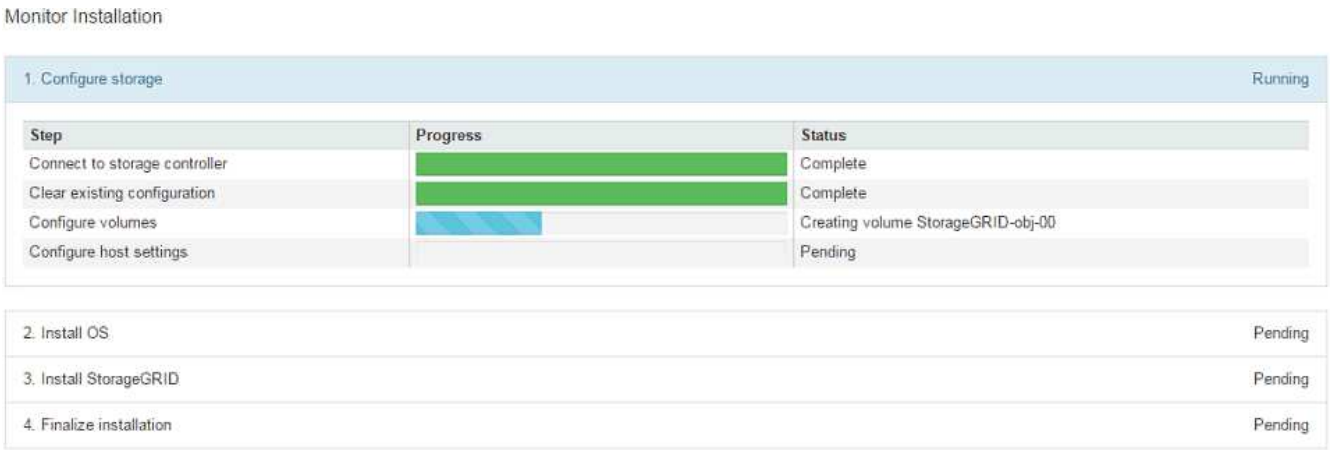
Monitorare l'installazione dell'appliance StorageGRID

Il programma di installazione dell'appliance StorageGRID indica lo stato fino al completamento dell'installazione. Una volta completata l'installazione del software, l'appliance viene riavviata.

Fasi

1. Per monitorare l'avanzamento dell'installazione, fare clic su **Monitor Installation** (Installazione monitor) nella barra dei menu.

   La pagina Monitor Installation (Installazione monitor) mostra lo stato di avanzamento dell'installazione.



   La barra di stato blu indica l'attività attualmente in corso. Le barre di stato verdi indicano le attività completate correttamente.

   > Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si sta eseguendo nuovamente un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "saltato".

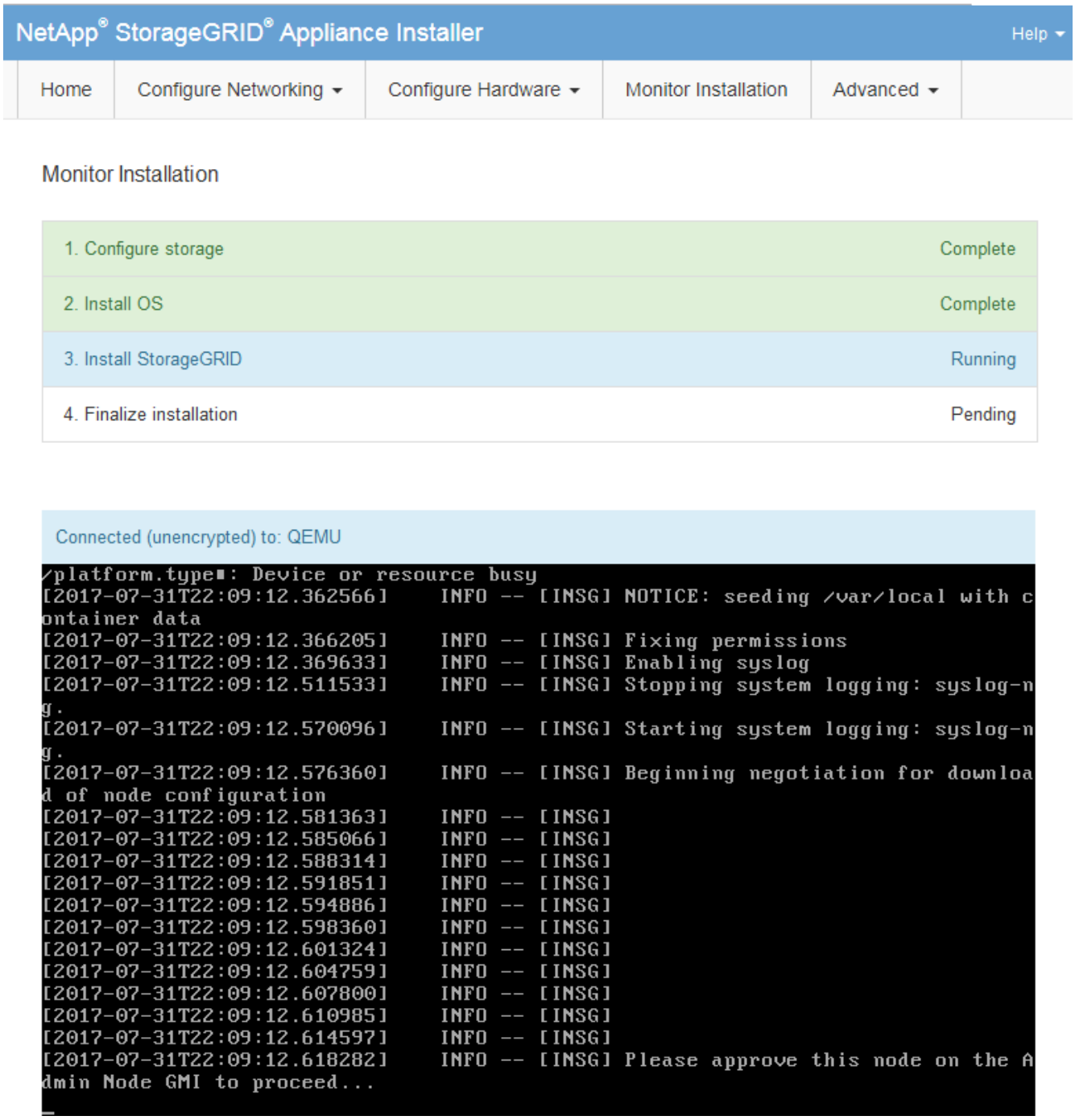
2. Esaminare i progressi delle prime due fasi dell'installazione.
   - **1. Configurare lo storage**

     Durante questa fase, il programma di installazione si connette al controller dello storage, cancella qualsiasi configurazione esistente, comunica con il sistema operativo SANtricity per configurare i volumi e configura le impostazioni dell'host.

   - **2. Installare il sistema operativo**

     In questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID nell'appliance.

3. Continuare a monitorare lo stato di avanzamento dell'installazione fino a quando la fase **Install StorageGRID** (Installazione guidata) non viene interrotta e sulla console integrata viene visualizzato un messaggio che richiede di approvare questo nodo nel nodo di amministrazione utilizzando Gestione griglia.



4. Passare a. "Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di storage dell'appliance".

Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di storage dell'appliance

Selezionare Start Recovery (Avvia ripristino) in Grid Manager (Gestione griglia) per configurare un nodo di storage dell'appliance come sostituzione del nodo guasto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.

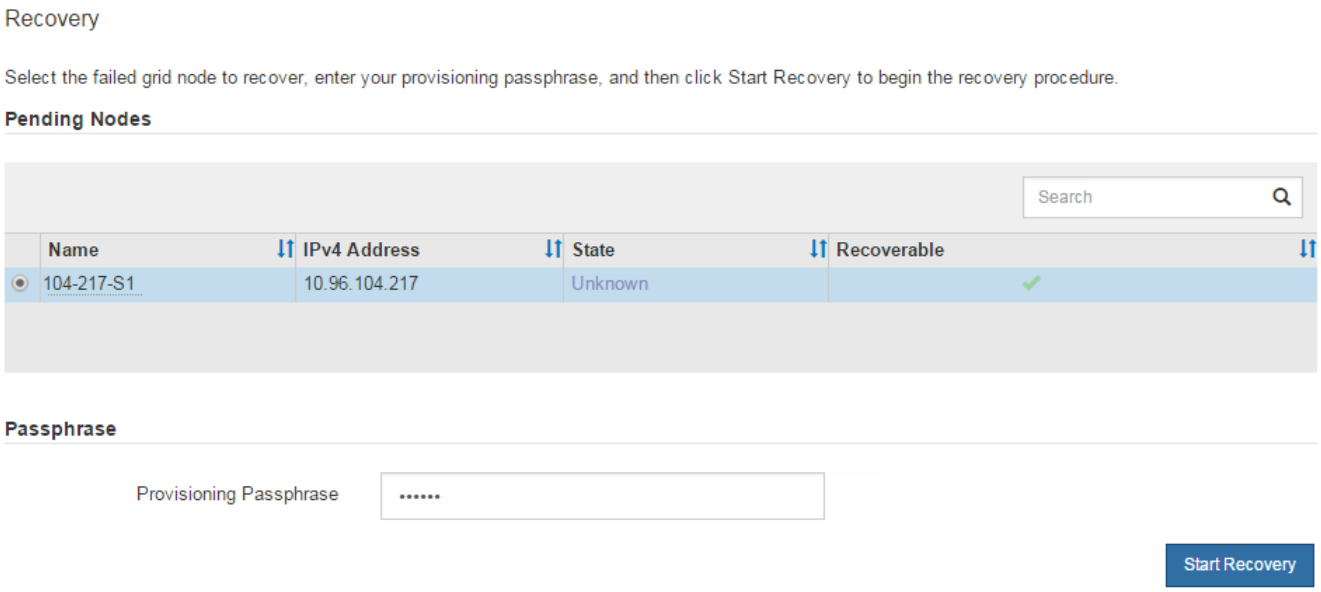
- Hai implementato un nodo storage dell'appliance di recovery.
- Si dispone della data di inizio di qualsiasi intervento di riparazione per i dati codificati per la cancellazione.
- Hai verificato che il nodo di storage non è stato ricostruito negli ultimi 15 giorni.

Fasi

1. In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **Ripristino**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

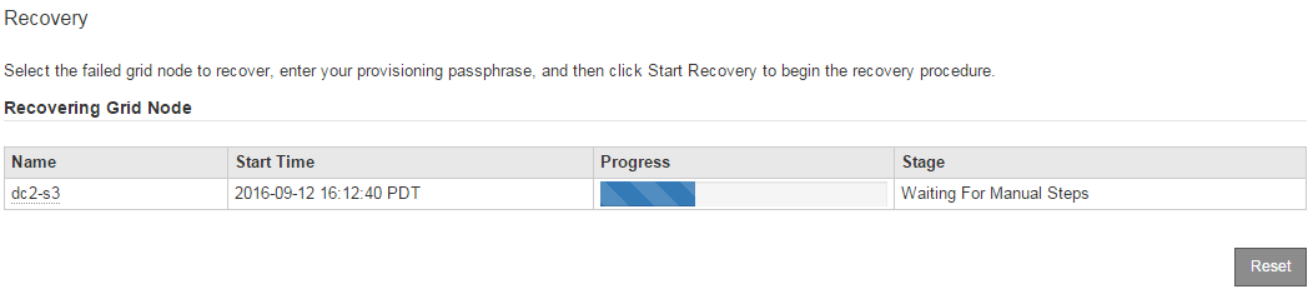
   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Immettere la **Provisioning Passphrase**.
4. Fare clic su **Start Recovery** (Avvia ripristino).

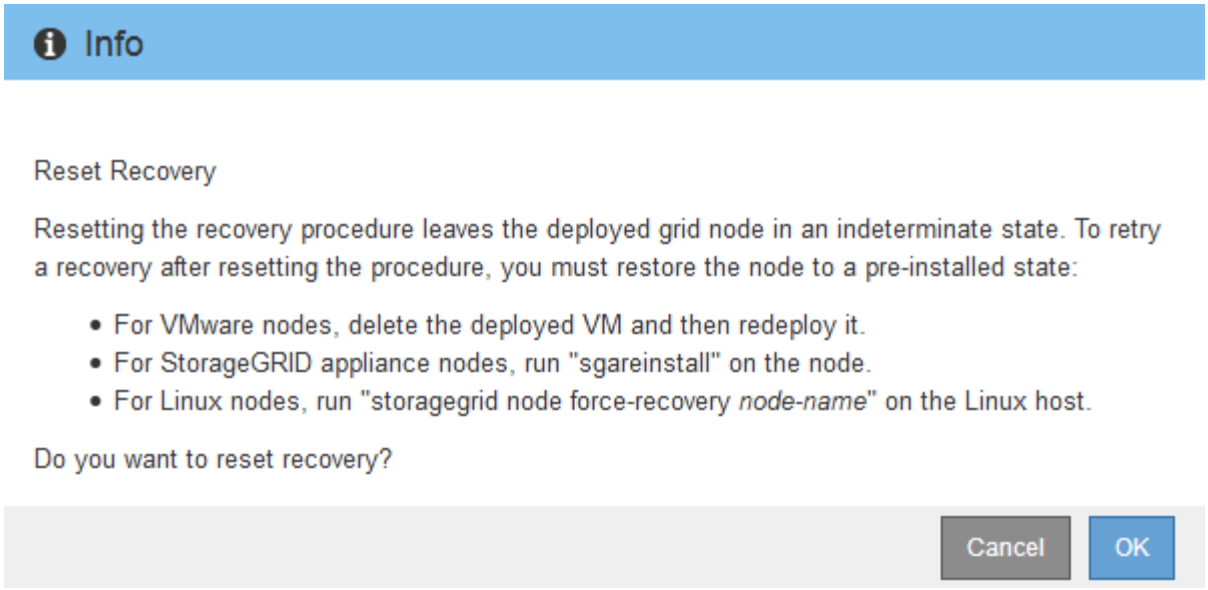


5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

   Quando il nodo grid raggiunge la fase "in attesa di passaggi manuali", passare all'argomento successivo ed eseguire i passaggi manuali per il rimontaggio e la riformattazione dei volumi di storage dell'appliance.



In qualsiasi momento durante il ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo appliance a uno stato preinstallato eseguendo `sgareinstall` sul nodo.

Rimontare e riformattare i volumi di storage delle appliance (procedura manuale)

È necessario eseguire manualmente due script per rimontare volumi di storage conservati e riformattare eventuali volumi di storage guasti. Il primo script consente di eseguire il remontaggio dei volumi correttamente formattati come volumi di storage StorageGRID. Il secondo script riformatta tutti i volumi non montati, ricostruisce il database Cassandra, se necessario, e avvia i servizi.

Prima di iniziare

- L'hardware è già stato sostituito per tutti i volumi di storage guasti che è necessario sostituire.

  Esecuzione di `sn-remount-volumes` lo script può aiutare a identificare altri volumi di storage guasti.

- È stato verificato che non è in corso la decommissionamento di un nodo di storage oppure che la procedura di decommissionamento del nodo è stata sospesa. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **smantellamento**).
- Hai verificato che non è in corso un'espansione. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **espansione**).

> ⚠ Contattare il supporto tecnico se più di un nodo di storage non è in linea o se un nodo di storage in questa griglia è stato ricostruito negli ultimi 15 giorni. Non eseguire `sn-recovery-postinstall.sh` script. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni l'uno dall'altro potrebbe causare la perdita di dati.

A proposito di questa attività

Per completare questa procedura, eseguire le seguenti attività di alto livello:

- Accedere al nodo di storage recuperato.
- Eseguire `sn-remount-volumes` script per il remount di volumi di storage correttamente formattati. Quando viene eseguito, lo script esegue le seguenti operazioni:

- Consente di montare e rimuovere ciascun volume di storage per riprodurre il journal XFS.
- Esegue un controllo di coerenza del file XFS.
- Se il file system è coerente, determina se il volume di storage è un volume di storage StorageGRID formattato correttamente.
- Se il volume di storage è formattato correttamente, esegue il remontaggio del volume di storage. Tutti i dati esistenti sul volume rimangono intatti.

- Esaminare l'output dello script e risolvere eventuali problemi.
- Eseguire `sn-recovery-postinstall.sh` script. Quando viene eseguito, lo script esegue le seguenti operazioni.

> Non riavviare un nodo di storage durante il ripristino prima dell'esecuzione `sn-recovery-postinstall.sh` (fase 4) per riformattare i volumi di storage guasti e ripristinare i metadati degli oggetti. Riavviare il nodo di storage prima `sn-recovery-postinstall.sh` Il completamento causa errori per i servizi che tentano di avviarsi e fa uscire i nodi dell'appliance StorageGRID dalla modalità di manutenzione.

- Consente di riformattare tutti i volumi di storage di `sn-remount-volumes` impossibile eseguire il montaggio dello script o che è stato trovato formattato in modo errato.

> Se un volume di storage viene riformattato, tutti i dati presenti in tale volume andranno persi. È necessario eseguire un'ulteriore procedura per ripristinare i dati degli oggetti da altre posizioni nella griglia, supponendo che le regole ILM siano state configurate per memorizzare più copie di un oggetto.

- Ricostruisce il database Cassandra sul nodo, se necessario.
- Avvia i servizi sul nodo di storage.

Fasi

1. Accedere al nodo di storage recuperato:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Eseguire il primo script per rimontare eventuali volumi di storage correttamente formattati.

   > Se tutti i volumi di storage sono nuovi e devono essere formattati, o se tutti i volumi di storage sono guasti, è possibile saltare questa fase ed eseguire il secondo script per riformattare tutti i volumi di storage non montati.

   a. Eseguire lo script: `sn-remount-volumes`

      Questo script potrebbe richiedere ore per essere eseguito su volumi di storage che contengono dati.

   b. Durante l'esecuzione dello script, esaminare l'output e rispondere alle richieste.

Se necessario, è possibile utilizzare `tail -f` per monitorare il contenuto del file di log dello script (`/var/local/log/sn-remount-volumes.log`) . Il file di log contiene informazioni più dettagliate rispetto all'output della riga di comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
```

```
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

Nell'output di esempio, un volume di storage è stato rimontato correttamente e tre volumi di storage hanno avuto errori.

- `/dev/sdb` Ha superato il controllo di coerenza del file system XFS e disponeva di una struttura di volume valida, quindi è stato rimontato correttamente. I dati sui dispositivi che vengono rimontati dallo script vengono conservati.
- `/dev/sdc` Verifica della coerenza del file system XFS non riuscita perché il volume di storage era nuovo o corrotto.
- `/dev/sdd` impossibile montare perché il disco non è stato inizializzato o il superblocco del disco è stato danneggiato. Quando lo script non riesce a montare un volume di storage, chiede se si desidera eseguire il controllo di coerenza del file system.
  - Se il volume di storage è collegato a un nuovo disco, rispondere **N** alla richiesta. Non è necessario controllare il file system su un nuovo disco.
  - Se il volume di storage è collegato a un disco esistente, rispondere **Y** alla richiesta. È possibile utilizzare i risultati del controllo del file system per determinare l'origine del danneggiamento. I

risultati vengono salvati in `/var/local/log/sn-remount-volumes.log` file di log.

- `/dev/sde` Ha superato la verifica di coerenza del file system XFS e disponeva di una struttura di volume valida; tuttavia, l'ID del nodo LDR in `volID` Il file non corrisponde all'ID per questo nodo di storage (il `configured LDR noid` visualizzato nella parte superiore). Questo messaggio indica che questo volume appartiene a un altro nodo di storage.

3. Esaminare l'output dello script e risolvere eventuali problemi.

> Se un volume di storage non ha superato il controllo di coerenza del file system XFS o non è stato possibile montarlo, esaminare attentamente i messaggi di errore nell'output. È necessario comprendere le implicazioni dell'esecuzione di `sn-recovery-postinstall.sh` creare script su questi volumi.

a. Verificare che i risultati includano una voce per tutti i volumi previsti. Se alcuni volumi non sono elencati, eseguire nuovamente lo script.

b. Esaminare i messaggi per tutti i dispositivi montati. Assicurarsi che non vi siano errori che indichino che un volume di storage non appartiene a questo nodo di storage.

   Nell'esempio, l'output per /dev/sde include il seguente messaggio di errore:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> Se un volume di storage viene segnalato come appartenente a un altro nodo di storage, contattare il supporto tecnico. Se si esegue `sn-recovery-postinstall.sh` script, il volume di storage verrà riformattato, causando la perdita di dati.

c. Se non è stato possibile montare alcun dispositivo di storage, annotare il nome del dispositivo e riparare o sostituire il dispositivo.

> È necessario riparare o sostituire i dispositivi di storage che non possono essere montati.

   Il nome del dispositivo viene utilizzato per cercare l'ID del volume, che è necessario immettere quando si esegue `repair-data` script per ripristinare i dati dell'oggetto nel volume (la procedura successiva).

d. Dopo aver riparato o sostituito tutti i dispositivi non montabili, eseguire `sn-remount-volumes` eseguire nuovamente lo script per confermare che tutti i volumi di storage che possono essere rimontati sono stati rimontati.

> Se un volume di storage non può essere montato o non è formattato correttamente e si passa alla fase successiva, il volume e i dati presenti nel volume verranno eliminati. Se si dispone di due copie di dati oggetto, si disporrà di una sola copia fino al completamento della procedura successiva (ripristino dei dati oggetto).

Non eseguire `sn-recovery-postinstall.sh` Eseguire uno script se si ritiene che i dati rimanenti su un volume di storage guasto non possano essere ricostruiti da un'altra parte della griglia (ad esempio, se il criterio ILM utilizza una regola che esegue una sola copia o se i volumi sono guasti su più nodi). Contattare invece il supporto tecnico per determinare come ripristinare i dati.

4. Eseguire `sn-recovery-postinstall.sh` script: `sn-recovery-postinstall.sh`

   Questo script riformatta tutti i volumi di storage che non possono essere montati o che sono stati trovati per essere formattati in modo non corretto; ricostruisce il database Cassandra sul nodo, se necessario; avvia i servizi sul nodo di storage.

   Tenere presente quanto segue:

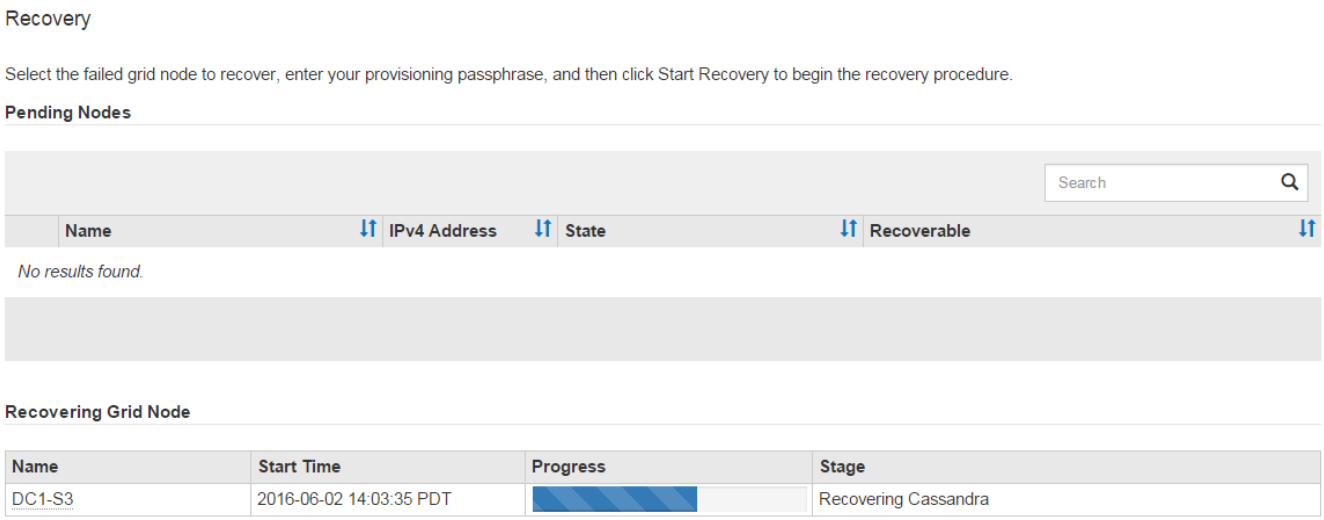
   - L'esecuzione dello script potrebbe richiedere ore.
   - In generale, si consiglia di lasciare la sessione SSH da sola mentre lo script è in esecuzione.
   - Non premere **Ctrl+C** mentre la sessione SSH è attiva.
   - Lo script viene eseguito in background se si verifica un'interruzione della rete e termina la sessione SSH, ma è possibile visualizzarne l'avanzamento dalla pagina Recovery (Ripristino).
   - Se Storage Node utilizza il servizio RSM, lo script potrebbe sembrare bloccato per 5 minuti quando i servizi del nodo vengono riavviati. Questo ritardo di 5 minuti è previsto ogni volta che il servizio RSM viene avviato per la prima volta.

     Il servizio RSM è presente sui nodi di storage che includono il servizio ADC.

   Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "riparazione Cassandra". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

5. Come `sn-recovery-postinstall.sh` Viene eseguito lo script, monitorare la pagina Recovery in Grid Manager.

   La barra di avanzamento e la colonna fase della pagina di ripristino forniscono uno stato di alto livello di `sn-recovery-postinstall.sh` script.



6. Dopo il `sn-recovery-postinstall.sh` lo script ha avviato i servizi sul nodo, è possibile ripristinare i dati degli oggetti su qualsiasi volume di storage formattato dallo script.

   Lo script chiede se si desidera utilizzare il processo di ripristino del volume di Grid Manager.

   - Nella maggior parte dei casi, dovresti "Ripristinare i dati degli oggetti utilizzando Grid Manager". Risposta `y` Per utilizzare Grid Manager.
   - In rari casi, ad esempio quando richiesto dal supporto tecnico o quando si sa che il nodo sostitutivo ha meno volumi disponibili per lo storage a oggetti rispetto al nodo originale, è necessario "ripristinare manualmente i dati dell'oggetto" utilizzando il `repair-data` script. Se si verifica uno di questi casi, rispondere `n`.

   > Se rispondi `n` Per utilizzare il processo di ripristino del volume di Grid Manager (ripristinare manualmente i dati degli oggetti):
   >
   > - Non è possibile ripristinare i dati degli oggetti utilizzando Grid Manager.
   > - È possibile monitorare l'avanzamento dei lavori di ripristino manuale utilizzando Grid Manager.

   Dopo aver effettuato la selezione, lo script viene completato e vengono visualizzati i passaggi successivi per recuperare i dati dell'oggetto. Dopo aver esaminato questi passaggi, premere un tasto qualsiasi per tornare alla riga di comando.

Ripristinare i dati dell'oggetto nel volume di storage per l'appliance

Dopo il ripristino dei volumi di storage per il nodo di storage dell'appliance, è possibile ripristinare i dati degli oggetti replicati o codificati in cancellazione che sono stati persi in caso di guasto del nodo di storage.

Quale procedura è necessario utilizzare?

Se possibile, ripristinare i dati dell'oggetto utilizzando la pagina **Volume Restore** in Grid Manager.

- Se i volumi sono elencati in **MANUTENZIONE** > **Ripristino volume** > **nodi da ripristinare**, ripristinare i dati degli oggetti utilizzando "Pagina di ripristino dei volumi in Grid Manager".

- Se i volumi non sono elencati in **MANUTENZIONE** > **Ripristino volume** > **nodi da ripristinare**, seguire la procedura riportata di seguito per l'utilizzo di `repair-data` script per ripristinare i dati dell'oggetto.

  Se il nodo di storage recuperato contiene un numero inferiore di volumi rispetto al nodo che sta sostituendo, è necessario utilizzare `repair-data` script.

> Lo script dei dati di riparazione è obsoleto e verrà rimosso in una versione futura. Se possibile, utilizzare "Procedura di ripristino del volume in Grid Manager".

Utilizzare `repair-data` script per ripristinare i dati dell'oggetto

Prima di iniziare

- È stato confermato che il nodo di archiviazione recuperato ha uno stato di connessione **connesso** Nella scheda **NODI** > **Panoramica** di Grid Manager.

A proposito di questa attività

I dati degli oggetti possono essere ripristinati da altri nodi di storage, da un nodo di archiviazione o da un pool di storage cloud, supponendo che le regole ILM del grid siano state configurate in modo da rendere disponibili le copie degli oggetti.

Tenere presente quanto segue:

- Se una regola ILM è stata configurata per memorizzare solo una copia replicata e tale copia esisteva su un volume di storage che non ha superato il test, non sarà possibile ripristinare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto. Prima di eseguire questa procedura, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi di ripristino e dei relativi costi.
- Se l'unica copia rimanente di un oggetto si trova su un nodo di archiviazione, i dati dell'oggetto vengono recuperati dal nodo di archiviazione. Il ripristino dei dati degli oggetti in un nodo di storage da un nodo di archiviazione richiede più tempo rispetto al ripristino delle copie da altri nodi di storage a causa della latenza associata ai recuperi da sistemi di storage di archiviazione esterni.

A proposito di `repair-data` script

Per ripristinare i dati dell'oggetto, eseguire `repair-data` script. Questo script inizia il processo di ripristino dei dati degli oggetti e lavora con la scansione ILM per garantire che le regole ILM siano soddisfatte.

Selezionare **Replicated data** o **Erasure-Coded (EC) data** per apprendere le diverse opzioni di `repair-data` script, in base al ripristino di dati replicati o a dati con codifica di cancellazione. Se è necessario ripristinare entrambi i tipi di dati, è necessario eseguire entrambi i set di comandi.

> Per ulteriori informazioni su `repair-data` script, invio `repair-data --help` Dalla riga di comando del nodo di amministrazione primario.

> Lo script dei dati di riparazione è obsoleto e verrà rimosso in una versione futura. Se possibile, utilizzare "Procedura di ripristino del volume in Grid Manager".

Dati replicati

Sono disponibili due comandi per il ripristino dei dati replicati, a seconda che sia necessario riparare l'intero nodo o solo alcuni volumi sul nodo:

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

È possibile tenere traccia delle riparazioni dei dati replicati con questo comando:

```
repair-data show-replicated-repair-status
```

Dati con erasure coding (EC)

Sono disponibili due comandi per il ripristino dei dati con codifica erasure, a seconda che sia necessario riparare l'intero nodo o solo determinati volumi sul nodo:

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

È possibile tenere traccia delle riparazioni dei dati con codifica per la cancellazione con questo comando:

```
repair-data show-ec-repair-status
```

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. Tuttavia, se non è possibile tenere conto di tutti i dati con codice di cancellazione, la riparazione non può essere completata. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

> Il lavoro di riparazione EC riserva temporaneamente una grande quantità di storage. Gli avvisi relativi allo storage potrebbero essere attivati, ma verranno risolti al termine della riparazione. Se lo storage non è sufficiente per la prenotazione, il lavoro di riparazione EC non avrà esito positivo. Le prenotazioni di storage vengono rilasciate al termine del lavoro di riparazione EC, indipendentemente dal fatto che il lavoro abbia avuto esito negativo o positivo.

Trovare il nome host per il nodo di storage

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Utilizzare `/etc/hosts` File per trovare il nome host del nodo di storage per i volumi di storage ripristinati. Per visualizzare un elenco di tutti i nodi nella griglia, immettere quanto segue: `cat /etc/hosts`.

Riparare i dati se tutti i volumi sono guasti

Se tutti i volumi di storage si sono guastati, riparare l'intero nodo. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codifica di cancellazione (EC) o entrambi.

Se solo alcuni volumi hanno avuto problemi, passare a. Riparare i dati se solo alcuni volumi sono guasti.

> Non puoi correre `repair-data` operazioni per più di un nodo contemporaneamente. Per ripristinare più nodi, contattare il supporto tecnico.

Dati replicati

Se la griglia include dati replicati, utilizzare `repair-data start-replicated-node-repair` con il `--nodes` opzione, dove `--nodes` È il nome host (nome di sistema) per riparare l'intero nodo di storage.

Questo comando ripara i dati replicati su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non riesce a individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. È necessario determinare la causa della perdita e se è possibile eseguire il ripristino. Vedere "Esaminare gli oggetti persi".

Dati con erasure coding (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `repair-data start-ec-node-repair` con il `--nodes` opzione, dove `--nodes` È il nome host (nome di sistema) per riparare l'intero nodo di storage.

Questo comando ripara i dati con codifica di cancellazione su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Riparare i dati se solo alcuni volumi sono guasti

Se solo alcuni volumi hanno avuto problemi, riparare i volumi interessati. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codifica di cancellazione (EC) o entrambi.

Se tutti i volumi non sono riusciti, passare a. Riparare i dati se tutti i volumi sono guasti.

Inserire gli ID del volume in formato esadecimale. Ad esempio, `0000` è il primo volume e. `000F` è il sedicesimo

volume. È possibile specificare un volume, un intervallo di volumi o più volumi che non si trovano in una sequenza.

Tutti i volumi devono trovarsi sullo stesso nodo di storage. Se è necessario ripristinare i volumi per più di un nodo di storage, contattare il supporto tecnico.

Dati replicati

Se la griglia contiene dati replicati, utilizzare `start-replicated-volume-repair` con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati replicati nel volume `0002` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati replicati in tutti i volumi dell'intervallo `0003` a. `0009` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Volumi multipli non in sequenza: Questo comando ripristina i dati replicati nei volumi `0001`, `0005`, e. `0008` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non riesce a individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. Prendere nota della descrizione dell'avviso e delle azioni consigliate per determinare la causa della perdita e se è possibile eseguire il ripristino.

Dati con erasure coding (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `start-ec-volume-repair` con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati con codifica erasure nel volume `0007` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati con codifica di cancellazione su tutti i volumi dell'intervallo `0004` a. `0006` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Volumi multipli non in sequenza: Questo comando ripristina i dati con codifica erasure nei volumi `000A`, `000C`, e. `000E` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Il `repair-data` l'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di

ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Monitorare le riparazioni

Monitorare lo stato dei lavori di riparazione, in base all'utilizzo di **dati replicati**, **dati EC (erasure-coded)** o entrambi.

È inoltre possibile monitorare lo stato dei lavori di ripristino dei volumi in corso e visualizzare la cronologia dei lavori di ripristino completati in "Grid Manager".

Dati replicati

- Per ottenere una percentuale di completamento stimata per la riparazione replicata, aggiungere `show-replicated-repair-status` al comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Per determinare se le riparazioni sono state completate:
  a. Selezionare **NODI** > ***nodo di storage in riparazione*** > **ILM**.
  b. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
  a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
  b. Selezionare ***Grid*** > ***Storage Node in riparazione*** > **LDR** > **Data Store**.
  c. Utilizzare una combinazione dei seguenti attributi per determinare, come possibile, se le riparazioni replicate sono complete.

  > Le incongruenze di Cassandra potrebbero essere presenti e le riparazioni non riuscite non vengono monitorate.

  - **Tentativi di riparazione (XRPA)**: Utilizzare questo attributo per tenere traccia dell'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo superiore al periodo di scansione corrente (fornito dall'attributo **Scan Period — Estimated**), significa che la scansione ILM non ha rilevato oggetti ad alto rischio che devono essere riparati su alcun nodo.

    > Gli oggetti ad alto rischio sono oggetti che rischiano di essere completamente persi. Non sono inclusi oggetti che non soddisfano la configurazione ILM.

  - **Periodo di scansione — stimato (XSCM)**: Utilizzare questo attributo per stimare quando verrà applicata una modifica di policy agli oggetti precedentemente acquisiti. Se l'attributo **riparazioni tentate** non aumenta per un periodo superiore al periodo di scansione corrente, è probabile che vengano eseguite riparazioni replicate. Si noti che il periodo di scansione può cambiare. L'attributo **Scan Period — Estimated (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione del nodo. È possibile eseguire una query nella cronologia degli attributi **Scan Period — Estimated** per la griglia per determinare un intervallo di tempo appropriato.

Dati con erasure coding (EC)

Per monitorare la riparazione dei dati con codifica erasure e riprovare eventuali richieste che potrebbero non essere riuscite:

1. Determinare lo stato delle riparazioni dei dati con codice di cancellazione:
   - Selezionare **SUPPORTO** > **Strumenti** > **metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).

- Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` funzionamento:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilizzare questo comando per elencare tutte le riparazioni:

  ```
  repair-data show-ec-repair-status
  ```

L'output elenca le informazioni, tra cui `repair ID`, per tutte le riparazioni precedentemente e attualmente in esecuzione.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

   Questo comando prova di nuovo una riparazione del nodo non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Questo comando prova di nuovo una riparazione del volume non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Controllare lo stato dello storage dopo il ripristino del nodo di storage dell'appliance

Dopo aver ripristinato un nodo di storage dell'appliance, è necessario verificare che lo stato desiderato del nodo di storage dell'appliance sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che si riavvia il server del nodo di storage.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Il nodo di storage è stato ripristinato e il ripristino dei dati è stato completato.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Controllare i valori di **Recovery Storage Node** > **LDR** > **Storage** > **Storage state — Desired** e **Storage state — Current**.

   Il valore di entrambi gli attributi deve essere Online.

3. Se lo stato di storage — desiderato è impostato su sola lettura, attenersi alla seguente procedura:
   a. Fare clic sulla scheda **Configurazione**.
   b. Dall'elenco a discesa **Storage state — Desired** (Stato storage — desiderato*), selezionare **Online**.
   c. Fare clic su **Applica modifiche**.
   d. Fare clic sulla scheda **Panoramica** e verificare che i valori di **Stato dello storage — desiderato** e **Stato dello storage — corrente** siano aggiornati a Online.

Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto

Eseguire il ripristino da un errore del volume di storage in cui l'unità di sistema è intatta: Panoramica

È necessario completare una serie di attività per ripristinare un nodo di storage basato su software in cui uno o più volumi di storage sul nodo di storage si sono guastati, ma il disco di sistema è intatto. Se solo i volumi di storage sono guasti, il nodo di storage è ancora disponibile per il sistema StorageGRID.

> Questa procedura di ripristino si applica solo ai nodi di storage basati su software. Se i volumi di storage si sono guastati su un nodo di storage dell'appliance, utilizzare la procedura dell'appliance: "Ripristinare il nodo storage dell'appliance".

Questa procedura di ripristino include le seguenti attività:

- "Esaminare gli avvisi per il ripristino del volume di archiviazione"
- "Identificare e smontare i volumi di storage guasti"
- "Recuperare i volumi e ricostruire il database Cassandra"
- "Ripristinare i dati degli oggetti"
- "Controllare lo stato di memorizzazione"

Avvertenze per il ripristino del volume di archiviazione

Prima di ripristinare volumi di archiviazione non riusciti per un nodo di archiviazione, esaminare i seguenti avvisi.

I volumi di storage (o rangedb) in un nodo di storage sono identificati da un numero esadecimale, noto come ID del volume. Ad esempio, 0000 è il primo volume e 000F è il sedicesimo volume. Il primo archivio di oggetti (volume 0) su ciascun nodo di storage utilizza fino a 4 TB di spazio per i metadati degli oggetti e le operazioni del database Cassandra; qualsiasi spazio rimanente su tale volume viene utilizzato per i dati degli oggetti. Tutti gli altri volumi di storage vengono utilizzati esclusivamente per i dati a oggetti.

Se il volume 0 non funziona e deve essere ripristinato, il database Cassandra potrebbe essere ricostruito come parte della procedura di ripristino del volume. Cassandra potrebbe essere ricostruita anche nelle seguenti circostanze:

- Un nodo di storage viene riportato online dopo essere stato offline per più di 15 giorni.
- Il disco di sistema e uno o più volumi di storage si guastano e vengono ripristinati.

Quando Cassandra viene ricostruita, il sistema utilizza le informazioni provenienti da altri nodi di storage. Se troppi nodi di storage sono offline, alcuni dati Cassandra potrebbero non essere disponibili. Se Cassandra è stata ricostruita di recente, i dati Cassandra potrebbero non essere ancora coerenti in tutta la griglia. La perdita di dati può verificarsi se Cassandra viene ricostruita quando troppi nodi di storage sono offline o se due o più nodi di storage vengono ricostruiti entro 15 giorni l'uno dall'altro.

> Se più di un nodo di storage si è guastato (o non è in linea), contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

Se si tratta del secondo guasto del nodo di storage in meno di 15 giorni dopo un guasto o un ripristino del nodo di storage, contattare il supporto tecnico. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni può causare la perdita di dati.

Se più di un nodo di storage in un sito si è guastato, potrebbe essere necessaria una procedura di ripristino del sito. Vedere "Come il supporto tecnico recupera un sito".

Se le regole ILM sono configurate in modo da memorizzare una sola copia replicata e la copia esiste su un volume di storage che ha avuto esito negativo, non sarà possibile ripristinare l'oggetto.

Se si verifica un allarme Services: Status - Cassandra (SVST) durante il ripristino, vedere "Ripristinare i volumi di storage guasti e ricostruire il database Cassandra". Dopo la ricostruzione di Cassandra, gli allarmi devono essere disattivati. Se gli allarmi non vengono disattivati, contattare il supporto tecnico.

Informazioni correlate

"Avvertenze e considerazioni per il ripristino del nodo grid"

Identificare e smontare i volumi di storage guasti

Durante il ripristino di un nodo di storage con volumi di storage guasti, è necessario identificare e smontare i volumi guasti. È necessario verificare che solo i volumi di storage guasti vengano riformattati come parte della procedura di ripristino.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

È necessario ripristinare i volumi di storage guasti il prima possibile.

La prima fase del processo di ripristino consiste nel rilevare i volumi che sono stati scollegati, che devono essere disinstallati o che presentano errori di i/O. Se i volumi guasti sono ancora collegati ma hanno un file system corrotto in modo casuale, il sistema potrebbe non rilevare alcun danneggiamento nelle parti del disco non utilizzate o non allocate.

È necessario completare questa procedura prima di eseguire la procedura manuale per ripristinare i volumi, ad esempio aggiungere o ricollegare i dischi, arrestare il nodo, avviare il nodo o riavviare. In caso contrario, quando si esegue `reformat_storage_block_devices.rb` script, potrebbe verificarsi un errore del file system che causa il blocco o l'errore dello script.

Riparare l'hardware e collegare correttamente i dischi prima di eseguire `reboot` comando.

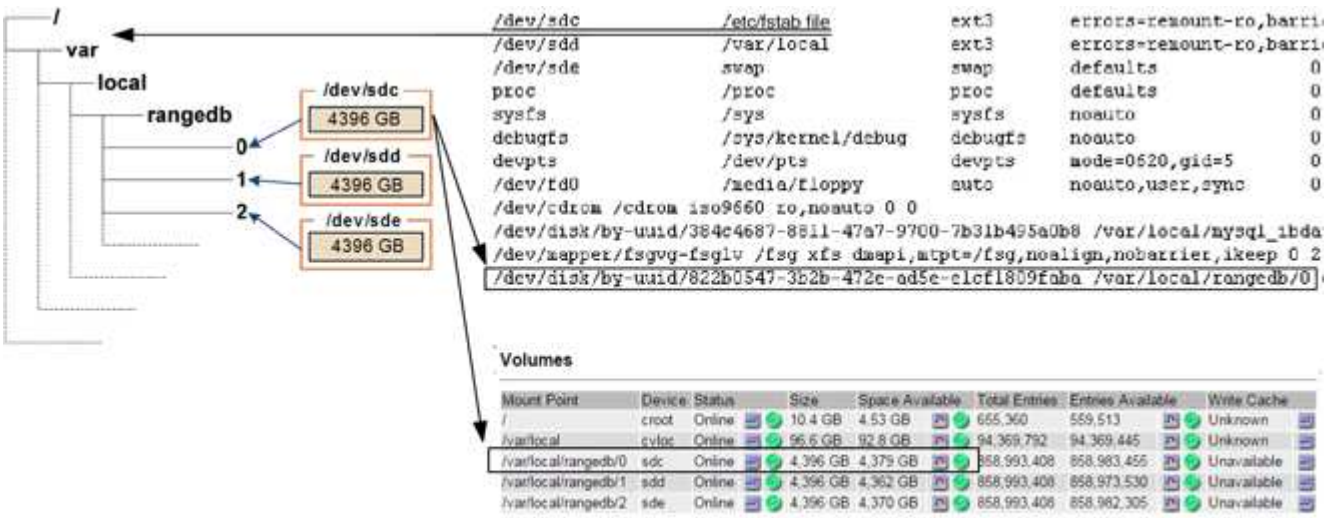
Identificare con attenzione i volumi di storage guasti. Queste informazioni verranno utilizzate per verificare quali volumi devono essere riformattati. Dopo la riformattazione di un volume, i dati del volume non possono essere recuperati.

Per ripristinare correttamente i volumi di storage guasti, è necessario conoscere i nomi dei dispositivi dei

volumi di storage guasti e i relativi ID dei volumi.

Al momento dell'installazione, a ciascun dispositivo di storage viene assegnato un UID (Universal Unique Identifier) del file system e viene montato in una directory rangedb sul nodo di storage utilizzando l'UID del file system assegnato. L'UUID del file system e la directory rangedb sono elencati in `/etc/fstab` file. Il nome del dispositivo, la directory rangedb e le dimensioni del volume montato vengono visualizzati in Grid Manager.

Nell'esempio seguente, dispositivo `/dev/sdc` Ha un volume di 4 TB, è montato su `/var/local/rangedb/0`, utilizzando il nome del dispositivo `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` in `/etc/fstab` file:



Fasi

1. Completare i seguenti passaggi per registrare i volumi di storage guasti e i relativi nomi dei dispositivi:

   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.

   b. Selezionare **sito** > **nodo di storage guasto** > **LDR** > **Storage** > **Panoramica** > **principale** e cercare gli archivi di oggetti con allarmi.

   Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

   c. Selezionare **sito** > **nodo storage guasto** > **SSM** > **risorse** > **Panoramica** > **principale**. Determinare il punto di montaggio e le dimensioni del volume di ciascun volume di storage guasto identificato nel passaggio precedente.

      Gli archivi di oggetti sono numerati in notazione esadecimale. Ad esempio, 0000 è il primo volume e 000F è il sedicesimo volume. Nell'esempio, l'archivio di oggetti con un ID di 0000 corrisponde a. `/var/local/rangedb/0` Con nome periferica sdc e una dimensione di 107 GB.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. Accedere al nodo di storage guasto:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

3. Eseguire il seguente script per smontare un volume di storage guasto:

   ```
   sn-unmount-volume object_store_ID
   ```

   Il `object_store_ID` È l'ID del volume di storage guasto. Ad esempio, specificare `0` Nel comando per un archivio di oggetti con ID 0000.

4. Se richiesto, premere **y** per arrestare il servizio Cassandra a seconda del volume di storage 0.

   Se il servizio Cassandra è già stato arrestato, non viene richiesto. Il servizio Cassandra viene arrestato solo per il volume 0.

   ```
   root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
   Services depending on storage volume 0 (cassandra) aren't down.
   Services depending on storage volume 0 must be stopped before running
   this script.
   Stop services that require storage volume 0 [y/N]? y
   Shutting down services that require storage volume 0.
   Services requiring storage volume 0 stopped.
   Unmounting /var/local/rangedb/0
   /var/local/rangedb/0 is unmounted.
   ```

   In pochi secondi, il volume viene dismontato. Vengono visualizzati messaggi che indicano ogni fase del processo. Il messaggio finale indica che il volume è stato dismontato.

5. Se il dismount non riesce a causa di un volume occupato, è possibile forzare il dismount utilizzando `--use -umountof` opzione:

   Forzatura di uno smontaggio mediante `--use-umountof` l'opzione potrebbe causare un comportamento imprevisto o un blocco dei processi o dei servizi che utilizzano il volume.

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

Ripristinare i volumi di storage guasti e ricostruire il database Cassandra

È necessario eseguire uno script che riformatta e rimontana lo storage su volumi di storage guasti e ricostruisce il database Cassandra sul nodo di storage, se il sistema lo ritiene necessario.

Prima di iniziare

- Hai il `Passwords.txt` file.
- I dischi di sistema sul server sono intatti.
- La causa del guasto è stata identificata e, se necessario, l'hardware di storage sostitutivo è già stato acquistato.
- Le dimensioni totali dello storage sostitutivo sono le stesse dell'originale.
- È stato verificato che non è in corso la decommissionamento di un nodo di storage oppure che la procedura di decommissionamento del nodo è stata sospesa. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **smantellamento**).
- Hai verificato che non è in corso un'espansione. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **espansione**).
- Lo hai fatto "analisi degli avvisi relativi al ripristino del volume di storage".

Fasi

1. Se necessario, sostituire lo storage fisico o virtuale guasto associato ai volumi di storage guasti identificati e non montati in precedenza.

   Non rimontare i volumi in questa fase. Lo storage viene rimontato e aggiunto a. `/etc/fstab` in un passaggio successivo.

2. In Grid Manager, andare a **NODES** > **`appliance Storage Node`** > **hardware**. Nella sezione dell'appliance StorageGRID della pagina, verificare che la modalità RAID dello storage sia corretta.
3. Accedere al nodo di storage guasto:
   a. Immettere il seguente comando: `ssh admin@`*`grid_node_IP`*
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

4. Utilizzare un editor di testo (vi o vim) per eliminare i volumi guasti da `/etc/fstab` quindi salvare il file.

Commenti su un volume guasto in `/etc/fstab` file insufficiente. Il volume deve essere cancellato da `fstab` mentre il processo di ripristino verifica che tutte le linee in `fstab` il file corrisponde ai file system montati.

5. Riformattare eventuali volumi di storage guasti e ricostruire il database Cassandra, se necessario. Inserire: `reformat_storage_block_devices.rb`
   - Quando il volume di storage 0 viene dismontato, vengono visualizzati messaggi e messaggi che indicano che il servizio Cassandra è in fase di arresto.
   - Se necessario, viene richiesto di ricostruire il database Cassandra.
     - Esaminare gli avvisi. Se non sono applicabili, ricostruire il database Cassandra. Immettere: **Y**
     - Se più di un nodo di storage non è in linea o se un altro nodo di storage è stato ricostruito negli ultimi 15 giorni. Immettere: **N**

       Lo script verrà chiuso senza ricostruire Cassandra. Contattare il supporto tecnico.
   - Per ogni disco rangedb sul nodo di storage, quando viene richiesto: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, immettere una delle seguenti risposte:
     - **y** per riformattare un disco con errori. In questo modo, il volume di storage viene riformattato e il volume di storage riformattato viene aggiunto a. `/etc/fstab` file.
     - **n** se il disco non contiene errori e non si desidera riformattarlo.

       Selezionando **n** si esce dallo script. Montare il disco (se si ritiene che i dati sul disco debbano essere conservati e il disco non è stato montato per errore) oppure rimuoverlo. Quindi, eseguire `reformat_storage_block_devices.rb` di nuovo comando.

       Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "riparazione Cassandra". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

     Nel seguente esempio di output, il disco `/dev/sdf` Deve essere riformattato e Cassandra non ha bisogno di essere ricostruito:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done.  Now do manual steps to
restore copies of data.
```

Una volta riformattati e rimontati i volumi di storage e completate le operazioni Cassandra necessarie, è possibile "Ripristinare i dati degli oggetti utilizzando Grid Manager".

Ripristinare i dati degli oggetti nel volume di storage in cui il disco di sistema è intatto

Dopo il ripristino di un volume di storage su un nodo di storage in cui il disco di sistema è intatto, è possibile ripristinare i dati degli oggetti replicati o codificati in cancellazione che sono stati persi in caso di guasto del volume di storage.

Quale procedura è necessario utilizzare?

Se possibile, ripristinare i dati dell'oggetto utilizzando la pagina **Volume Restore** in Grid Manager.

- Se i volumi sono elencati in **MANUTENZIONE** > **Ripristino volume** > **nodi da ripristinare**, ripristinare i dati degli oggetti utilizzando "Pagina di ripristino dei volumi in Grid Manager".
- Se i volumi non sono elencati in **MANUTENZIONE** > **Ripristino volume** > **nodi da ripristinare**, seguire la procedura riportata di seguito per l'utilizzo di `repair-data` script per ripristinare i dati dell'oggetto.

  Se il nodo di storage recuperato contiene un numero inferiore di volumi rispetto al nodo che sta sostituendo, è necessario utilizzare `repair-data` script.

> Lo script dei dati di riparazione è obsoleto e verrà rimosso in una versione futura. Se possibile, utilizzare "Procedura di ripristino del volume in Grid Manager".

Utilizzare `repair-data` script per ripristinare i dati dell'oggetto

Prima di iniziare

- È stato confermato che il nodo di archiviazione recuperato ha uno stato di connessione **connesso** Nella scheda **NODI** > **Panoramica** di Grid Manager.

A proposito di questa attività

I dati degli oggetti possono essere ripristinati da altri nodi di storage, da un nodo di archiviazione o da un pool di storage cloud, supponendo che le regole ILM del grid siano state configurate in modo da rendere disponibili le copie degli oggetti.

Tenere presente quanto segue:

- Se una regola ILM è stata configurata per memorizzare solo una copia replicata e tale copia esisteva su un volume di storage che non ha superato il test, non sarà possibile ripristinare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto. Prima di eseguire questa procedura, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi di ripristino e dei relativi costi.
- Se l'unica copia rimanente di un oggetto si trova su un nodo di archiviazione, i dati dell'oggetto vengono recuperati dal nodo di archiviazione. Il ripristino dei dati degli oggetti in un nodo di storage da un nodo di archiviazione richiede più tempo rispetto al ripristino delle copie da altri nodi di storage a causa della latenza associata ai recuperi da sistemi di storage di archiviazione esterni.

A proposito di `repair-data` script

Per ripristinare i dati dell'oggetto, eseguire `repair-data` script. Questo script inizia il processo di ripristino dei dati degli oggetti e lavora con la scansione ILM per garantire che le regole ILM siano soddisfatte.

Selezionare **Replicated data** o **Erasure-Coded (EC) data** per apprendere le diverse opzioni di `repair-data` script, in base al ripristino di dati replicati o a dati con codifica di cancellazione. Se è necessario ripristinare entrambi i tipi di dati, è necessario eseguire entrambi i set di comandi.

> Per ulteriori informazioni su `repair-data` script, invio `repair-data --help` Dalla riga di comando del nodo di amministrazione primario.

> Lo script dei dati di riparazione è obsoleto e verrà rimosso in una versione futura. Se possibile, utilizzare "Procedura di ripristino del volume in Grid Manager".

Dati replicati

Sono disponibili due comandi per il ripristino dei dati replicati, a seconda che sia necessario riparare l'intero nodo o solo alcuni volumi sul nodo:

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

È possibile tenere traccia delle riparazioni dei dati replicati con questo comando:

```
repair-data show-replicated-repair-status
```

Dati con erasure coding (EC)

Sono disponibili due comandi per il ripristino dei dati con codifica erasure, a seconda che sia necessario riparare l'intero nodo o solo determinati volumi sul nodo:

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

È possibile tenere traccia delle riparazioni dei dati con codifica per la cancellazione con questo comando:

```
repair-data show-ec-repair-status
```

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. Tuttavia, se non è possibile tenere conto di tutti i dati con codice di cancellazione, la riparazione non può essere completata. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

> Il lavoro di riparazione EC riserva temporaneamente una grande quantità di storage. Gli avvisi relativi allo storage potrebbero essere attivati, ma verranno risolti al termine della riparazione. Se lo storage non è sufficiente per la prenotazione, il lavoro di riparazione EC non avrà esito positivo. Le prenotazioni di storage vengono rilasciate al termine del lavoro di riparazione EC, indipendentemente dal fatto che il lavoro abbia avuto esito negativo o positivo.

Trovare il nome host per il nodo di storage

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Utilizzare `/etc/hosts` File per trovare il nome host del nodo di storage per i volumi di storage ripristinati. Per visualizzare un elenco di tutti i nodi nella griglia, immettere quanto segue: `cat /etc/hosts`.

Riparare i dati se tutti i volumi sono guasti

Se tutti i volumi di storage si sono guastati, riparare l'intero nodo. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codifica di cancellazione (EC) o entrambi.

Se solo alcuni volumi hanno avuto problemi, passare a. Riparare i dati se solo alcuni volumi sono guasti.

> Non puoi correre `repair-data` operazioni per più di un nodo contemporaneamente. Per ripristinare più nodi, contattare il supporto tecnico.

Dati replicati

Se la griglia include dati replicati, utilizzare `repair-data start-replicated-node-repair` con il `--nodes` opzione, dove `--nodes` È il nome host (nome di sistema) per riparare l'intero nodo di storage.

Questo comando ripara i dati replicati su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non riesce a individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. È necessario determinare la causa della perdita e se è possibile eseguire il ripristino. Vedere "Esaminare gli oggetti persi".

Dati con erasure coding (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `repair-data start-ec-node-repair` con il `--nodes` opzione, dove `--nodes` È il nome host (nome di sistema) per riparare l'intero nodo di storage.

Questo comando ripara i dati con codifica di cancellazione su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Riparare i dati se solo alcuni volumi sono guasti

Se solo alcuni volumi hanno avuto problemi, riparare i volumi interessati. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codifica di cancellazione (EC) o entrambi.

Se tutti i volumi non sono riusciti, passare a. Riparare i dati se tutti i volumi sono guasti.

Inserire gli ID del volume in formato esadecimale. Ad esempio, `0000` è il primo volume e. `000F` è il sedicesimo

volume. È possibile specificare un volume, un intervallo di volumi o più volumi che non si trovano in una sequenza.

Tutti i volumi devono trovarsi sullo stesso nodo di storage. Se è necessario ripristinare i volumi per più di un nodo di storage, contattare il supporto tecnico.

Dati replicati

Se la griglia contiene dati replicati, utilizzare `start-replicated-volume-repair` con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati replicati nel volume `0002` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati replicati in tutti i volumi dell'intervallo `0003` a. `0009` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Volumi multipli non in sequenza: Questo comando ripristina i dati replicati nei volumi `0001`, `0005`, e. `0008` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non riesce a individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. Prendere nota della descrizione dell'avviso e delle azioni consigliate per determinare la causa della perdita e se è possibile eseguire il ripristino.

Dati con erasure coding (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `start-ec-volume-repair` con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati con codifica erasure nel volume `0007` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati con codifica di cancellazione su tutti i volumi dell'intervallo `0004` a. `0006` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Volumi multipli non in sequenza: Questo comando ripristina i dati con codifica erasure nei volumi `000A`, `000C`, e. `000E` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Il `repair-data` l'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di

ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Monitorare le riparazioni

Monitorare lo stato dei lavori di riparazione, in base all'utilizzo di **dati replicati**, **dati EC (erasure-coded)** o entrambi.

È inoltre possibile monitorare lo stato dei lavori di ripristino dei volumi in corso e visualizzare la cronologia dei lavori di ripristino completati in
"Grid Manager".

Dati replicati

- Per ottenere una percentuale di completamento stimata per la riparazione replicata, aggiungere `show-replicated-repair-status` al comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Per determinare se le riparazioni sono state completate:
  a. Selezionare **NODI** > ***nodo di storage in riparazione*** > **ILM**.
  b. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
  a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
  b. Selezionare ***Grid*** > ***Storage Node in riparazione*** > **LDR** > **Data Store**.
  c. Utilizzare una combinazione dei seguenti attributi per determinare, come possibile, se le riparazioni replicate sono complete.

  > Le incongruenze di Cassandra potrebbero essere presenti e le riparazioni non riuscite non vengono monitorate.

  - **Tentativi di riparazione (XRPA)**: Utilizzare questo attributo per tenere traccia dell'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo superiore al periodo di scansione corrente (fornito dall'attributo **Scan Period — Estimated**), significa che la scansione ILM non ha rilevato oggetti ad alto rischio che devono essere riparati su alcun nodo.

    > Gli oggetti ad alto rischio sono oggetti che rischiano di essere completamente persi. Non sono inclusi oggetti che non soddisfano la configurazione ILM.

  - **Periodo di scansione — stimato (XSCM)**: Utilizzare questo attributo per stimare quando verrà applicata una modifica di policy agli oggetti precedentemente acquisiti. Se l'attributo **riparazioni tentate** non aumenta per un periodo superiore al periodo di scansione corrente, è probabile che vengano eseguite riparazioni replicate. Si noti che il periodo di scansione può cambiare. L'attributo **Scan Period — Estimated (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione del nodo. È possibile eseguire una query nella cronologia degli attributi **Scan Period — Estimated** per la griglia per determinare un intervallo di tempo appropriato.

Dati con erasure coding (EC)

Per monitorare la riparazione dei dati con codifica erasure e riprovare eventuali richieste che potrebbero non essere riuscite:

1. Determinare lo stato delle riparazioni dei dati con codice di cancellazione:
   - Selezionare **SUPPORTO** > **Strumenti** > **metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).

- Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` funzionamento:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilizzare questo comando per elencare tutte le riparazioni:

  ```
  repair-data show-ec-repair-status
  ```

L'output elenca le informazioni, tra cui `repair ID`, per tutte le riparazioni precedentemente e attualmente in esecuzione.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

   Questo comando prova di nuovo una riparazione del nodo non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Questo comando prova di nuovo una riparazione del volume non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Controllare lo stato dello storage dopo il ripristino dei volumi di storage

Dopo il ripristino dei volumi di storage, è necessario verificare che lo stato desiderato del nodo di storage sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che si riavvia il server del nodo di storage.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Il nodo di storage è stato ripristinato e il ripristino dei dati è stato completato.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Controllare i valori di **Recovery Storage Node** > **LDR** > **Storage** > **Storage state — Desired** e **Storage state — Current**.

   Il valore di entrambi gli attributi deve essere Online.

3. Se lo stato di storage — desiderato è impostato su sola lettura, attenersi alla seguente procedura:
   a. Fare clic sulla scheda **Configurazione**.
   b. Dall'elenco a discesa **Storage state — Desired** (Stato storage — desiderato*), selezionare **Online**.
   c. Fare clic su **Applica modifiche**.
   d. Fare clic sulla scheda **Panoramica** e verificare che i valori di **Stato dello storage — desiderato** e **Stato dello storage — corrente** siano aggiornati a Online.

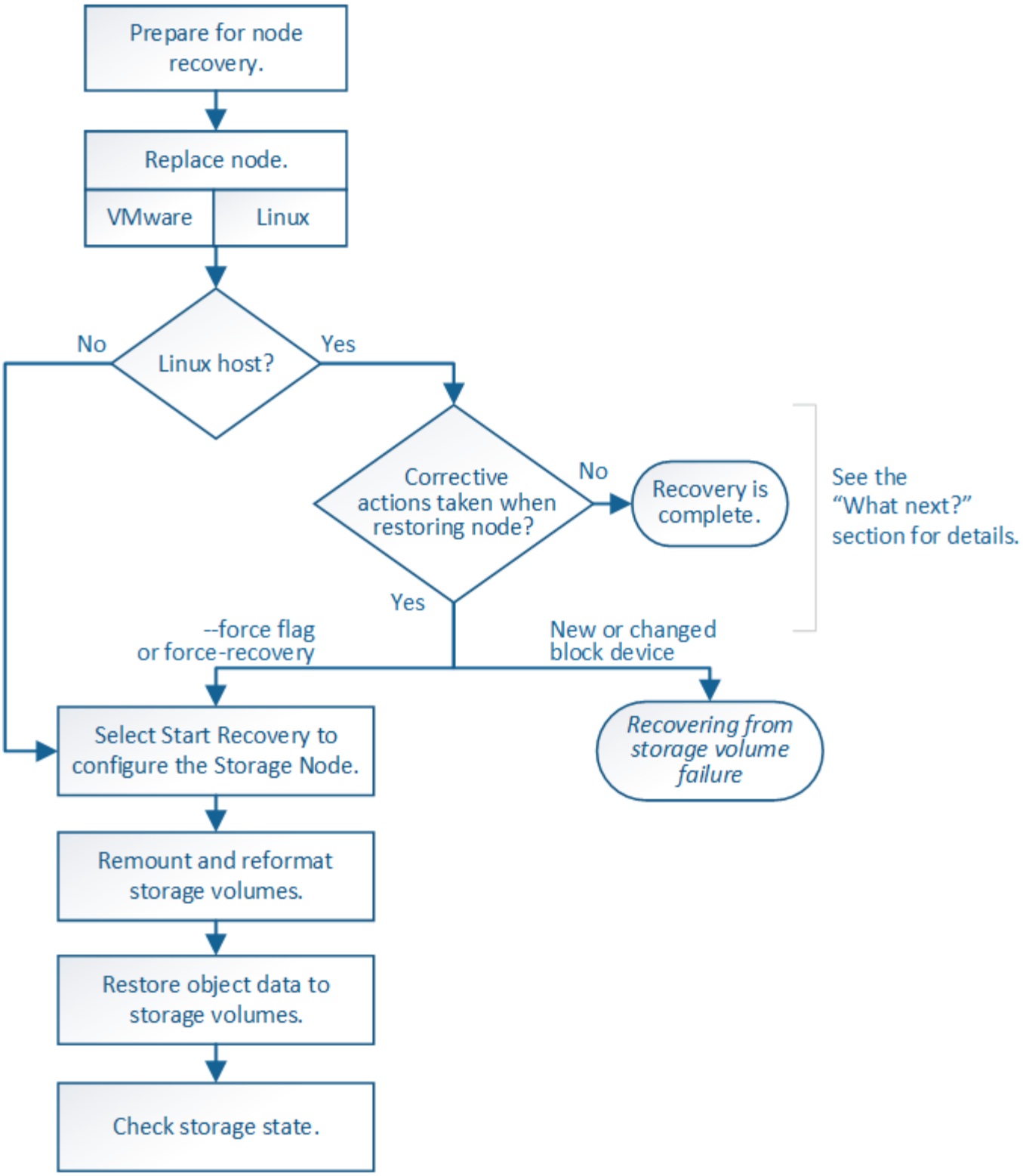
Ripristino in caso di guasto al disco di sistema

Recovery from system drive failure: Workflow

Se il disco di sistema su un nodo di storage basato su software si è guastato, il nodo di storage non è disponibile per il sistema StorageGRID. È necessario completare una serie specifica di attività per eseguire il ripristino da un guasto al disco di sistema.

Utilizzare questa procedura per eseguire il ripristino da un guasto del disco di sistema su un nodo di storage basato su software. Questa procedura include i passaggi da seguire se anche i volumi di storage non sono riusciti o non possono essere rimontati.

> Questa procedura si applica solo ai nodi di storage basati su software. Seguire una procedura diversa da "Ripristinare un nodo di storage dell'appliance".



Avvisi per il ripristino delle unità del sistema Storage Node

Prima di ripristinare un disco di sistema guasto di un nodo di storage, consultare le informazioni generali "avvertenze e considerazioni per il ripristino del nodo grid" e le seguenti avvertenze specifiche.

I nodi di storage dispongono di un database Cassandra che include metadati a oggetti. Il database Cassandra potrebbe essere ricostruito nei seguenti casi:

- Un nodo di storage viene riportato online dopo essere stato offline per più di 15 giorni.
- Un volume di storage ha subito un errore e è stato ripristinato.
- Il disco di sistema e uno o più volumi di storage si guastano e vengono ripristinati.

Quando Cassandra viene ricostruita, il sistema utilizza le informazioni provenienti da altri nodi di storage. Se troppi nodi di storage sono offline, alcuni dati Cassandra potrebbero non essere disponibili. Se Cassandra è stata ricostruita di recente, i dati Cassandra potrebbero non essere ancora coerenti in tutta la griglia. La perdita di dati può verificarsi se Cassandra viene ricostruita quando troppi nodi di storage sono offline o se due o più nodi di storage vengono ricostruiti entro 15 giorni l'uno dall'altro.

Se più di un nodo di storage si è guastato (o non è in linea), contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

Se si tratta del secondo guasto del nodo di storage in meno di 15 giorni dopo un guasto o un ripristino del nodo di storage, contattare il supporto tecnico. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni può causare la perdita di dati.

Se più di un nodo di storage in un sito si è guastato, potrebbe essere necessaria una procedura di ripristino del sito. Vedere "Come il supporto tecnico recupera un sito".

Se questo nodo di storage è in modalità di manutenzione in sola lettura per consentire il recupero di oggetti da parte di un altro nodo di storage con volumi di storage guasti, ripristinare i volumi sul nodo di storage con volumi di storage guasti prima di ripristinare questo nodo di storage guasto. Consultare le istruzioni a. "ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto".

Se le regole ILM sono configurate in modo da memorizzare una sola copia replicata e la copia esiste su un volume di storage che ha avuto esito negativo, non sarà possibile ripristinare l'oggetto.

Se si verifica un allarme Services: Status - Cassandra (SVST) durante il ripristino, vedere "Ripristinare i volumi di storage guasti e ricostruire il database Cassandra". Dopo la ricostruzione di Cassandra, gli allarmi devono essere disattivati. Se gli allarmi non vengono disattivati, contattare il supporto tecnico.

Sostituire il nodo di storage

Se il disco di sistema presenta un guasto, è necessario sostituire il nodo di storage.

Selezionare la procedura di sostituzione del nodo per la piattaforma. I passaggi per sostituire un nodo sono gli stessi per tutti i tipi di nodi griglia.

Questa procedura si applica solo ai nodi di storage basati su software. Seguire una procedura diversa da "Ripristinare un nodo di storage dell'appliance".

Linux: se non si è sicuri che il disco di sistema sia guasto, seguire le istruzioni per sostituire il nodo per determinare quali passaggi di ripristino sono necessari.

Piattaforma	Procedura
VMware	"Sostituire un nodo VMware"
Linux	"Sostituire un nodo Linux"
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per "Sostituzione di un nodo Linux".

Selezionare Avvia ripristino per configurare il nodo di storage

Dopo aver sostituito un nodo di storage, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.
- Il nodo sostitutivo è stato implementato e configurato.
- Si dispone della data di inizio di qualsiasi intervento di riparazione per i dati codificati per la cancellazione.
- Hai verificato che il nodo di storage non è stato ricostruito negli ultimi 15 giorni.

A proposito di questa attività

Se Storage Node è installato come container su un host Linux, eseguire questa operazione solo se si verifica una delle seguenti condizioni:

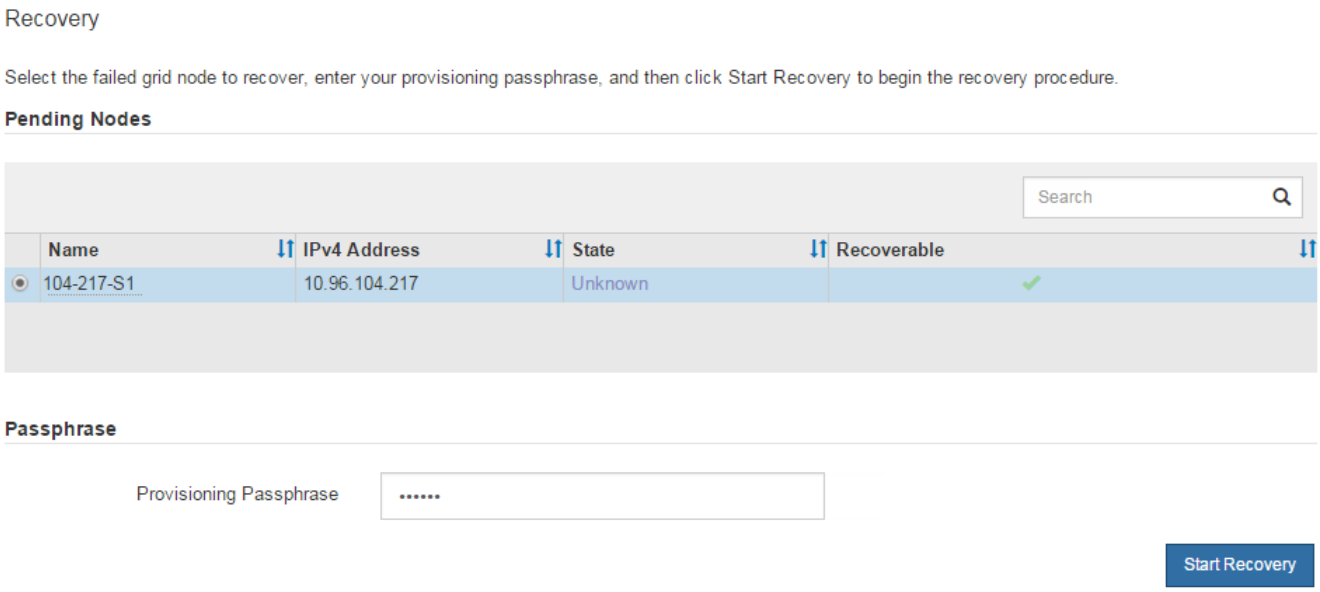
- È stato necessario utilizzare `--force` contrassegno per importare il nodo o emesso `storagegrid node force-recovery` *`node-name`*
- Era necessario eseguire una reinstallazione completa del nodo oppure ripristinare /var/local.

Fasi

1. In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **Ripristino**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

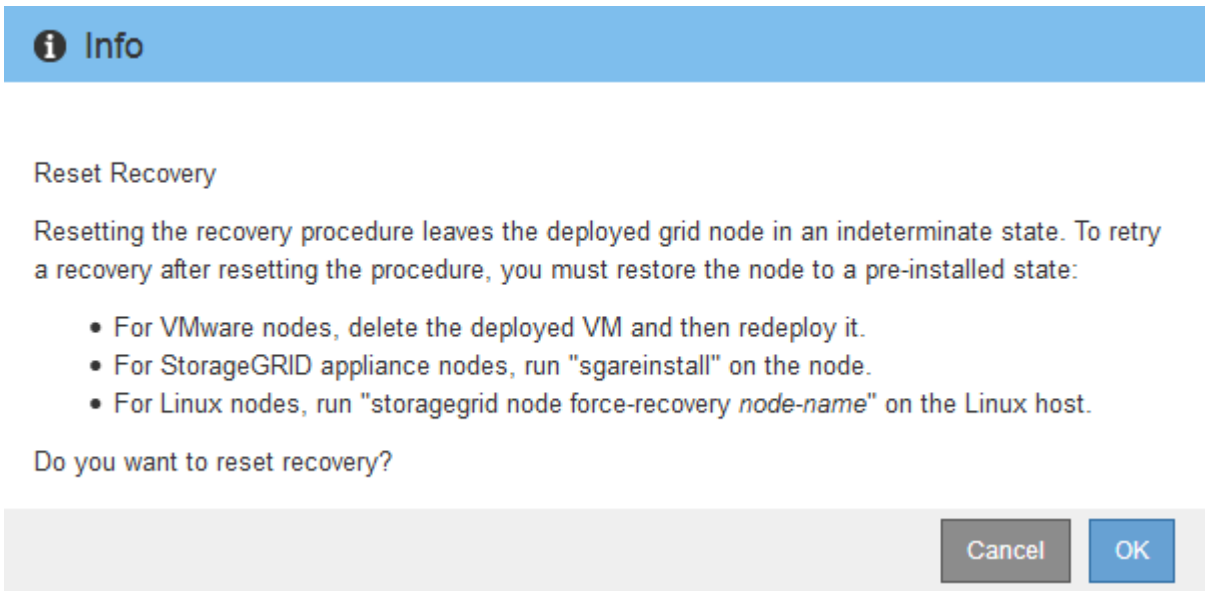
   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Immettere la **Provisioning Passphrase**.
4. Fare clic su **Start Recovery** (Avvia ripristino).



5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

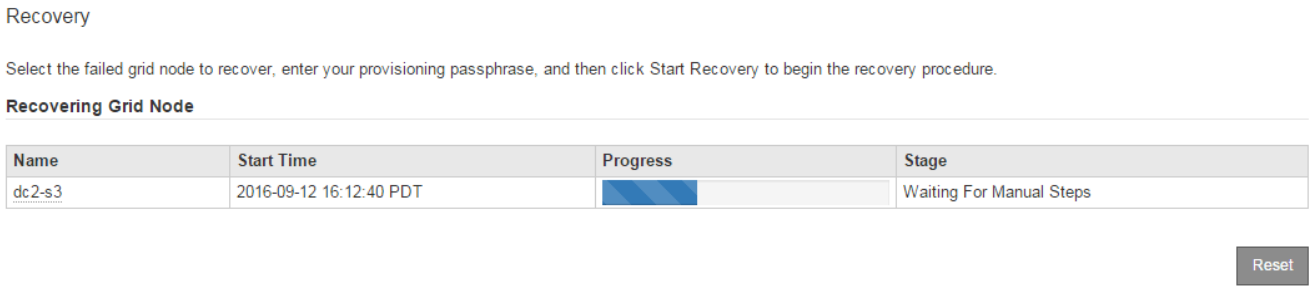
> Durante l'esecuzione della procedura di ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware**: Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux**: Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`

6. Quando il nodo di archiviazione raggiunge la fase "in attesa delle fasi manuali", passare a. "Rimontare e riformattare i volumi di storage (procedura manuale)".



Rimontare e riformattare i volumi di storage (procedura manuale)

È necessario eseguire manualmente due script per rimontare volumi di storage conservati e riformattare eventuali volumi di storage guasti. Il primo script consente di eseguire il remontaggio dei volumi correttamente formattati come volumi di storage StorageGRID. Il secondo script riformatta tutti i volumi non montati, ricostruisce Cassandra, se necessario, e avvia i servizi.

Prima di iniziare

- L'hardware è già stato sostituito per tutti i volumi di storage guasti che è necessario sostituire.

  Esecuzione di `sn-remount-volumes` lo script può aiutare a identificare altri volumi di storage guasti.

- È stato verificato che non è in corso la decommissionamento di un nodo di storage oppure che la procedura di decommissionamento del nodo è stata sospesa. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **smantellamento**).
- Hai verificato che non è in corso un'espansione. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **espansione**).
- Lo hai fatto "Esaminate le avvertenze relative al ripristino del disco di sistema Storage Node".

> Contattare il supporto tecnico se più di un nodo di storage non è in linea o se un nodo di storage in questa griglia è stato ricostruito negli ultimi 15 giorni. Non eseguire `sn-recovery-postinstall.sh` script. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni l'uno dall'altro potrebbe causare la perdita di dati.

A proposito di questa attività

Per completare questa procedura, eseguire le seguenti attività di alto livello:

- Accedere al nodo di storage recuperato.
- Eseguire `sn-remount-volumes` script per il remount di volumi di storage correttamente formattati. Quando viene eseguito, lo script esegue le seguenti operazioni:
  - Consente di montare e rimuovere ciascun volume di storage per riprodurre il journal XFS.
  - Esegue un controllo di coerenza del file XFS.
  - Se il file system è coerente, determina se il volume di storage è un volume di storage StorageGRID formattato correttamente.
  - Se il volume di storage è formattato correttamente, esegue il remontaggio del volume di storage. Tutti i dati esistenti sul volume rimangono intatti.
- Esaminare l'output dello script e risolvere eventuali problemi.

- Eseguire `sn-recovery-postinstall.sh` script. Quando viene eseguito, lo script esegue le seguenti operazioni.

> Non riavviare un nodo di storage durante il ripristino prima dell'esecuzione `sn-recovery-postinstall.sh` per riformattare i volumi di storage guasti e ripristinare i metadati degli oggetti. Riavviare il nodo di storage prima `sn-recovery-postinstall.sh` Il completamento causa errori per i servizi che tentano di avviarsi e fa uscire i nodi dell'appliance StorageGRID dalla modalità di manutenzione. Vedere la fase per script post-installazione.

  - Consente di riformattare tutti i volumi di storage di `sn-remount-volumes` impossibile eseguire il montaggio dello script o che è stato trovato formattato in modo errato.

> Se un volume di storage viene riformattato, tutti i dati presenti in tale volume andranno persi. È necessario eseguire un'ulteriore procedura per ripristinare i dati degli oggetti da altre posizioni nella griglia, supponendo che le regole ILM siano state configurate per memorizzare più copie di un oggetto.

  - Ricostruisce il database Cassandra sul nodo, se necessario.
  - Avvia i servizi sul nodo di storage.

Fasi

1. Accedere al nodo di storage recuperato:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Eseguire il primo script per rimontare eventuali volumi di storage correttamente formattati.

> Se tutti i volumi di storage sono nuovi e devono essere formattati, o se tutti i volumi di storage sono guasti, è possibile saltare questa fase ed eseguire il secondo script per riformattare tutti i volumi di storage non montati.

   a. Eseguire lo script: `sn-remount-volumes`

      Questo script potrebbe richiedere ore per essere eseguito su volumi di storage che contengono dati.

   b. Durante l'esecuzione dello script, esaminare l'output e rispondere alle richieste.

> Se necessario, è possibile utilizzare `tail -f` per monitorare il contenuto del file di log dello script (`/var/local/log/sn-remount-volumes.log`) . Il file di log contiene informazioni più dettagliate rispetto all'output della riga di comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740
```

```
====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
```

```
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

Nell'output di esempio, un volume di storage è stato rimontato correttamente e tre volumi di storage hanno avuto errori.

- `/dev/sdb` Ha superato il controllo di coerenza del file system XFS e disponeva di una struttura di volume valida, quindi è stato rimontato correttamente. I dati sui dispositivi che vengono rimontati dallo script vengono conservati.
- `/dev/sdc` Verifica della coerenza del file system XFS non riuscita perché il volume di storage era nuovo o corrotto.

- `/dev/sdd` impossibile montare perché il disco non è stato inizializzato o il superblocco del disco è stato danneggiato. Quando lo script non riesce a montare un volume di storage, chiede se si desidera eseguire il controllo di coerenza del file system.
  - Se il volume di storage è collegato a un nuovo disco, rispondere **N** alla richiesta. Non è necessario controllare il file system su un nuovo disco.
  - Se il volume di storage è collegato a un disco esistente, rispondere **Y** alla richiesta. È possibile utilizzare i risultati del controllo del file system per determinare l'origine del danneggiamento. I risultati vengono salvati in `/var/local/log/sn-remount-volumes.log` file di log.
- `/dev/sde` Ha superato la verifica di coerenza del file system XFS e disponeva di una struttura di volume valida; tuttavia, l'ID del nodo LDR nel file volID non corrisponde all'ID per questo nodo di storage (la `configured LDR noid` visualizzato nella parte superiore). Questo messaggio indica che questo volume appartiene a un altro nodo di storage.

3. Esaminare l'output dello script e risolvere eventuali problemi.

> Se un volume di storage non ha superato il controllo di coerenza del file system XFS o non è stato possibile montarlo, esaminare attentamente i messaggi di errore nell'output. È necessario comprendere le implicazioni dell'esecuzione di `sn-recovery-postinstall.sh` creare script su questi volumi.

a. Verificare che i risultati includano una voce per tutti i volumi previsti. Se alcuni volumi non sono elencati, eseguire nuovamente lo script.

b. Esaminare i messaggi per tutti i dispositivi montati. Assicurarsi che non vi siano errori che indichino che un volume di storage non appartiene a questo nodo di storage.

   Nell'esempio, l'output per `/dev/sde` include il seguente messaggio di errore:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> Se un volume di storage viene segnalato come appartenente a un altro nodo di storage, contattare il supporto tecnico. Se si esegue `sn-recovery-postinstall.sh` script, il volume di storage verrà riformattato, causando la perdita di dati.

c. Se non è stato possibile montare alcun dispositivo di storage, annotare il nome del dispositivo e riparare o sostituire il dispositivo.

> È necessario riparare o sostituire i dispositivi di storage che non possono essere montati.

   Il nome del dispositivo viene utilizzato per cercare l'ID del volume, che è necessario immettere quando si esegue `repair-data` script per ripristinare i dati dell'oggetto nel volume (la procedura successiva).

d. Dopo aver riparato o sostituito tutti i dispositivi non montabili, eseguire `sn-remount-volumes` eseguire nuovamente lo script per confermare che tutti i volumi di storage che possono essere rimontati sono stati rimontati.

Se un volume di storage non può essere montato o non è formattato correttamente e si passa alla fase successiva, il volume e i dati presenti nel volume verranno eliminati. Se si dispone di due copie di dati oggetto, si disporrà di una sola copia fino al completamento della procedura successiva (ripristino dei dati oggetto).

Non eseguire `sn-recovery-postinstall.sh` Eseguire uno script se si ritiene che i dati rimanenti su un volume di storage guasto non possano essere ricostruiti da un'altra parte della griglia (ad esempio, se il criterio ILM utilizza una regola che esegue una sola copia o se i volumi sono guasti su più nodi). Contattare invece il supporto tecnico per determinare come ripristinare i dati.

4. Eseguire `sn-recovery-postinstall.sh` script: `sn-recovery-postinstall.sh`

   Questo script riformatta tutti i volumi di storage che non possono essere montati o che sono stati trovati per essere formattati in modo non corretto; ricostruisce il database Cassandra sul nodo, se necessario; avvia i servizi sul nodo di storage.

   Tenere presente quanto segue:

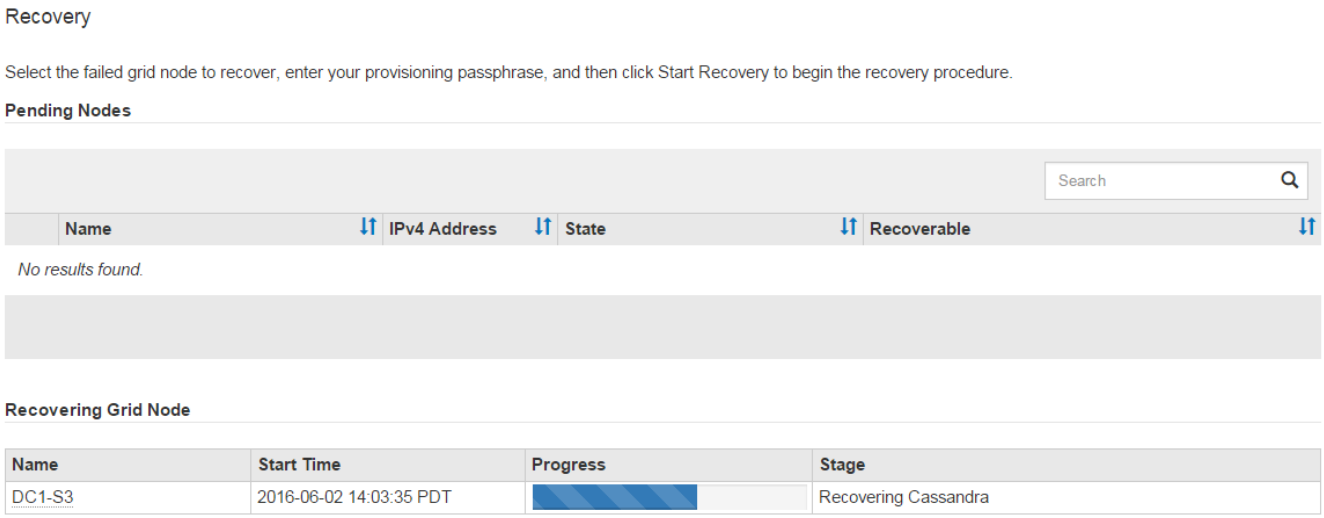
   - L'esecuzione dello script potrebbe richiedere ore.
   - In generale, si consiglia di lasciare la sessione SSH da sola mentre lo script è in esecuzione.
   - Non premere **Ctrl+C** mentre la sessione SSH è attiva.
   - Lo script viene eseguito in background se si verifica un'interruzione della rete e termina la sessione SSH, ma è possibile visualizzarne l'avanzamento dalla pagina Recovery (Ripristino).
   - Se Storage Node utilizza il servizio RSM, lo script potrebbe sembrare bloccato per 5 minuti quando i servizi del nodo vengono riavviati. Questo ritardo di 5 minuti è previsto ogni volta che il servizio RSM viene avviato per la prima volta.

     Il servizio RSM è presente sui nodi di storage che includono il servizio ADC.

   Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "riparazione Cassandra". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

5. come `sn-recovery-postinstall.sh` Viene eseguito lo script, monitorare la pagina Recovery in Grid Manager.

   La barra di avanzamento e la colonna fase della pagina di ripristino forniscono uno stato di alto livello di `sn-recovery-postinstall.sh` script.



6. Dopo il `sn-recovery-postinstall.sh` lo script ha avviato i servizi sul nodo, è possibile ripristinare i dati degli oggetti su qualsiasi volume di storage formattato dallo script.

   Lo script chiede se si desidera utilizzare il processo di ripristino del volume di Grid Manager.

   - Nella maggior parte dei casi, dovresti "Ripristinare i dati degli oggetti utilizzando Grid Manager". Risposta `y` Per utilizzare Grid Manager.
   - In rari casi, ad esempio quando richiesto dal supporto tecnico o quando si sa che il nodo sostitutivo ha meno volumi disponibili per lo storage a oggetti rispetto al nodo originale, è necessario "ripristinare manualmente i dati dell'oggetto" utilizzando il `repair-data` script. Se si verifica uno di questi casi, rispondere `n`.

   > Se rispondi `n` Per utilizzare il processo di ripristino del volume di Grid Manager (ripristinare manualmente i dati degli oggetti):
   >
   > - Non è possibile ripristinare i dati degli oggetti utilizzando Grid Manager.
   > - È possibile monitorare l'avanzamento dei lavori di ripristino manuale utilizzando Grid Manager.

   Dopo aver effettuato la selezione, lo script viene completato e vengono visualizzati i passaggi successivi per recuperare i dati dell'oggetto. Dopo aver esaminato questi passaggi, premere un tasto qualsiasi per tornare alla riga di comando.

Ripristinare i dati dell'oggetto nel volume di storage (errore del disco di sistema)

Dopo il ripristino dei volumi di storage per un nodo di storage non appliance, è possibile ripristinare i dati degli oggetti replicati o codificati in cancellazione che sono stati persi in caso di guasto del nodo di storage.

Quale procedura è necessario utilizzare?

Se possibile, ripristinare i dati dell'oggetto utilizzando la pagina **Volume Restore** in Grid Manager.

- Se i volumi sono elencati in **MANUTENZIONE** > **Ripristino volume** > **nodi da ripristinare**, ripristinare i dati degli oggetti utilizzando "Pagina di ripristino dei volumi in Grid Manager".

- Se i volumi non sono elencati in **MANUTENZIONE** > **Ripristino volume** > **nodi da ripristinare**, seguire la procedura riportata di seguito per l'utilizzo di `repair-data` script per ripristinare i dati dell'oggetto.

  Se il nodo di storage recuperato contiene un numero inferiore di volumi rispetto al nodo che sta sostituendo, è necessario utilizzare `repair-data` script.

> Lo script dei dati di riparazione è obsoleto e verrà rimosso in una versione futura. Se possibile, utilizzare "Procedura di ripristino del volume in Grid Manager".

Utilizzare `repair-data` script per ripristinare i dati dell'oggetto

Prima di iniziare

- È stato confermato che il nodo di archiviazione recuperato ha uno stato di connessione **connesso** Nella scheda **NODI** > **Panoramica** di Grid Manager.

A proposito di questa attività

I dati degli oggetti possono essere ripristinati da altri nodi di storage, da un nodo di archiviazione o da un pool di storage cloud, supponendo che le regole ILM del grid siano state configurate in modo da rendere disponibili le copie degli oggetti.

Tenere presente quanto segue:

- Se una regola ILM è stata configurata per memorizzare solo una copia replicata e tale copia esisteva su un volume di storage che non ha superato il test, non sarà possibile ripristinare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto. Prima di eseguire questa procedura, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi di ripristino e dei relativi costi.
- Se l'unica copia rimanente di un oggetto si trova su un nodo di archiviazione, i dati dell'oggetto vengono recuperati dal nodo di archiviazione. Il ripristino dei dati degli oggetti in un nodo di storage da un nodo di archiviazione richiede più tempo rispetto al ripristino delle copie da altri nodi di storage a causa della latenza associata ai recuperi da sistemi di storage di archiviazione esterni.

A proposito di `repair-data` script

Per ripristinare i dati dell'oggetto, eseguire `repair-data` script. Questo script inizia il processo di ripristino dei dati degli oggetti e lavora con la scansione ILM per garantire che le regole ILM siano soddisfatte.

Selezionare **Replicated data** o **Erasure-Coded (EC) data** per apprendere le diverse opzioni di `repair-data` script, in base al ripristino di dati replicati o a dati con codifica di cancellazione. Se è necessario ripristinare entrambi i tipi di dati, è necessario eseguire entrambi i set di comandi.

> Per ulteriori informazioni su `repair-data` script, invio `repair-data --help` Dalla riga di comando del nodo di amministrazione primario.

> Lo script dei dati di riparazione è obsoleto e verrà rimosso in una versione futura. Se possibile, utilizzare "Procedura di ripristino del volume in Grid Manager".

Dati replicati

Sono disponibili due comandi per il ripristino dei dati replicati, a seconda che sia necessario riparare l'intero nodo o solo alcuni volumi sul nodo:

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

È possibile tenere traccia delle riparazioni dei dati replicati con questo comando:

```
repair-data show-replicated-repair-status
```

Dati con erasure coding (EC)

Sono disponibili due comandi per il ripristino dei dati con codifica erasure, a seconda che sia necessario riparare l'intero nodo o solo determinati volumi sul nodo:

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

È possibile tenere traccia delle riparazioni dei dati con codifica per la cancellazione con questo comando:

```
repair-data show-ec-repair-status
```

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. Tuttavia, se non è possibile tenere conto di tutti i dati con codice di cancellazione, la riparazione non può essere completata. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

> Il lavoro di riparazione EC riserva temporaneamente una grande quantità di storage. Gli avvisi relativi allo storage potrebbero essere attivati, ma verranno risolti al termine della riparazione. Se lo storage non è sufficiente per la prenotazione, il lavoro di riparazione EC non avrà esito positivo. Le prenotazioni di storage vengono rilasciate al termine del lavoro di riparazione EC, indipendentemente dal fatto che il lavoro abbia avuto esito negativo o positivo.

Trovare il nome host per il nodo di storage

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Utilizzare `/etc/hosts` File per trovare il nome host del nodo di storage per i volumi di storage ripristinati. Per visualizzare un elenco di tutti i nodi nella griglia, immettere quanto segue: `cat /etc/hosts`.

Riparare i dati se tutti i volumi sono guasti

Se tutti i volumi di storage si sono guastati, riparare l'intero nodo. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codifica di cancellazione (EC) o entrambi.

Se solo alcuni volumi hanno avuto problemi, passare a. Riparare i dati se solo alcuni volumi sono guasti.

> Non puoi correre `repair-data` operazioni per più di un nodo contemporaneamente. Per ripristinare più nodi, contattare il supporto tecnico.

Dati replicati

Se la griglia include dati replicati, utilizzare `repair-data start-replicated-node-repair` con il `--nodes` opzione, dove `--nodes` È il nome host (nome di sistema) per riparare l'intero nodo di storage.

Questo comando ripara i dati replicati su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non riesce a individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. È necessario determinare la causa della perdita e se è possibile eseguire il ripristino. Vedere "Esaminare gli oggetti persi".

Dati con erasure coding (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `repair-data start-ec-node-repair` con il `--nodes` opzione, dove `--nodes` È il nome host (nome di sistema) per riparare l'intero nodo di storage.

Questo comando ripara i dati con codifica di cancellazione su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Riparare i dati se solo alcuni volumi sono guasti

Se solo alcuni volumi hanno avuto problemi, riparare i volumi interessati. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codifica di cancellazione (EC) o entrambi.

Se tutti i volumi non sono riusciti, passare a. Riparare i dati se tutti i volumi sono guasti.

Inserire gli ID del volume in formato esadecimale. Ad esempio, `0000` è il primo volume e. `000F` è il sedicesimo

volume. È possibile specificare un volume, un intervallo di volumi o più volumi che non si trovano in una sequenza.

Tutti i volumi devono trovarsi sullo stesso nodo di storage. Se è necessario ripristinare i volumi per più di un nodo di storage, contattare il supporto tecnico.

Dati replicati

Se la griglia contiene dati replicati, utilizzare `start-replicated-volume-repair` con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati replicati nel volume `0002` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati replicati in tutti i volumi dell'intervallo `0003` a. `0009` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Volumi multipli non in sequenza: Questo comando ripristina i dati replicati nei volumi `0001`, `0005`, e. `0008` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non riesce a individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. Prendere nota della descrizione dell'avviso e delle azioni consigliate per determinare la causa della perdita e se è possibile eseguire il ripristino.

Dati con erasure coding (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `start-ec-volume-repair` con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati con codifica erasure nel volume `0007` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati con codifica di cancellazione su tutti i volumi dell'intervallo `0004` a. `0006` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Volumi multipli non in sequenza: Questo comando ripristina i dati con codifica erasure nei volumi `000A`, `000C`, e. `000E` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Il `repair-data` l'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di

ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Monitorare le riparazioni

Monitorare lo stato dei lavori di riparazione, in base all'utilizzo di **dati replicati**, **dati EC (erasure-coded)** o entrambi.

È inoltre possibile monitorare lo stato dei lavori di ripristino dei volumi in corso e visualizzare la cronologia dei lavori di ripristino completati in "Grid Manager".

Dati replicati

- Per ottenere una percentuale di completamento stimata per la riparazione replicata, aggiungere `show-replicated-repair-status` al comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Per determinare se le riparazioni sono state completate:
  a. Selezionare **NODI** > ***nodo di storage in riparazione*** > **ILM**.
  b. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
  a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
  b. Selezionare ***Grid*** > ***Storage Node in riparazione*** > **LDR** > **Data Store**.
  c. Utilizzare una combinazione dei seguenti attributi per determinare, come possibile, se le riparazioni replicate sono complete.

  > Le incongruenze di Cassandra potrebbero essere presenti e le riparazioni non riuscite non vengono monitorate.

  - **Tentativi di riparazione (XRPA)**: Utilizzare questo attributo per tenere traccia dell'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo superiore al periodo di scansione corrente (fornito dall'attributo **Scan Period — Estimated**), significa che la scansione ILM non ha rilevato oggetti ad alto rischio che devono essere riparati su alcun nodo.

    > Gli oggetti ad alto rischio sono oggetti che rischiano di essere completamente persi. Non sono inclusi oggetti che non soddisfano la configurazione ILM.

  - **Periodo di scansione — stimato (XSCM)**: Utilizzare questo attributo per stimare quando verrà applicata una modifica di policy agli oggetti precedentemente acquisiti. Se l'attributo **riparazioni tentate** non aumenta per un periodo superiore al periodo di scansione corrente, è probabile che vengano eseguite riparazioni replicate. Si noti che il periodo di scansione può cambiare. L'attributo **Scan Period — Estimated (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione del nodo. È possibile eseguire una query nella cronologia degli attributi **Scan Period — Estimated** per la griglia per determinare un intervallo di tempo appropriato.

Dati con erasure coding (EC)

Per monitorare la riparazione dei dati con codifica erasure e riprovare eventuali richieste che potrebbero non essere riuscite:

1. Determinare lo stato delle riparazioni dei dati con codice di cancellazione:
   - Selezionare **SUPPORTO** > **Strumenti** > **metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).

- Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` funzionamento:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilizzare questo comando per elencare tutte le riparazioni:

  ```
  repair-data show-ec-repair-status
  ```

L'output elenca le informazioni, tra cui `repair ID`, per tutte le riparazioni precedentemente e attualmente in esecuzione.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

   Questo comando prova di nuovo una riparazione del nodo non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Questo comando prova di nuovo una riparazione del volume non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Controllare lo stato dello storage dopo il ripristino del disco di sistema Storage Node

Dopo aver ripristinato l'unità di sistema per un nodo di storage, è necessario verificare che lo stato desiderato del nodo di storage sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che il server del nodo di storage viene riavviato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Il nodo di storage è stato ripristinato e il ripristino dei dati è stato completato.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Controllare i valori di **Recovery Storage Node** > **LDR** > **Storage** > **Storage state — Desired** e **Storage state — Current**.

   Il valore di entrambi gli attributi deve essere Online.

3. Se lo stato di storage — desiderato è impostato su sola lettura, attenersi alla seguente procedura:
   a. Fare clic sulla scheda **Configurazione**.
   b. Dall'elenco a discesa **Storage state — Desired** (Stato storage — desiderato*), selezionare **Online**.
   c. Fare clic su **Applica modifiche**.
   d. Fare clic sulla scheda **Panoramica** e verificare che i valori di **Stato dello storage — desiderato** e **Stato dello storage — corrente** siano aggiornati a Online.

Ripristinare i dati degli oggetti utilizzando Grid Manager

È possibile ripristinare i dati degli oggetti per un volume di storage o un nodo di storage guasto utilizzando Grid Manager. È inoltre possibile utilizzare Grid Manager per monitorare i processi di ripristino in corso e visualizzare una cronologia di ripristino.

Prima di iniziare

- Una di queste procedure è stata completata per formattare i volumi guasti:
  - "Rimontare e riformattare i volumi di storage delle appliance (procedura manuale)"
  - "Rimontare e riformattare i volumi di storage (procedura manuale)"
- Hai confermato che lo stato di connessione del nodo di storage in cui stai ripristinando gli oggetti è **connesso** Nella scheda **NODI** > **Panoramica** di Grid Manager.
- Hai confermato quanto segue:
  - Non è in corso un'espansione della griglia per aggiungere un nodo di storage.
  - La decommissionazione di un nodo di storage non è in corso o non è riuscita.
  - Non è in corso il ripristino di un volume di storage guasto.
  - Non è in corso il ripristino di un nodo di storage con un disco di sistema guasto.
  - Un lavoro di ribilanciamento EC non è in corso.
  - La clonazione del nodo dell'appliance non è in corso.

A proposito di questa attività

Dopo aver sostituito i dischi ed eseguito le procedure manuali per la formattazione dei volumi, Grid Manager visualizza i volumi come candidati per il ripristino nella scheda **MANUTENZIONE** > **Ripristino volume** > **nodi da ripristinare**.

Se possibile, ripristinare i dati degli oggetti utilizzando la pagina di ripristino del volume in Grid Manager. È possibile farlo attivare la modalità di ripristino automatico per avviare automaticamente il ripristino del volume quando i volumi sono pronti per essere ripristinati o. eseguire manualmente il ripristino del volume. Attenersi alle seguenti linee guida:

- Se i volumi sono elencati in **MANUTENZIONE** > **Ripristino volume** > **nodi da ripristinare**, ripristinare i dati degli oggetti come descritto di seguito. I volumi vengono elencati se:
  - Alcuni, ma non tutti, volumi di storage in un nodo sono guasti
  - Tutti i volumi di storage in un nodo sono guasti e vengono sostituiti con lo stesso numero di volumi o più volumi

  Anche la pagina di ripristino del volume in Grid Manager consente di monitorare il processo di ripristino del volume e. visualizzare la cronologia del ripristino.
- Se i volumi non sono elencati in Grid Manager come candidati per il ripristino, seguire la procedura appropriata per l'utilizzo di `repair-data` script per ripristinare i dati dell'oggetto:
  - "Ripristino dei dati degli oggetti nel volume di storage (errore del disco di sistema)"
  - "Ripristinare i dati degli oggetti nel volume di storage in cui il disco di sistema è intatto"
  - "Ripristinare i dati dell'oggetto nel volume di storage per l'appliance"

Lo script dei dati di riparazione è obsoleto e verrà rimosso in una versione futura.

Se il nodo di storage recuperato contiene un numero inferiore di volumi rispetto al nodo che sta sostituendo, è necessario utilizzare `repair-data` script.

È possibile ripristinare due tipi di dati oggetto:

- Gli oggetti dati replicati vengono ripristinati da altre posizioni, supponendo che le regole ILM della griglia siano state configurate per rendere disponibili le copie degli oggetti.
  - Se una regola ILM è stata configurata per memorizzare solo una copia replicata e tale copia esisteva su un volume di storage che non ha superato il test, non sarà possibile ripristinare l'oggetto.
  - Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto.
  - Se l'unica copia rimanente di un oggetto si trova su un nodo di archiviazione, i dati dell'oggetto vengono recuperati dal nodo di archiviazione. Il ripristino dei dati degli oggetti in un nodo di storage da un nodo di archiviazione richiede più tempo rispetto al ripristino delle copie degli oggetti da altri nodi di storage.
- Gli oggetti dati con erasure coding (EC) vengono ripristinati riassemblando i frammenti memorizzati. I frammenti corrotti o persi vengono ricreati dall'algoritmo di erasure coding dai dati rimanenti e dai frammenti di parità.

  Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. Tuttavia, se non è possibile tenere conto di tutti i dati sottoposti a erasure coding, la riparazione non può essere completata. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Il ripristino dei volumi dipende dalla disponibilità delle risorse in cui sono memorizzate le copie a oggetti. L'avanzamento del ripristino dei volumi non è lineare e potrebbe richiedere giorni o settimane.

attiva la modalità di ripristino automatico

Quando si attiva la modalità di ripristino automatico, il ripristino del volume si avvia automaticamente quando i volumi sono pronti per essere ripristinati.

Fasi

1. In Grid Manager, andare a **MANUTENZIONE** > **Volume repristino**.
2. Selezionare la scheda **nodi da ripristinare**, quindi spostare l'interruttore per **modalità di ripristino automatico** sulla posizione abilitata.
3. Quando viene visualizzata la finestra di dialogo di conferma, rivedere i dettagli.

   - Non sarà possibile avviare manualmente i processi di ripristino dei volumi su nessun nodo.
   - I ripristini del volume inizieranno automaticamente solo quando non sono in corso altre procedure di manutenzione.
   - È possibile monitorare lo stato del lavoro dalla pagina di monitoraggio dell'avanzamento.
   - StorageGRID ritenta automaticamente il ripristino del volume che non si avvia.

4. Una volta compresi i risultati dell'attivazione della modalità di ripristino automatico, selezionare **Sì** nella finestra di dialogo di conferma.

   È possibile disattivare la modalità di ripristino automatico in qualsiasi momento.

Ripristino manuale di un volume o nodo non riuscito

Per ripristinare un volume o un nodo guasto, procedere come segue.

Fasi

1. In Grid Manager, andare a **MANUTENZIONE** > **Volume repristino**.
2. Selezionare la scheda **nodi da ripristinare**, quindi far scorrere l'interruttore per **modalità di ripristino automatico** sulla posizione disattivata.

   Il numero sulla scheda indica il numero di nodi con volumi che richiedono il ripristino.

3. Espandere ciascun nodo per visualizzare i volumi in esso che richiedono il ripristino e il relativo stato.
4. Correggere eventuali problemi che impediscono il ripristino di ciascun volume. I problemi saranno indicati quando si seleziona **in attesa di passaggi manuali**, se viene visualizzato come stato del volume.
5. Selezionare un nodo da ripristinare in cui tutti i volumi indicano uno stato Pronto per il ripristino.

   È possibile ripristinare i volumi solo per un nodo alla volta.

   Ogni volume nel nodo deve indicare che è pronto per il ripristino.

6. Selezionare **Avvia ripristino**.
7. Risolvere eventuali avvisi che potrebbero essere visualizzati o selezionare **Avvia comunque** per ignorare gli avvisi e avviare il ripristino.

I nodi vengono spostati dalla scheda **Nodes to restore** (nodi da ripristinare) alla scheda **Restoration Progress** (avanzamento ripristino) all'avvio del ripristino.

Se non è possibile avviare il ripristino di un volume, il nodo torna alla scheda **nodi da ripristinare**.

Visualizza l'avanzamento del ripristino

La scheda **Restoration Progress** (avanzamento ripristino) mostra lo stato del processo di ripristino del volume e le informazioni sui volumi di un nodo da ripristinare.

I tassi di riparazione dei dati per gli oggetti replicati e con erasure coding in tutti i volumi sono la media che riepiloga tutti i ripristini in corso, inclusi quelli avviati utilizzando `repair-data` script. Viene indicata anche la percentuale di oggetti in quei volumi che sono intatti e non richiedono il ripristino.

> Il ripristino dei dati replicati dipende dalla disponibilità delle risorse in cui sono memorizzate le copie replicate. L'avanzamento del ripristino dei dati replicati non è lineare e potrebbe richiedere giorni o settimane.

La sezione lavori di ripristino visualizza informazioni sui ripristini dei volumi avviati da Grid Manager.

- Il numero nell'intestazione della sezione lavori di ripristino indica il numero di volumi che vengono ripristinati o messi in coda per il ripristino.

- La tabella visualizza le informazioni relative a ciascun volume di un nodo da ripristinare e al relativo stato di avanzamento.
  - L'avanzamento per ciascun nodo visualizza la percentuale per ciascun lavoro.
  - Espandere la colonna Dettagli per visualizzare l'ora di inizio del ripristino e l'ID del processo.
- Se il ripristino di un volume non riesce:
  - La colonna Stato indica `failed (attempting retry)`, e verranno rieseguiti automaticamente.
  - Se più lavori di ripristino non hanno avuto esito positivo, il lavoro più recente verrà rielaborato automaticamente per primo.
  - L'avviso **guasto riparazione EC** viene attivato se i tentativi continuano a non riuscire. Per risolvere il problema, attenersi alla procedura riportata nell'avviso.

Visualizza la cronologia del ripristino

La scheda **Restoration history** (Cronologia ripristino) mostra informazioni su tutti i ripristini dei volumi completati correttamente.

> Le dimensioni non sono applicabili agli oggetti replicati e vengono visualizzate solo per i ripristini che contengono oggetti di dati EC (erasure coding).

Monitorare i lavori dei dati di riparazione

È possibile monitorare lo stato dei lavori di riparazione utilizzando `repair-data` script dalla riga di comando.

Questi includono i processi avviati manualmente o quelli avviati automaticamente da StorageGRID nell'ambito di una procedura di decommissionamento.

> Se si eseguono processi di ripristino dei volumi, "Monitorare l'avanzamento e visualizzare una cronologia di tali lavori in Grid Manager" invece.

Monitorare lo stato di `repair-data` Processi basati sull'utilizzo di **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi.

Dati replicati

- Per ottenere una percentuale di completamento stimata per la riparazione replicata, aggiungere `show-replicated-repair-status` al comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Per determinare se le riparazioni sono state completate:
  a. Selezionare **NODI** > ***nodo di storage in riparazione*** > **ILM**.
  b. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
  a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
  b. Selezionare ***Grid*** > ***Storage Node in riparazione*** > **LDR** > **Data Store**.
  c. Utilizzare una combinazione dei seguenti attributi per determinare, come possibile, se le riparazioni replicate sono complete.

    > Le incongruenze di Cassandra potrebbero essere presenti e le riparazioni non riuscite non vengono monitorate.

    - **Tentativi di riparazione (XRPA)**: Utilizzare questo attributo per tenere traccia dell'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo superiore al periodo di scansione corrente (fornito dall'attributo **Scan Period — Estimated**), significa che la scansione ILM non ha rilevato oggetti ad alto rischio che devono essere riparati su alcun nodo.

      > Gli oggetti ad alto rischio sono oggetti che rischiano di essere completamente persi. Non sono inclusi oggetti che non soddisfano la configurazione ILM.

    - **Periodo di scansione — stimato (XSCM)**: Utilizzare questo attributo per stimare quando verrà applicata una modifica di policy agli oggetti precedentemente acquisiti. Se l'attributo **riparazioni tentate** non aumenta per un periodo superiore al periodo di scansione corrente, è probabile che vengano eseguite riparazioni replicate. Si noti che il periodo di scansione può cambiare. L'attributo **Scan Period — Estimated (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione del nodo. È possibile eseguire una query nella cronologia degli attributi **Scan Period — Estimated** per la griglia per determinare un intervallo di tempo appropriato.

Dati con erasure coding (EC)

Per monitorare la riparazione dei dati con codifica erasure e riprovare eventuali richieste che potrebbero non essere riuscite:

1. Determinare lo stato delle riparazioni dei dati con codice di cancellazione:
   - Selezionare **SUPPORTO** > **Strumenti** > **metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).

- Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` funzionamento:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilizzare questo comando per elencare tutte le riparazioni:

  ```
  repair-data show-ec-repair-status
  ```

L'output elenca le informazioni, tra cui `repair ID`, per tutte le riparazioni precedentemente e attualmente in esecuzione.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

   Questo comando prova di nuovo una riparazione del nodo non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Questo comando prova di nuovo una riparazione del volume non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Ripristino da errori del nodo di amministrazione

Recovery from Admin Node Failures: Workflow

Il processo di ripristino per un nodo di amministrazione dipende dal fatto che si tratti del nodo di amministrazione primario o di un nodo di amministrazione non primario.

I passaggi di alto livello per il ripristino di un nodo di amministrazione primario o non primario sono gli stessi, anche se i dettagli dei passaggi differiscono.

Seguire sempre la procedura di ripristino corretta per l'Admin Node che si sta ripristinando. Le procedure hanno lo stesso aspetto ad un livello elevato, ma differiscono nei dettagli.

Scelte

- "Ripristino da guasti principali del nodo di amministrazione"
- "Ripristino da guasti non primari del nodo di amministrazione"

Ripristino da guasti principali del nodo di amministrazione

Recovery from primary Admin Node failures (Ripristino da guasti principali del nodo di amministrazione

È necessario completare un set specifico di attività per eseguire il ripristino da un guasto primario del nodo di amministrazione. Il nodo di amministrazione primario ospita il servizio CMN (Configuration Management Node) per la griglia.

Un nodo di amministrazione primario guasto deve essere sostituito tempestivamente. Il servizio CMN (Configuration Management Node) sul nodo di amministrazione primario è responsabile dell'emissione di blocchi di identificatori di oggetti per la griglia. Questi identificatori vengono assegnati agli oggetti man mano che vengono acquisiti. Non è possibile acquisire nuovi oggetti a meno che non siano disponibili identificatori. L'acquisizione degli oggetti può continuare anche quando la CMN non è disponibile, poiché la fornitura di identificatori di circa un mese viene memorizzata nella cache della griglia. Tuttavia, una volta esauriti gli identificatori memorizzati nella cache, non è possibile aggiungere nuovi oggetti.

> È necessario riparare o sostituire un nodo di amministrazione primario guasto entro circa un mese, altrimenti la griglia potrebbe perdere la capacità di acquisire nuovi oggetti. Il periodo di tempo esatto dipende dal tasso di acquisizione degli oggetti: Se hai bisogno di una valutazione più accurata del periodo di tempo per la tua griglia, contatta il supporto tecnico.

Copia i registri di controllo dal nodo di amministrazione primario non riuscito

Se è possibile copiare i registri di controllo dal nodo di amministrazione primario guasto, è necessario conservarli per mantenere il record dell'attività e dell'utilizzo del sistema della griglia. È possibile ripristinare i registri di controllo conservati nel nodo di amministrazione primario recuperato dopo che è attivo e in esecuzione.

A proposito di questa attività

Questa procedura copia i file di log di audit dal nodo di amministrazione non riuscito in una posizione temporanea su un nodo griglia separato. Questi registri di controllo conservati possono quindi essere copiati nel nodo di amministrazione sostitutivo. I registri di controllo non vengono copiati automaticamente nel nuovo nodo di amministrazione.

A seconda del tipo di errore, potrebbe non essere possibile copiare i registri di controllo da un nodo di amministrazione non riuscito. Se l'implementazione ha un solo nodo di amministrazione, il nodo di amministrazione recuperato avvia la registrazione degli eventi nel registro di controllo in un nuovo file vuoto e i dati precedentemente registrati vengono persi. Se l'implementazione include più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione.

> Se i registri di controllo non sono ora accessibili sul nodo di amministrazione guasto, potrebbe essere possibile accedervi in un secondo momento, ad esempio dopo il ripristino dell'host.

Fasi

1. Se possibile, accedere al nodo Admin non riuscito. In caso contrario, accedere al nodo di amministrazione primario o a un altro nodo di amministrazione, se disponibile.
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Arrestare il servizio AMS per impedire la creazione di un nuovo file di log:`service ams stop`
3. Accedere alla directory di esportazione della verifica:

   ```
   cd /var/local/log
   ```

4. Rinominare l'origine `audit.log` file con un nome di file numerato univoco. Ad esempio, rinominare il file audit.log in `2023-10-25.txt.1`.

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. Riavviare il servizio AMS: `service ams start`
6. Creare la directory per copiare tutti i file di log dell'audit in una posizione temporanea su un nodo griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Quando richiesto, inserire la password per admin.

7. Copiare tutti i file di log di controllo nella posizione temporanea: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Quando richiesto, inserire la password per admin.

8. Disconnettersi come root: `exit`

Sostituire nodo amministratore primario

Per ripristinare un nodo di amministrazione primario, è necessario prima sostituire l'hardware fisico o virtuale.

È possibile sostituire un nodo di amministrazione primario guasto con un nodo di amministrazione primario in esecuzione sulla stessa piattaforma oppure sostituire un nodo di amministrazione primario in esecuzione su VMware o su un host Linux con un nodo di amministrazione primario in hosting su un'appliance di servizi.

Utilizzare la procedura corrispondente alla piattaforma sostitutiva selezionata per il nodo. Una volta completata la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino primario del nodo di amministrazione.

Piattaforma sostitutiva	Procedura
VMware	"Sostituire un nodo VMware"
Linux	"Sostituire un nodo Linux"
Appliance di servizi	"Sostituire un'appliance di servizi"
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per "Sostituzione di un nodo Linux".

Configurare il nodo amministrativo primario sostitutivo

Il nodo sostitutivo deve essere configurato come nodo amministratore primario per il

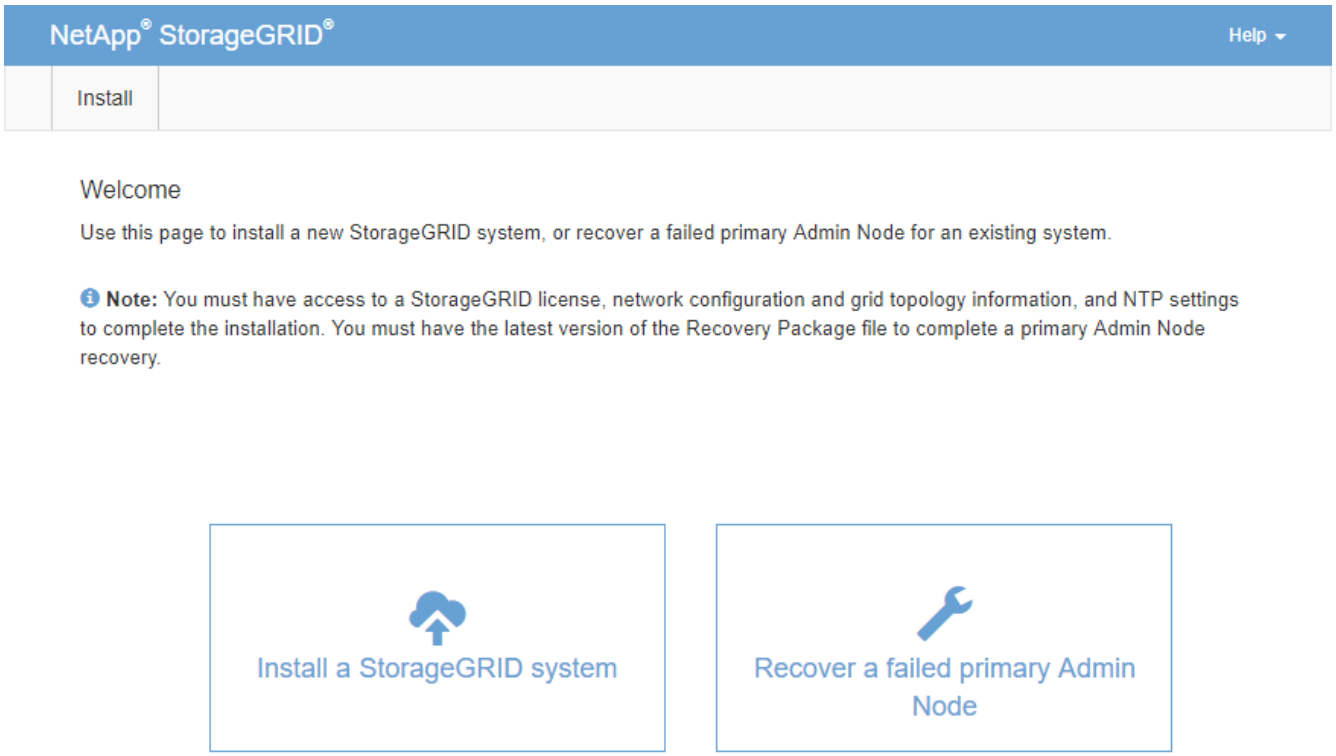
sistema StorageGRID.

Prima di iniziare

- Per i nodi di amministrazione primari ospitati su macchine virtuali, la macchina virtuale è stata implementata, attivata e inizializzata.
- Per i nodi di amministrazione primari ospitati su un'appliance di servizi, l'appliance è stata sostituita e il software è stato installato. Vedere "istruzioni per l'installazione dell'apparecchio".
- Si dispone dell'ultimo backup del file del pacchetto di ripristino (`sgws-recovery-package-id-revision.zip`).
- Si dispone della passphrase di provisioning.

Fasi

1. Aprire il browser Web e accedere a. `https://primary_admin_node_ip`.



2. Fare clic su **Recover a failed primary Admin Node** (Ripristina nodo amministratore primario guasto
3. Caricare il backup più recente del pacchetto di ripristino:
   a. Fare clic su **Sfoglia**.
   b. Individuare il file del pacchetto di ripristino più recente per il sistema StorageGRID in uso e fare clic su **Apri**.
4. Inserire la passphrase di provisioning.
5. Fare clic su **Start Recovery** (Avvia ripristino).

   Viene avviato il processo di ripristino. Grid Manager potrebbe non essere disponibile per alcuni minuti all'avvio dei servizi richiesti. Al termine del ripristino, viene visualizzata la pagina di accesso.

6. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID e il trust della parte di base per il nodo di amministrazione ripristinato è stato configurato per utilizzare il certificato dell'interfaccia di gestione predefinita, aggiornare (o eliminare e ricreare) il trust della parte di base del nodo in Active Directory Federation Services (ad FS). Utilizzare il nuovo certificato server predefinito generato durante il processo di ripristino del nodo di amministrazione.

   > Per configurare un trust di parte che si basa, vedere "Configurare il single sign-on". Per accedere al certificato del server predefinito, accedere alla shell dei comandi del nodo di amministrazione. Accedere alla `/var/local/mgmt-api` e selezionare `server.crt` file.

7. Determinare se è necessario applicare una correzione rapida.
   a. Accedere a Grid Manager utilizzando un "browser web supportato".
   b. Selezionare **NODI**.
   c. Dall'elenco a sinistra, selezionare il nodo di amministrazione principale.
   d. Nella scheda Overview (Panoramica), annotare la versione visualizzata nel campo **Software Version** (versione software).
   e. Selezionare qualsiasi altro nodo della griglia.
   f. Nella scheda Overview (Panoramica), annotare la versione visualizzata nel campo **Software Version** (versione software).
      - Se le versioni visualizzate nei campi **versione software** sono identiche, non è necessario applicare una correzione rapida.
      - Se le versioni visualizzate nei campi **versione software** sono diverse, è necessario "applicare una correzione rapida" Per aggiornare il nodo di amministrazione primario recuperato alla stessa versione.

Ripristinare il log di audit sul nodo di amministrazione primario recuperato

Se è stato possibile conservare il registro di controllo dal nodo di amministrazione primario guasto, è possibile copiarlo nel nodo di amministrazione primario che si sta ripristinando.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- I registri di controllo sono stati copiati in un'altra posizione dopo l'errore del nodo di amministrazione originale.

A proposito di questa attività

In caso di errore di un nodo amministratore, i registri di controllo salvati in quel nodo amministratore potrebbero andare persi. Potrebbe essere possibile conservare i dati in caso di perdita copiando i registri di controllo dal nodo di amministrazione non riuscito e ripristinando questi registri di controllo nel nodo di amministrazione ripristinato. A seconda dell'errore, potrebbe non essere possibile copiare i registri di controllo dal nodo di amministrazione non riuscito. In tal caso, se l'implementazione ha più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione, poiché i registri di controllo vengono replicati in tutti i nodi di amministrazione.

Se esiste un solo nodo Admin e non è possibile copiare il log di audit dal nodo guasto, il nodo Admin recuperato inizia a registrare gli eventi nel log di audit come se l'installazione fosse nuova.

Per ripristinare la funzionalità di registrazione, è necessario ripristinare un nodo amministratore il prima

possibile.

> Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile saltare questi passaggi se si verifica una delle seguenti condizioni:
>
> - È stato configurato un server syslog esterno e i registri di controllo vengono inviati al server syslog invece che ai nodi di amministrazione.
> - È stato specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.
>
> Vedere "Configurare i messaggi di audit e le destinazioni dei log" per ulteriori informazioni.

Fasi

1. Accedere al nodo di amministrazione recuperato:
   a. Immettere il seguente comando: `ssh admin@recovery_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
2. Controllare quali file di audit sono stati conservati: `cd /var/local/log`
3. Copiare i file di log di controllo conservati nel nodo di amministrazione recuperato: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   Quando richiesto, inserire la password per admin.
4. Per motivi di sicurezza, eliminare i registri di controllo dal nodo Grid guasto dopo aver verificato che siano stati copiati correttamente nel nodo Admin ripristinato.
5. Aggiornare le impostazioni di utente e gruppo dei file di log di controllo sul nodo di amministrazione recuperato: `chown ams-user: bycast *`
6. Disconnettersi come root: `exit`

È inoltre necessario ripristinare qualsiasi accesso client preesistente alla condivisione di controllo. Per ulteriori informazioni, vedere "Configurare l'accesso al client di audit".

Ripristinare il database Admin Node durante il ripristino del nodo Admin primario

Se si desidera conservare le informazioni cronologiche relative ad attributi, allarmi e avvisi su un nodo di amministrazione primario che ha avuto esito negativo, è possibile ripristinare il database del nodo di amministrazione. È possibile ripristinare questo database solo se il sistema StorageGRID include un altro nodo amministratore.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.

- Hai il `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

In caso di errore di un nodo amministratore, le informazioni storiche memorizzate nel database del nodo amministratore andranno perse. Questo database include le seguenti informazioni:

- Cronologia degli avvisi
- Cronologia degli allarmi
- Dati storici degli attributi, utilizzati nei grafici e nei report di testo disponibili nella pagina **SUPPORTO** > **Strumenti** > **topologia griglia**.

Quando si ripristina un nodo amministratore, il processo di installazione del software crea un database Admin Node vuoto sul nodo recuperato. Tuttavia, il nuovo database include solo le informazioni relative ai server e ai servizi attualmente presenti nel sistema o aggiunti successivamente.

Se è stato ripristinato un nodo di amministrazione primario e il sistema StorageGRID dispone di un altro nodo di amministrazione, è possibile ripristinare le informazioni storiche copiando il database del nodo di amministrazione da un nodo di amministrazione non primario (il *nodo di amministrazione di origine*) al nodo di amministrazione primario recuperato. Se il sistema dispone solo di un nodo di amministrazione primario, non è possibile ripristinare il database del nodo di amministrazione.

> La copia del database Admin Node potrebbe richiedere diverse ore. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.
2. Dal nodo Admin di origine, arrestare il servizio MI: `service mi stop`
3. Dal nodo di amministrazione di origine, arrestare il servizio Management Application Program Interface (mgmt-api): `service mgmt-api stop`
4. Completare i seguenti passaggi sul nodo di amministrazione ripristinato:
   a. Accedere al nodo di amministrazione recuperato:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file.
   b. Arrestare il servizio MI: `service mi stop`
   c. Arrestare il servizio mgmt-api: `service mgmt-api stop`

d. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`

e. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

f. Copiare il database dal nodo Admin di origine al nodo Admin recuperato: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Quando richiesto, confermare che si desidera sovrascrivere il database MI nel nodo Admin recuperato.

   Il database e i relativi dati storici vengono copiati nel nodo di amministrazione recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato.

h. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`

5. Riavviare i servizi sul nodo di amministrazione di origine: `service servermanager start`

Ripristinare le metriche Prometheus durante il ripristino del nodo di amministrazione primario

Facoltativamente, è possibile conservare le metriche storiche gestite da Prometheus su un nodo di amministrazione primario che ha avuto problemi. Le metriche Prometheus possono essere ripristinate solo se il sistema StorageGRID include un altro nodo di amministrazione.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Hai il `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

In caso di guasto di un nodo di amministrazione, le metriche mantenute nel database Prometheus sul nodo di amministrazione andranno perse. Quando si ripristina l'Admin Node, il processo di installazione del software crea un nuovo database Prometheus. Una volta avviato il nodo di amministrazione recuperato, vengono registrate le metriche come se fosse stata eseguita una nuova installazione del sistema StorageGRID.

Se è stato ripristinato un nodo di amministrazione primario e il sistema StorageGRID dispone di un altro nodo di amministrazione, è possibile ripristinare le metriche storiche copiando il database Prometheus da un nodo di amministrazione non primario (il *nodo di amministrazione di origine*) al nodo di amministrazione primario recuperato. Se il sistema dispone solo di un nodo di amministrazione primario, non è possibile ripristinare il database Prometheus.

> La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

c. Immettere il seguente comando per passare a root: `su -`

d. Immettere la password elencata in `Passwords.txt` file.

2. Dal nodo Admin di origine, arrestare il servizio Prometheus: `service prometheus stop`

3. Completare i seguenti passaggi sul nodo di amministrazione ripristinato:

   a. Accedere al nodo di amministrazione recuperato:

      i. Immettere il seguente comando: `ssh admin@grid_node_IP`

      ii. Immettere la password elencata in `Passwords.txt` file.

      iii. Immettere il seguente comando per passare a root: `su -`

      iv. Immettere la password elencata in `Passwords.txt` file.

   b. Interrompere il servizio Prometheus: `service prometheus stop`

   c. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`

   d. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

   e. Copiare il database Prometheus dal nodo di amministrazione di origine al nodo di amministrazione recuperato: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

   f. Quando richiesto, premere **Invio** per confermare che si desidera distruggere il nuovo database Prometheus nel nodo di amministrazione recuperato.

      Il database Prometheus originale e i relativi dati storici vengono copiati nel nodo Admin recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato. Viene visualizzato il seguente stato:

Database clonato, avvio dei servizi

   a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`

4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.`service prometheus start`

Ripristino da guasti non primari del nodo di amministrazione

Recovery from non-Primary Admin Node failures (Ripristino da guasti non primari del nodo di amministrazione)

È necessario completare le seguenti attività per eseguire il ripristino da un errore non primario del nodo di amministrazione. Un nodo amministratore ospita il servizio CMN (Configuration Management Node) ed è noto come nodo amministratore primario. Sebbene sia possibile avere più nodi di amministrazione, ogni sistema StorageGRID include un solo nodo di amministrazione primario. Tutti gli altri nodi Admin non sono nodi Admin primari.

Copia i registri di controllo dal nodo di amministrazione non primario non riuscito

Se è possibile copiare i registri di controllo dal nodo di amministrazione non riuscito, è

necessario conservarli per mantenere il record dell'attività e dell'utilizzo del sistema della griglia. È possibile ripristinare i registri di controllo conservati nel nodo di amministrazione non primario recuperato una volta attivato e in esecuzione.

Questa procedura copia i file di log di audit dal nodo di amministrazione non riuscito in una posizione temporanea su un nodo griglia separato. Questi registri di controllo conservati possono quindi essere copiati nel nodo di amministrazione sostitutivo. I registri di controllo non vengono copiati automaticamente nel nuovo nodo di amministrazione.

A seconda del tipo di errore, potrebbe non essere possibile copiare i registri di controllo da un nodo di amministrazione non riuscito. Se l'implementazione ha un solo nodo di amministrazione, il nodo di amministrazione recuperato avvia la registrazione degli eventi nel registro di controllo in un nuovo file vuoto e i dati precedentemente registrati vengono persi. Se l'implementazione include più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione.

> Se i registri di controllo non sono ora accessibili sul nodo di amministrazione guasto, potrebbe essere possibile accedervi in un secondo momento, ad esempio dopo il ripristino dell'host.

1. Se possibile, accedere al nodo Admin non riuscito. In caso contrario, accedere al nodo di amministrazione primario o a un altro nodo di amministrazione, se disponibile.
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
2. Arrestare il servizio AMS per impedire la creazione di un nuovo file di log:`service ams stop`
3. Accedere alla directory di esportazione della verifica:

   ```
   cd /var/local/log
   ```
4. Rinominare il file di origine audit.log con un nome di file numerato univoco. Ad esempio, rinominare il file audit.log in `2023-10-25.txt.1`.

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```
5. Riavviare il servizio AMS: `service ams start`
6. Creare la directory per copiare tutti i file di log dell'audit in una posizione temporanea su un nodo griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Quando richiesto, inserire la password per admin.
7. Copiare tutti i file di log di controllo nella posizione temporanea: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Quando richiesto, inserire la password per admin.

8. Disconnettersi come root: `exit`

Sostituire nodo amministratore non primario

Per ripristinare un nodo di amministrazione non primario, è necessario sostituire l'hardware fisico o virtuale.

È possibile sostituire un nodo di amministrazione non primario guasto con un nodo di amministrazione non primario in esecuzione sulla stessa piattaforma oppure sostituire un nodo di amministrazione non primario in esecuzione su VMware o su un host Linux con un nodo di amministrazione non primario in hosting su un'appliance di servizi.

Utilizzare la procedura corrispondente alla piattaforma sostitutiva selezionata per il nodo. Una volta completata la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino del nodo Admin non primario.

Piattaforma sostitutiva	Procedura
VMware	"Sostituire un nodo VMware"
Linux	"Sostituire un nodo Linux"
Appliance di servizi	"Sostituire un'appliance di servizi"
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per "Sostituzione di un nodo Linux".

Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario

Dopo aver sostituito un nodo Admin non primario, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.
- Il nodo sostitutivo è stato implementato e configurato.

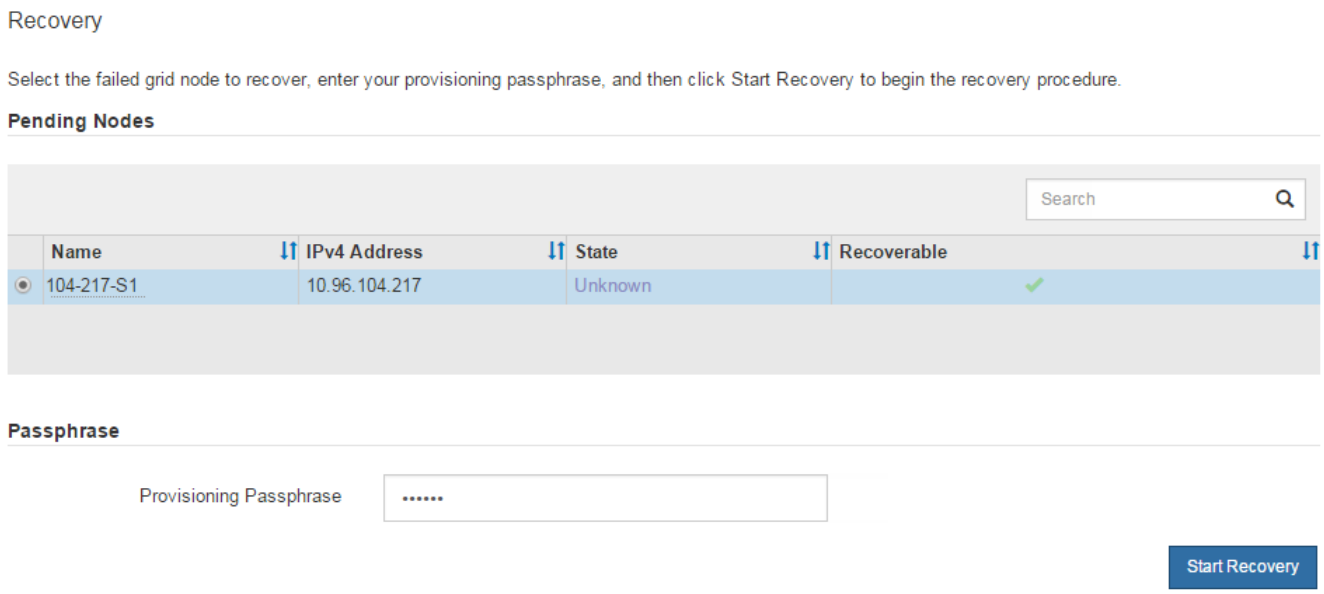
Fasi

1. In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **Ripristino**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

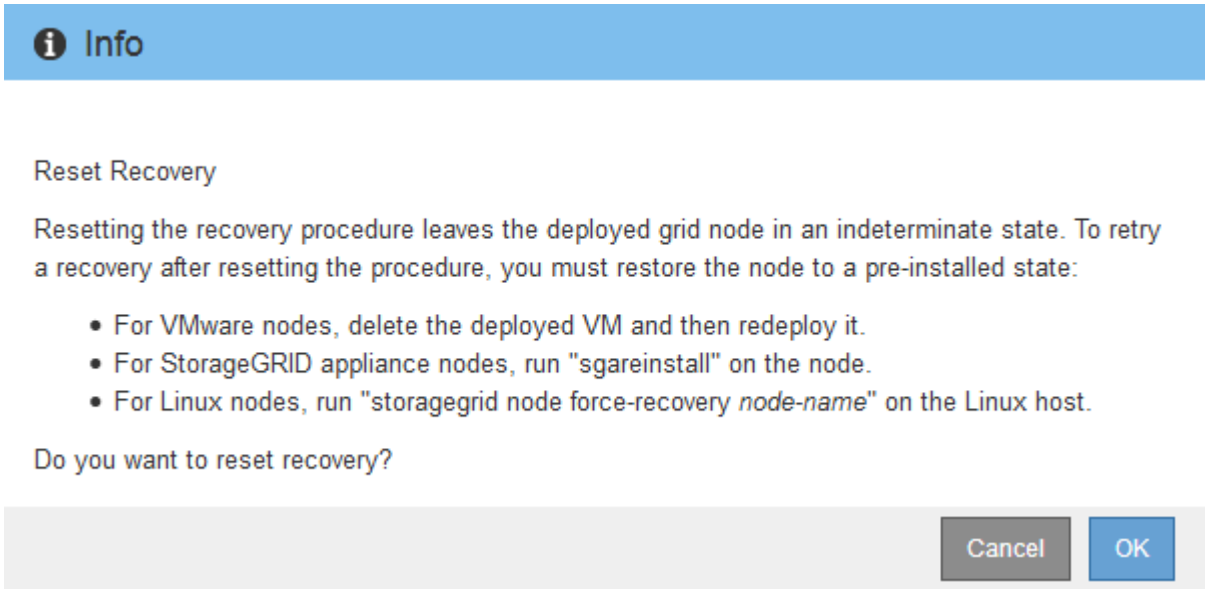
3. Immettere la **Provisioning Passphrase**.

4. Fare clic su **Start Recovery** (Avvia ripristino).



5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

> Durante l'esecuzione della procedura di ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware**: Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux**: Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`
- **Appliance**: Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario

ripristinare il nodo appliance a uno stato preinstallato eseguendo `sgareinstall` sul nodo. Vedere "Preparazione dell'appliance per la reinstallazione (solo sostituzione della piattaforma)".

6. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID e il trust della parte di base per il nodo di amministrazione ripristinato è stato configurato per utilizzare il certificato dell'interfaccia di gestione predefinita, aggiornare (o eliminare e ricreare) il trust della parte di base del nodo in Active Directory Federation Services (ad FS). Utilizzare il nuovo certificato server predefinito generato durante il processo di ripristino del nodo di amministrazione.

> Per configurare un trust di parte che si basa, vedere "Configurare il single sign-on". Per accedere al certificato del server predefinito, accedere alla shell dei comandi del nodo di amministrazione. Accedere alla `/var/local/mgmt-api` e selezionare `server.crt` file.

Ripristina log di audit su nodo Admin non primario recuperato

Se è stato possibile conservare il registro di controllo dal nodo di amministrazione non primario non riuscito, in modo da conservare le informazioni del registro di controllo cronologico, è possibile copiarle nel nodo di amministrazione non primario che si sta ripristinando.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- I registri di controllo sono stati copiati in un'altra posizione dopo l'errore del nodo di amministrazione originale.

A proposito di questa attività

In caso di errore di un nodo amministratore, i registri di controllo salvati in quel nodo amministratore potrebbero andare persi. Potrebbe essere possibile conservare i dati in caso di perdita copiando i registri di controllo dal nodo di amministrazione non riuscito e ripristinando questi registri di controllo nel nodo di amministrazione ripristinato. A seconda dell'errore, potrebbe non essere possibile copiare i registri di controllo dal nodo di amministrazione non riuscito. In tal caso, se l'implementazione ha più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione, poiché i registri di controllo vengono replicati in tutti i nodi di amministrazione.

Se esiste un solo nodo Admin e non è possibile copiare il log di audit dal nodo guasto, il nodo Admin recuperato inizia a registrare gli eventi nel log di audit come se l'installazione fosse nuova.

Per ripristinare la funzionalità di registrazione, è necessario ripristinare un nodo amministratore il prima possibile.

> Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile saltare questi passaggi se si verifica una delle seguenti condizioni:
>
> - È stato configurato un server syslog esterno e i registri di controllo vengono inviati al server syslog invece che ai nodi di amministrazione.
> - È stato specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.
>
> Vedere "Configurare i messaggi di audit e le destinazioni dei log" per ulteriori informazioni.

Fasi

1. Accedere al nodo di amministrazione recuperato:

   a. Immettere il seguente comando:

      `ssh admin@recovery_Admin_Node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Controllare quali file di audit sono stati conservati:

   `cd /var/local/log`

3. Copiare i file di log di controllo conservati nel nodo di amministrazione recuperato:

   `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*`

   Quando richiesto, inserire la password per admin.

4. Per motivi di sicurezza, eliminare i registri di controllo dal nodo Grid guasto dopo aver verificato che siano stati copiati correttamente nel nodo Admin ripristinato.

5. Aggiornare le impostazioni di utente e gruppo dei file di log di controllo sul nodo di amministrazione recuperato:

   `chown ams-user:bycast *`

6. Disconnettersi come root: `exit`

È inoltre necessario ripristinare qualsiasi accesso client preesistente alla condivisione di controllo. Per ulteriori informazioni, vedere "Configurare l'accesso al client di audit".

Ripristinare il database Admin Node durante il ripristino del nodo Admin non primario

Se si desidera conservare le informazioni cronologiche relative ad attributi, allarmi e avvisi su un nodo di amministrazione non primario che ha avuto esito negativo, è possibile ripristinare il database del nodo di amministrazione dal nodo di amministrazione primario.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Hai il `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

In caso di errore di un nodo amministratore, le informazioni storiche memorizzate nel database del nodo

amministratore andranno perse. Questo database include le seguenti informazioni:

- Cronologia degli avvisi
- Cronologia degli allarmi
- Dati storici degli attributi, utilizzati nei grafici e nei report di testo disponibili nella pagina **SUPPORTO** > **Strumenti** > **topologia griglia**.

Quando si ripristina un nodo amministratore, il processo di installazione del software crea un database Admin Node vuoto sul nodo recuperato. Tuttavia, il nuovo database include solo le informazioni relative ai server e ai servizi attualmente presenti nel sistema o aggiunti successivamente.

Se è stato ripristinato un nodo Admin non primario, è possibile ripristinare le informazioni storiche copiando il database del nodo Admin dal nodo Admin primario (il *nodo Admin di origine*) nel nodo recuperato.

> La copia del database Admin Node potrebbe richiedere diverse ore. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.
2. Eseguire il seguente comando dal nodo di amministrazione di origine. Quindi, inserire la passphrase di provisioning, se richiesto. `recover-access-points`
3. Dal nodo Admin di origine, arrestare il servizio MI: `service mi stop`
4. Dal nodo di amministrazione di origine, arrestare il servizio Management Application Program Interface (mgmt-api): `service mgmt-api stop`
5. Completare i seguenti passaggi sul nodo di amministrazione ripristinato:
   a. Accedere al nodo di amministrazione recuperato:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file.
   b. Arrestare il servizio MI: `service mi stop`
   c. Arrestare il servizio mgmt-api: `service mgmt-api stop`
   d. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`
   e. Inserire la password di accesso SSH elencata in `Passwords.txt` file.
   f. Copiare il database dal nodo Admin di origine al nodo Admin recuperato: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Quando richiesto, confermare che si desidera sovrascrivere il database MI nel nodo Admin recuperato.

Il database e i relativi dati storici vengono copiati nel nodo di amministrazione recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato.

h. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`

6. Riavviare i servizi sul nodo di amministrazione di origine: `service servermanager start`

Ripristinare le metriche Prometheus durante il ripristino del nodo di amministrazione non primario

In alternativa, è possibile conservare le metriche storiche gestite da Prometheus su un nodo amministrativo non primario che ha avuto problemi.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Hai il `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

In caso di guasto di un nodo di amministrazione, le metriche mantenute nel database Prometheus sul nodo di amministrazione andranno perse. Quando si ripristina l'Admin Node, il processo di installazione del software crea un nuovo database Prometheus. Una volta avviato il nodo di amministrazione recuperato, vengono registrate le metriche come se fosse stata eseguita una nuova installazione del sistema StorageGRID.

Se è stato ripristinato un nodo di amministrazione non primario, è possibile ripristinare le metriche storiche copiando il database Prometheus dal nodo di amministrazione primario (il *nodo di amministrazione di origine*) al nodo di amministrazione recuperato.

> La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.
2. Dal nodo Admin di origine, arrestare il servizio Prometheus: `service prometheus stop`
3. Completare i seguenti passaggi sul nodo di amministrazione ripristinato:
   a. Accedere al nodo di amministrazione recuperato:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`

iv. Immettere la password elencata in `Passwords.txt` file.

b. Interrompere il servizio Prometheus: `service prometheus stop`

c. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`

d. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

e. Copiare il database Prometheus dal nodo di amministrazione di origine al nodo di amministrazione recuperato: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Quando richiesto, premere **Invio** per confermare che si desidera distruggere il nuovo database Prometheus nel nodo di amministrazione recuperato.

   Il database Prometheus originale e i relativi dati storici vengono copiati nel nodo Admin recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato. Viene visualizzato il seguente stato:

Database clonato, avvio dei servizi

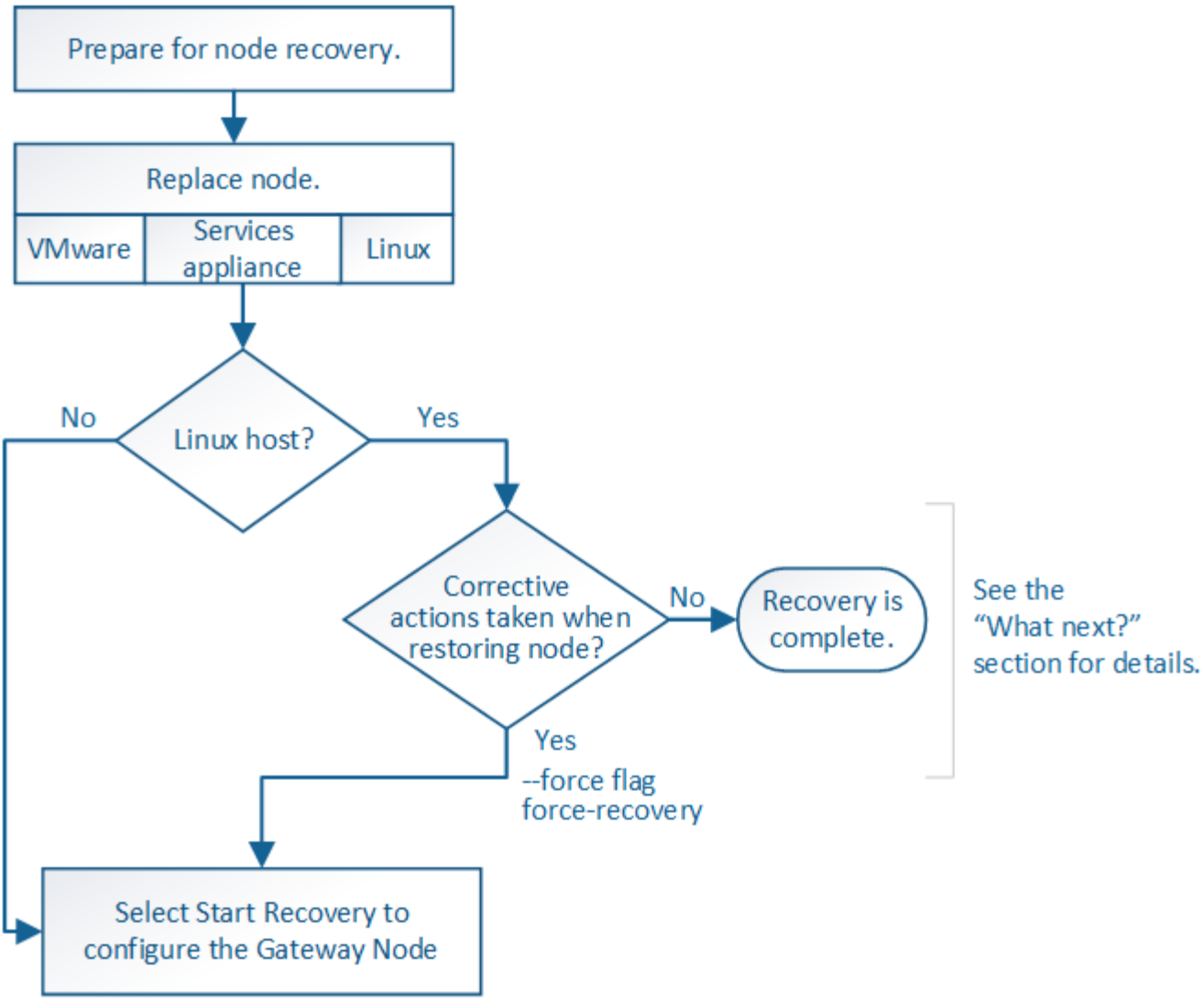
a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`

4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.`service prometheus start`

Ripristino da guasti del nodo gateway

Recovery from Gateway Node Failures: Workflow

È necessario completare una sequenza di attività nell'ordine esatto per eseguire il ripristino in caso di guasto di un nodo gateway.



Sostituire il nodo gateway

È possibile sostituire un nodo gateway guasto con un nodo gateway in esecuzione sullo stesso hardware fisico o virtuale oppure sostituire un nodo gateway in esecuzione su VMware o su un host Linux con un nodo gateway in hosting su un'appliance di servizi.

La procedura di sostituzione del nodo da seguire dipende dalla piattaforma utilizzata dal nodo sostitutivo. Una volta completata la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino del nodo gateway.

Piattaforma sostitutiva	Procedura
VMware	"Sostituire un nodo VMware"
Linux	"Sostituire un nodo Linux"
Appliance di servizi	"Sostituire un'appliance di servizi"

Piattaforma sostitutiva	Procedura
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per "Sostituzione di un nodo Linux".

Selezionare Avvia ripristino per configurare il nodo gateway

Dopo aver sostituito un nodo gateway, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Prima di iniziare

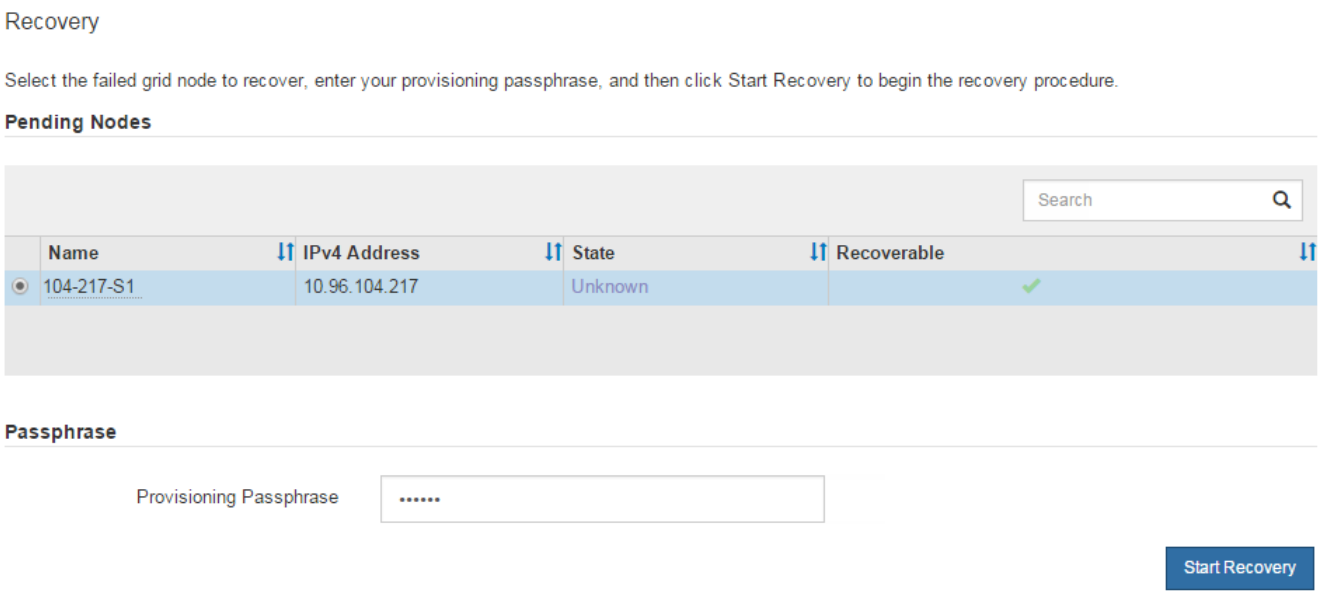
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.
- Il nodo sostitutivo è stato implementato e configurato.

Fasi

1. In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **Ripristino**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

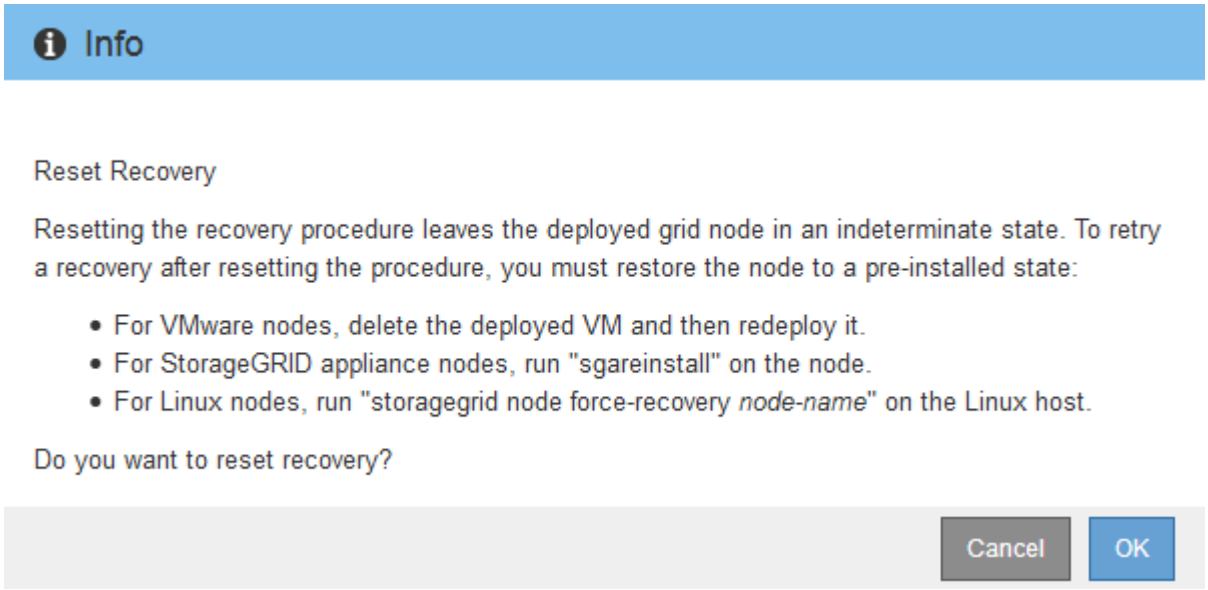
   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Immettere la **Provisioning Passphrase**.
4. Fare clic su **Start Recovery** (Avvia ripristino).



5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

Durante l'esecuzione della procedura di ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



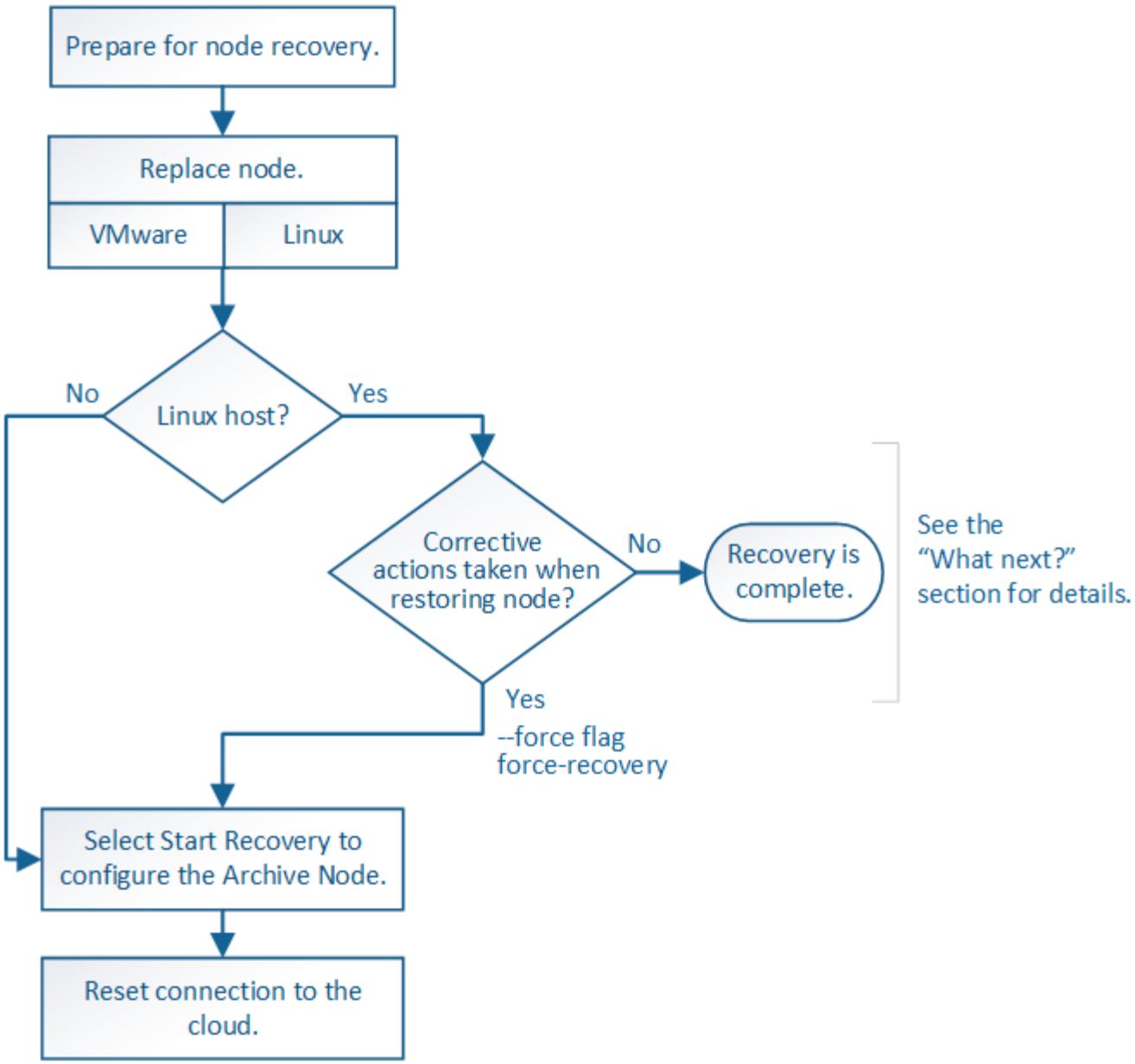
Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware**: Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux**: Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`
- **Appliance**: Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo appliance a uno stato preinstallato eseguendo `sgareinstall` sul nodo. Vedere "Preparazione dell'appliance per la reinstallazione (solo sostituzione della piattaforma)".

Ripristino da errori del nodo di archiviazione

Recovery from Archive Node Failures: Workflow

È necessario completare una sequenza di attività nell'ordine esatto per eseguire il ripristino in caso di guasto di un nodo di archiviazione.



Il ripristino del nodo di archiviazione è interessato dai seguenti problemi:

- Se il criterio ILM è configurato per replicare una singola copia.

  In un sistema StorageGRID configurato per eseguire una singola copia di oggetti, un guasto al nodo di archiviazione potrebbe causare una perdita di dati irreversibile. In caso di errore, tutti questi oggetti vengono persi; tuttavia, è necessario eseguire le procedure di ripristino per "ripulire" il sistema StorageGRID ed eliminare le informazioni sugli oggetti persi dal database.

- Se si verifica un errore del nodo di archiviazione durante il ripristino del nodo di storage.

  Se il nodo di archiviazione non riesce durante l'elaborazione di recuperi in blocco come parte di un ripristino del nodo di storage, È necessario ripetere la procedura per ripristinare le copie dei dati dell'oggetto nel nodo di storage dall'inizio per garantire che tutti i dati dell'oggetto recuperati dal nodo di archiviazione vengano ripristinati nel nodo di storage.

Sostituisci nodo archivio

Per ripristinare un nodo di archiviazione, è necessario sostituirlo.

Selezionare la procedura di sostituzione del nodo per la piattaforma. I passaggi per sostituire un nodo sono gli stessi per tutti i tipi di nodi griglia.

Piattaforma	Procedura
VMware	"Sostituire un nodo VMware"
Linux	"Sostituire un nodo Linux"
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per "Sostituzione di un nodo Linux".

Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di archiviazione

Dopo aver sostituito un nodo di archiviazione, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Prima di iniziare

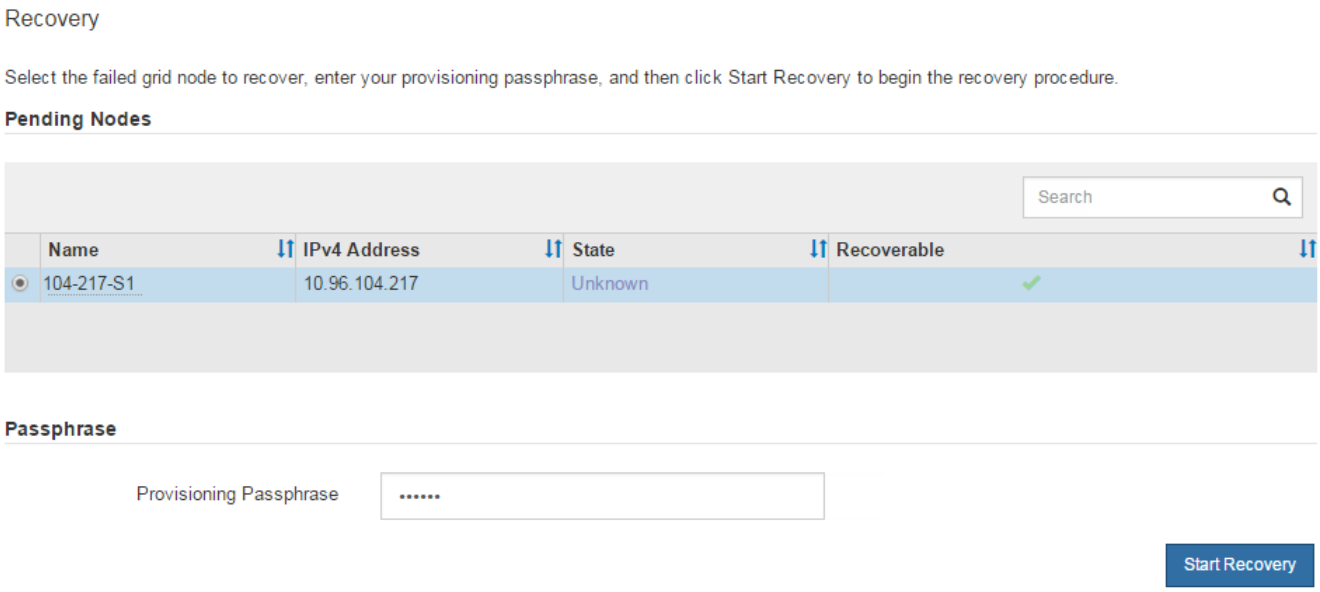
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning.
- Il nodo sostitutivo è stato implementato e configurato.

Fasi

1. In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **Ripristino**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

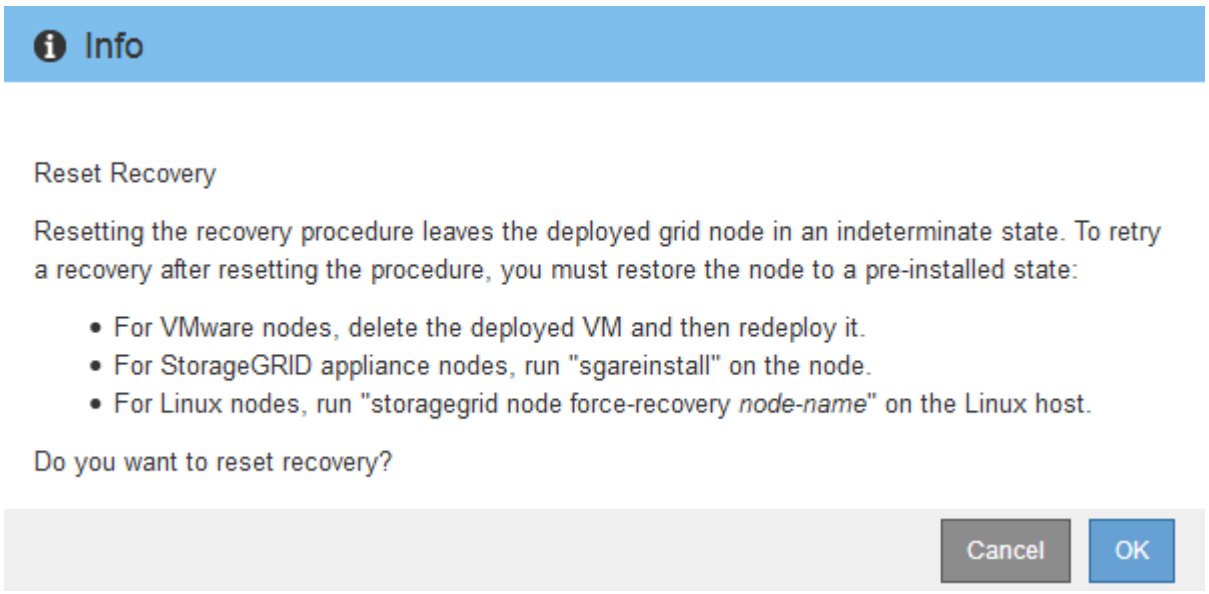
   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Immettere la **Provisioning Passphrase**.
4. Fare clic su **Start Recovery** (Avvia ripristino).



5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

> Durante l'esecuzione della procedura di ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware**: Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux**: Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`

Ripristinare la connessione del nodo di archiviazione al cloud

Dopo aver ripristinato un nodo di archiviazione che ha come destinazione il cloud tramite l'API S3, è necessario modificare le impostazioni di configurazione per ripristinare le connessioni. Un allarme ORSU (Outbound Replication Status) viene attivato se il nodo di archiviazione non è in grado di recuperare i dati dell'oggetto.

> Se il nodo di archiviazione si connette allo storage esterno tramite il middleware TSM, il nodo si ripristina automaticamente e non è necessario riconfigurare.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare **Archive Node** > **ARC** > **Target**.
3. Modificare il campo **Access Key** inserendo un valore errato e fare clic su **Apply Changes** (Applica modifiche).
4. Modificare il campo **Access Key** inserendo il valore corretto e fare clic su **Apply Changes** (Applica modifiche).

Sostituire il nodo Linux

Sostituire il nodo Linux

Se un guasto richiede l'implementazione di uno o più nuovi host fisici o virtuali o la reinstallazione di Linux su un host esistente, implementare e configurare l'host sostitutivo prima di poter ripristinare il nodo grid. Questa procedura è una fase del processo di ripristino del nodo grid per tutti i tipi di nodi grid.

"Linux" si riferisce a una distribuzione Red Hat® Enterprise Linux®, Ubuntu® o Debian®. Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp (IMT)".

Questa procedura viene eseguita solo come una fase del processo di ripristino dei nodi di storage basati su software, dei nodi di amministrazione primari o non primari, dei nodi gateway o dei nodi di archivio. I passaggi sono identici indipendentemente dal tipo di nodo di griglia che si sta ripristinando.

Se su un host Linux fisico o virtuale sono ospitati più nodi grid, è possibile ripristinare i nodi grid in qualsiasi ordine. Tuttavia, il ripristino di un nodo di amministrazione primario, se presente, impedisce il blocco del ripristino di altri nodi della griglia quando tentano di contattare il nodo di amministrazione primario per la registrazione per il ripristino.

Implementare nuovi host Linux

Con alcune eccezioni, è possibile preparare i nuovi host come durante il processo di installazione iniziale.

Per implementare host Linux fisici o virtuali nuovi o reinstallati, seguire la procedura per la preparazione degli host nelle istruzioni di installazione di StorageGRID per il sistema operativo Linux in uso:

- "Installare Linux (Red Hat Enterprise Linux)"
- "Installare Linux (Ubuntu o Debian)"

Questa procedura include i passaggi per eseguire le seguenti attività:

1. Installare Linux.
2. Configurare la rete host.
3. Configurare lo storage host.
4. Installare il motore del container.
5. Installare il servizio host StorageGRID.

> Interrompere dopo aver completato l'attività "Installa servizio host StorageGRID" nelle istruzioni di installazione. Non avviare l'attività "distribuzione dei nodi della griglia".

Durante l'esecuzione di questi passaggi, prendere nota delle seguenti importanti linee guida:

- Assicurarsi di utilizzare gli stessi nomi di interfaccia host utilizzati sull'host originale.
- Se si utilizza lo storage condiviso per supportare i nodi StorageGRID o si sono spostati alcuni o tutti i dischi o gli SSD dai nodi guasti ai nodi sostitutivi, è necessario ristabilire le stesse mappature dello storage presenti sull'host originale. Ad esempio, se sono stati utilizzati WWID e alias in `/etc/multipath.conf` Come consigliato nelle istruzioni di installazione, assicurarsi di utilizzare le stesse coppie alias/WWID in `/etc/multipath.conf` sull'host sostitutivo.
- Se il nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verifica che il volume non disponga di una policy di tiering FabricPool abilitata. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

> Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

Ripristinare i nodi della griglia nell'host

Per ripristinare un nodo Grid guasto in un nuovo host Linux, eseguire questa procedura per ripristinare il file di configurazione del nodo.

1. Ripristinare e convalidare il nodo ripristinando il file di configurazione del nodo. Per una nuova installazione, viene creato un file di configurazione del nodo per ciascun nodo della griglia da installare su un host. Quando si ripristina un nodo della griglia su un host sostitutivo, il file di configurazione del nodo viene ripristinato o sostituito per eventuali nodi della griglia guasti.
2. Avviare il servizio host StorageGRID.
3. In base alle necessità, ripristinare i nodi che non si avviano.

Se sono stati conservati volumi di storage a blocchi dall'host precedente, potrebbe essere necessario eseguire ulteriori procedure di ripristino. I comandi di questa sezione consentono di determinare quali procedure aggiuntive sono necessarie.

Ripristinare e validare i nodi della griglia

È necessario ripristinare i file di configurazione della griglia per eventuali nodi della griglia guasti, quindi validare i file di configurazione della griglia e risolvere eventuali errori.

A proposito di questa attività

È possibile importare qualsiasi nodo di griglia che dovrebbe essere presente sull'host, a condizione che sia `/var/local` il volume non è stato perso a causa del guasto dell'host precedente. Ad esempio, il `/var/local` Il volume potrebbe ancora esistere se si utilizza lo storage condiviso per i volumi di dati del sistema StorageGRID, come descritto nelle istruzioni di installazione di StorageGRID per il sistema operativo Linux in uso. L'importazione del nodo ripristina il file di configurazione del nodo sull'host.

Se non è possibile importare nodi mancanti, è necessario ricreare i file di configurazione della griglia.

È quindi necessario convalidare il file di configurazione della griglia e risolvere eventuali problemi di rete o storage che potrebbero verificarsi prima di riavviare StorageGRID. Quando si crea nuovamente il file di configurazione per un nodo, è necessario utilizzare lo stesso nome per il nodo sostitutivo utilizzato per il nodo che si sta ripristinando.

Per ulteriori informazioni sulla posizione di, consultare le istruzioni di installazione di `/var/local` volume per un nodo.

- "Installare StorageGRID su Red Hat Enterprise Linux"
- "Installare StorageGRID su Ubuntu o Debian"

Fasi

1. Nella riga di comando dell'host recuperato, elencare tutti i nodi StorageGRID attualmente configurati:`sudo storagegrid node list`

   Se non sono configurati nodi di griglia, non verrà generato alcun output. Se alcuni nodi della griglia sono configurati, l'output deve essere nel seguente formato:

   ```
   Name               Metadata-Volume
   ============================================================
   dc1-adm1           /dev/mapper/sgws-adm1-var-local
   dc1-gw1            /dev/mapper/sgws-gw1-var-local
   dc1-sn1            /dev/mapper/sgws-sn1-var-local
   dc1-arc1           /dev/mapper/sgws-arc1-var-local
   ```

   Se alcuni o tutti i nodi della griglia che devono essere configurati sull'host non sono elencati, è necessario ripristinare i nodi della griglia mancanti.

2. Per importare nodi griglia che hanno un `/var/local` volume:

   a. Eseguire il seguente comando per ciascun nodo da importare:`sudo storagegrid node import node-var-local-volume-path`

      Il `storagegrid node import` il comando ha esito positivo solo se il nodo di destinazione è stato chiuso correttamente sull'host su cui è stato eseguito l'ultima volta. In caso contrario, si verificherà un errore simile al seguente:

```
    This node (node-name) appears to be owned by another host (UUID host-uuid).

Use the --force flag if you are sure import is safe.
```

a. Se viene visualizzato un errore relativo al nodo di proprietà di un altro host, eseguire nuovamente il comando con `--force` contrassegno per completare l'importazione:`sudo storagegrid --force node import node-var-local-volume-path`

> Tutti i nodi importati con `--force` flag richiederà ulteriori passaggi di ripristino prima che possano ricongiungersi alla griglia, come descritto in "Cosa c'è di seguito: Se necessario, eseguire ulteriori passaggi di ripristino".

3. Per i nodi griglia che non dispongono di `/var/local` creare nuovamente il file di configurazione del nodo per ripristinarlo nell'host. Per istruzioni, vedere:

   - "Creare file di configurazione dei nodi per Red Hat Enterprise Linux"
   - "Creare file di configurazione del nodo per Ubuntu o Debian"

> Quando si crea nuovamente il file di configurazione per un nodo, è necessario utilizzare lo stesso nome per il nodo sostitutivo utilizzato per il nodo che si sta ripristinando. Per le implementazioni Linux, assicurarsi che il nome del file di configurazione contenga il nome del nodo. Se possibile, utilizzare le stesse interfacce di rete, le mappature dei dispositivi a blocchi e gli stessi indirizzi IP. Questa procedura riduce al minimo la quantità di dati che devono essere copiati nel nodo durante il ripristino, il che potrebbe rendere il ripristino molto più rapido (in alcuni casi, minuti piuttosto che settimane).

> Se si utilizzano nuovi dispositivi a blocchi (dispositivi che il nodo StorageGRID non ha utilizzato in precedenza) come valori per una qualsiasi delle variabili di configurazione che iniziano con `BLOCK_DEVICE_` quando si crea nuovamente il file di configurazione per un nodo, seguire le linee guida in Correggere gli errori del dispositivo a blocchi mancanti.

4. Eseguire il seguente comando sull'host ripristinato per elencare tutti i nodi StorageGRID.

```
sudo storagegrid node list
```

5. Convalidare il file di configurazione del nodo per ogni nodo della griglia il cui nome è stato visualizzato nell'output dell'elenco dei nodi StorageGRID:

```
sudo storagegrid node validate node-name
```

   Prima di avviare il servizio host StorageGRID, è necessario risolvere eventuali errori o avvisi. Le sezioni seguenti forniscono ulteriori dettagli sugli errori che potrebbero avere un significato speciale durante il ripristino.

Correggere gli errori di interfaccia di rete mancanti

Se la rete host non è configurata correttamente o se un nome viene scritto in modo errato, si verifica un errore quando StorageGRID controlla la mappatura specificata in `/etc/storagegrid/nodes/node-name.conf` file.

Potrebbe essere visualizzato un errore o un avviso corrispondente a questo modello:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

L'errore potrebbe essere segnalato per Grid Network, Admin Network o Client Network. Questo errore indica che `/etc/storagegrid/nodes/node-name.conf` Il file associa la rete StorageGRID indicata all'interfaccia host denominata *`host-interface-name`*, ma non esiste alcuna interfaccia con questo nome sull'host corrente.

Se viene visualizzato questo errore, verificare di aver completato la procedura descritta in "Implementare nuovi host Linux". Utilizzare gli stessi nomi per tutte le interfacce host utilizzati sull'host originale.

Se non è possibile assegnare un nome alle interfacce host in modo che corrispondano al file di configurazione del nodo, è possibile modificare il file di configurazione del nodo e modificare il valore DI GRID_NETWORK_TARGET, ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET in modo che corrisponda a un'interfaccia host esistente.

Assicurarsi che l'interfaccia host fornisca l'accesso alla porta di rete fisica o alla VLAN appropriata e che l'interfaccia non faccia riferimento direttamente a un dispositivo di collegamento o di bridge. È necessario configurare una VLAN (o un'altra interfaccia virtuale) sulla parte superiore del dispositivo bond sull'host oppure utilizzare una coppia di bridge e Virtual Ethernet (veth).

Correggere gli errori del dispositivo a blocchi mancanti

Il sistema verifica che ciascun nodo recuperato sia mappato a un file speciale valido per il dispositivo a blocchi o a un softlink valido a un file speciale per il dispositivo a blocchi. Se StorageGRID rileva una mappatura non valida in `/etc/storagegrid/nodes/node-name.conf` file, viene visualizzato un errore di dispositivo a blocchi mancante.

Se si verifica un errore corrispondente a questo modello:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

Significa che `/etc/storagegrid/nodes/node-name.conf` mappa il dispositivo a blocchi utilizzato da *node-name* per `PURPOSE` Al nome del percorso specificato nel file system Linux, ma non esiste un file speciale valido per il dispositivo a blocchi o un softlink a un file speciale per il dispositivo a blocchi in tale posizione.

Verificare di aver completato le operazioni descritte in "Implementare nuovi host Linux". Utilizzare gli stessi nomi persistenti dei dispositivi per tutti i dispositivi a blocchi utilizzati sull'host originale.

Se non è possibile ripristinare o ricreare il file speciale del dispositivo a blocchi mancante, è possibile allocare un nuovo dispositivo a blocchi della dimensione e della categoria di storage appropriate e modificare il file di configurazione del nodo per modificare il valore di `BLOCK_DEVICE_PURPOSE` per puntare al nuovo file speciale del dispositivo a blocchi.

Determinare le dimensioni e la categoria di storage appropriate utilizzando le tabelle per il sistema operativo

Linux in uso:

- "Requisiti di storage e prestazioni per Red Hat Enterprise Linux"
- "Requisiti di storage e performance per Ubuntu o Debian"

Prima di procedere con la sostituzione del dispositivo a blocchi, consultare le raccomandazioni per la configurazione dello storage host:

- "Configurare lo storage host per Red Hat Enterprise Linux"
- "Configurare lo storage host per Ubuntu o Debian"

> Se è necessario fornire un nuovo dispositivo di storage a blocchi per qualsiasi variabile del file di configurazione che inizia con `BLOCK_DEVICE_` poiché il dispositivo a blocchi originale è stato perso con l'host guasto, assicurarsi che il nuovo dispositivo a blocchi non sia formattato prima di tentare ulteriori procedure di ripristino. Il nuovo dispositivo a blocchi non verrà formattato se si utilizza lo storage condiviso e si è creato un nuovo volume. In caso di dubbi, eseguire il seguente comando per tutti i nuovi file speciali del dispositivo di storage a blocchi.

> Eseguire il seguente comando solo per i nuovi dispositivi di storage a blocchi. Non eseguire questo comando se si ritiene che lo storage a blocchi contenga ancora dati validi per il nodo da ripristinare, in quanto i dati sul dispositivo andranno persi.
>
> ```
> sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
> ```

Avviare il servizio host StorageGRID

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

Fasi

1. Eseguire i seguenti comandi su ciascun host:

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

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

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

3. Se un nodo restituisce lo stato "Not Running" (non in esecuzione) o "Stopped" (arrestato), eseguire il comando seguente:

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

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

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

Ripristinare i nodi che non si avviano normalmente

Se un nodo StorageGRID non si ricongiungerà normalmente alla griglia e non verrà visualizzato come ripristinabile, potrebbe essere danneggiato. È possibile forzare il nodo in modalità di ripristino.

Fasi

1. Verificare che la configurazione di rete del nodo sia corretta.

   Il nodo potrebbe non essere riuscito a ricongiungersi alla griglia a causa di mappature dell'interfaccia di rete non corrette o di un gateway o indirizzo IP Grid Network non corretto.

2. Se la configurazione di rete è corretta, eseguire il `force-recovery` comando:

   `sudo storagegrid node force-recovery node-name`

3. Eseguire le fasi di ripristino aggiuntive per il nodo. Vedere "Cosa c'è di seguito: Se necessario, eseguire ulteriori passaggi di ripristino".

Cosa succederà dopo: Se necessario, eseguire ulteriori passaggi di ripristino

A seconda delle azioni specifiche intraprese per eseguire i nodi StorageGRID sull'host sostitutivo, potrebbe essere necessario eseguire ulteriori operazioni di ripristino per ciascun nodo.

Il ripristino del nodo è completo se non è stato necessario intraprendere alcuna azione correttiva durante la sostituzione dell'host Linux o il ripristino del nodo Grid guasto nel nuovo host.

Azioni correttive e passi successivi

Durante la sostituzione del nodo, potrebbe essere necessario intraprendere una delle seguenti azioni correttive:

- È stato necessario utilizzare `--force` flag per importare il nodo.
- Per qualsiasi `<PURPOSE>`, il valore di `BLOCK_DEVICE_<PURPOSE>` la variabile del file di configurazione si riferisce a un dispositivo a blocchi che non contiene gli stessi dati che ha fatto prima dell'errore dell'host.
- Hai emesso `storagegrid node force-recovery node-name` per il nodo.
- È stato aggiunto un nuovo dispositivo a blocchi.

Se è stata eseguita una di queste azioni correttive, è necessario eseguire ulteriori operazioni di ripristino.

Tipo di ripristino	Passo successivo
Nodo amministratore primario	"Configurare il nodo amministrativo primario sostitutivo"

Tipo di ripristino	Passo successivo
Nodo amministrativo non primario	"Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario"
Nodo gateway	"Selezionare Avvia ripristino per configurare il nodo gateway"
Nodo di archiviazione	"Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di archiviazione"
Nodo di storage (basato su software): • Se è stato necessario utilizzare `--force` contrassegno per importare il nodo o emesso `storagegrid node force-recovery node-name` • Se è stata eseguita una reinstallazione completa del nodo o se è stato necessario ripristinare /var/local	"Selezionare Avvia ripristino per configurare il nodo di storage"
Nodo di storage (basato su software): • Se è stato aggiunto un nuovo dispositivo a blocchi. • Se, per qualsiasi `<PURPOSE>`, il valore di `BLOCK_DEVICE_<PURPOSE>` la variabile del file di configurazione si riferisce a un dispositivo a blocchi che non contiene gli stessi dati che ha fatto prima dell'errore dell'host.	"Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto"

Sostituire il nodo VMware

Quando si ripristina un nodo StorageGRID guasto ospitato su VMware, si rimuove il nodo guasto e si implementa un nodo di ripristino.

Prima di iniziare

Hai determinato che la macchina virtuale non può essere ripristinata e deve essere sostituita.

A proposito di questa attività

VMware vSphere Web Client viene utilizzato per rimuovere prima la macchina virtuale associata al nodo Grid guasto. Quindi, è possibile implementare una nuova macchina virtuale.

Questa procedura è solo una fase del processo di ripristino del nodo grid. La procedura di rimozione e implementazione dei nodi è la stessa per tutti i nodi VMware, inclusi i nodi Admin, i nodi Storage, i nodi Gateway e i nodi Archive.

Fasi

1. Accedere a VMware vSphere Web Client.
2. Passare alla macchina virtuale del nodo della griglia guasto.

3. Prendere nota di tutte le informazioni necessarie per implementare il nodo di ripristino.
   a. Fare clic con il pulsante destro del mouse sulla macchina virtuale, selezionare la scheda **Edit Settings** (Modifica impostazioni) e annotare le impostazioni in uso.
   b. Selezionare la scheda **vApp Options** per visualizzare e registrare le impostazioni di rete del nodo della griglia.
4. Se il nodo Grid guasto è un nodo Storage, determinare se uno dei dischi rigidi virtuali utilizzati per lo storage dei dati non è danneggiato e conservarlo per il ricollegamento al nodo Grid ripristinato.
5. Spegnere la macchina virtuale.
6. Selezionare **azioni** > **tutte le azioni vCenter** > **Elimina dal disco** per eliminare la macchina virtuale.
7. Implementare una nuova macchina virtuale come nodo sostitutivo e connetterla a una o più reti StorageGRID. Per istruzioni, vedere "Implementazione di un nodo StorageGRID come macchina virtuale".

   Quando si implementa il nodo, è possibile rimappare le porte del nodo o aumentare le impostazioni della CPU o della memoria.

   > Dopo aver implementato il nuovo nodo, è possibile aggiungere nuovi dischi virtuali in base ai requisiti di storage, ricollegare eventuali dischi rigidi virtuali conservati dal nodo Grid guasto precedentemente rimosso o da entrambi.

8. Completare la procedura di ripristino del nodo, in base al tipo di nodo che si sta ripristinando.

Tipo di nodo	Passare a.
Nodo amministratore primario	"Configurare il nodo amministrativo primario sostitutivo"
Nodo amministrativo non primario	"Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario"
Nodo gateway	"Selezionare Avvia ripristino per configurare il nodo gateway"
Nodo di storage	"Selezionare Avvia ripristino per configurare il nodo di storage"
Nodo di archiviazione	"Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di archiviazione"

Sostituire il nodo guasto con l'appliance di servizi

Sostituisci nodo guasto con appliance di servizi: Panoramica

È possibile utilizzare un'appliance di servizi per recuperare un nodo gateway guasto, un nodo di amministrazione non primario guasto o un nodo di amministrazione primario guasto ospitato su VMware, un host Linux o un'appliance di servizi. Questa procedura è una fase della procedura di ripristino del nodo di rete.

Prima di iniziare

- Hai determinato che è vera una delle seguenti situazioni:

- Impossibile ripristinare la macchina virtuale che ospita il nodo.
- L'host Linux fisico o virtuale per il nodo grid è guasto e deve essere sostituito.
- L'appliance di servizi che ospita il nodo Grid deve essere sostituita.

- Hai confermato che la versione del programma di installazione dell'appliance StorageGRID sul dispositivo di servizi corrisponde alla versione software del tuo sistema StorageGRID. Vedere "Verificare e aggiornare la versione del programma di installazione dell'appliance StorageGRID".

> Non installare un'appliance di servizi SG110 e SG1100 o un'appliance di servizi SG100 e SG1000 nello stesso sito. Potrebbero verificarsi performance imprevedibili.

A proposito di questa attività

È possibile utilizzare un'appliance per i servizi per ripristinare un nodo grid guasto nei seguenti casi:

- Il nodo guasto è stato ospitato su VMware o Linux ("cambiamento di piattaforma")
- Il nodo guasto è stato ospitato su un'appliance di servizi ("sostituzione della piattaforma")

Installare l'appliance di servizi (solo modifica della piattaforma)

Quando si ripristina un nodo Grid guasto ospitato su VMware o su un host Linux e si utilizza un'appliance di servizi per il nodo sostitutivo, è necessario prima installare il nuovo hardware dell'appliance utilizzando lo stesso nome di nodo (nome di sistema) del nodo guasto.

Prima di iniziare

Sono disponibili le seguenti informazioni sul nodo guasto:

- **Node name** (Nome nodo): È necessario installare l'appliance di servizi utilizzando lo stesso nome di nodo del nodo guasto. Il nome del nodo è il nome host (nome del sistema).
- **Indirizzi IP**: È possibile assegnare al dispositivo di servizi gli stessi indirizzi IP del nodo guasto, che è l'opzione preferita, oppure selezionare un nuovo indirizzo IP inutilizzato su ciascuna rete.

A proposito di questa attività

Eseguire questa procedura solo se si sta ripristinando un nodo guasto ospitato su VMware o Linux e lo si sta sostituendo con un nodo ospitato su un'appliance di servizi.

Fasi

1. Seguire le istruzioni per l'installazione di un nuovo dispositivo di servizi. Vedere "Avvio rapido per l'installazione dell'hardware".
2. Quando viene richiesto il nome di un nodo, utilizzare il nome del nodo guasto.

Preparazione dell'appliance per la reinstallazione (solo sostituzione della piattaforma)

Durante il ripristino di un nodo Grid ospitato su un'appliance di servizi, è necessario preparare l'appliance per la reinstallazione del software StorageGRID.

Eseguire questa procedura solo se si sta sostituendo un nodo guasto ospitato su un'appliance di servizi. Non seguire questi passaggi se il nodo guasto era originariamente ospitato su un host VMware o Linux.

Fasi

1. Accedere al nodo Grid guasto:

   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Preparare l'appliance per l'installazione del software StorageGRID. Inserire: `sgareinstall`

3. Quando viene richiesto di continuare, immettere: `y`

   L'apparecchio si riavvia e la sessione SSH termina. In genere, il programma di installazione dell'appliance StorageGRID richiede circa 5 minuti, anche se in alcuni casi potrebbe essere necessario attendere fino a 30 minuti.

   L'appliance di servizi viene reimpostata e i dati sul nodo Grid non sono più accessibili. Gli indirizzi IP configurati durante il processo di installazione originale devono rimanere intatti; tuttavia, si consiglia di confermarli al termine della procedura.

   Dopo aver eseguito il `sgareinstall` Comando, tutti gli account, le password e le chiavi SSH forniti da StorageGRID vengono rimossi e vengono generate nuove chiavi host.

Avviare l'installazione del software sull'appliance di servizi

Per installare un nodo gateway o un nodo amministrativo su un'appliance di servizi, utilizzare il programma di installazione dell'appliance StorageGRID, incluso nell'appliance.

Prima di iniziare

- L'appliance viene installata in un rack, collegata alla rete e accesa.
- I collegamenti di rete e gli indirizzi IP vengono configurati per l'appliance mediante il programma di installazione dell'appliance StorageGRID.
- Se si installa un nodo gateway o un nodo amministratore non primario, si conosce l'indirizzo IP del nodo amministratore primario per la griglia StorageGRID.
- Tutte le subnet della rete griglia elencate nella pagina di configurazione IP del programma di installazione dell'appliance StorageGRID sono definite nell'elenco delle subnet della rete griglia sul nodo di amministrazione primario.

  Vedere "Avvio rapido per l'installazione dell'hardware".

- Si sta utilizzando un "browser web supportato".
- Uno degli indirizzi IP assegnati al dispositivo. È possibile utilizzare l'indirizzo IP per Admin Network, Grid Network o Client Network.
- Se si installa un nodo amministrativo primario, sono disponibili i file di installazione di Ubuntu o Debian per questa versione di StorageGRID.

Una versione recente del software StorageGRID viene precaricata sull'appliance di servizi durante la produzione. Se la versione precaricata del software corrisponde alla versione utilizzata nella distribuzione di StorageGRID, non sono necessari i file di installazione.

A proposito di questa attività

Per installare il software StorageGRID su un'appliance di servizi:

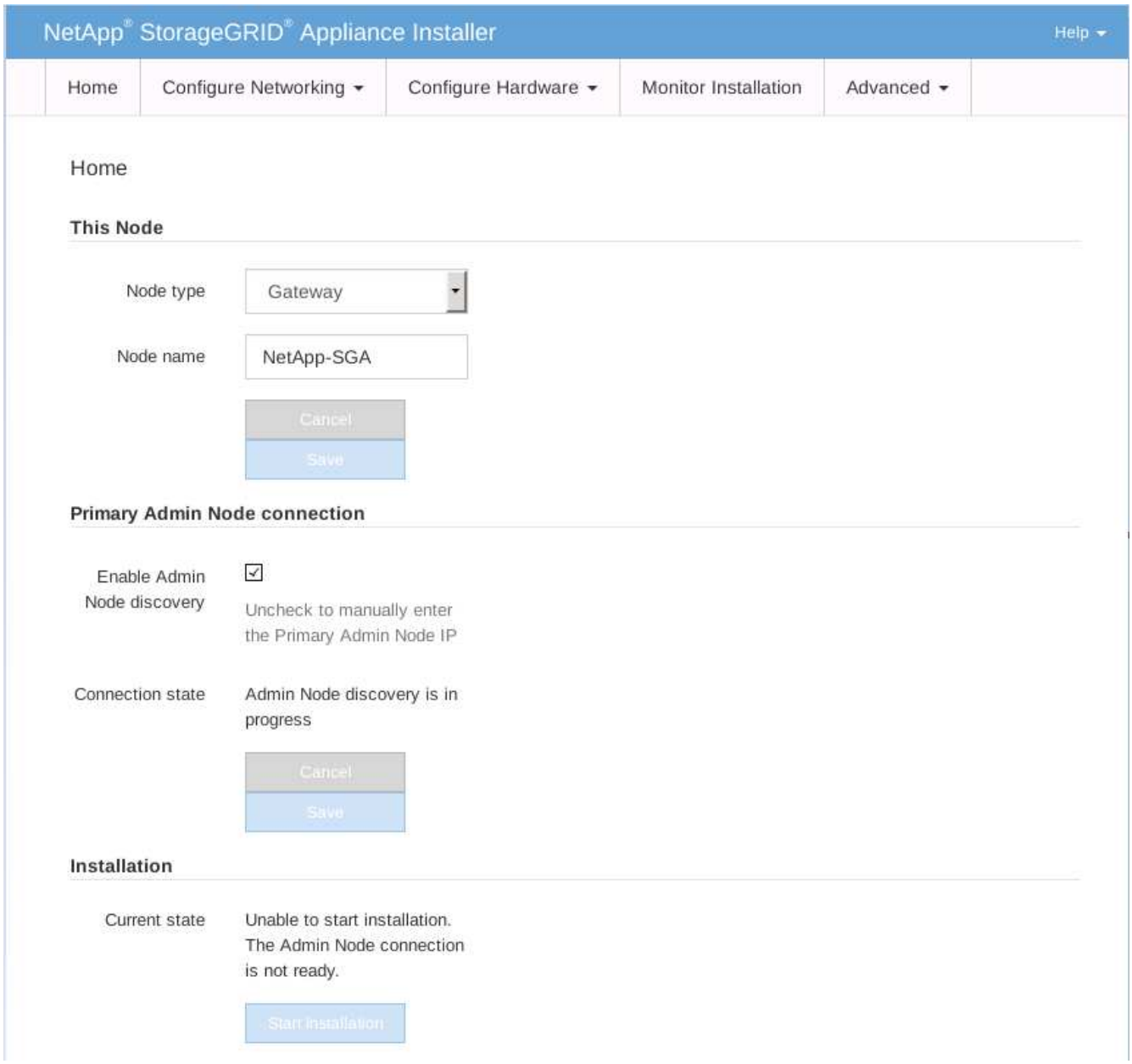
- Per un nodo amministrativo primario, specificare il nome del nodo e caricare i pacchetti software appropriati (se necessario).
- Per un nodo Admin non primario o un nodo gateway, specificare o confermare l'indirizzo IP del nodo Admin primario e il nome del nodo.
- Avviare l'installazione e attendere la configurazione dei volumi e l'installazione del software.
- Durante il processo, l'installazione viene interrotta. Per riprendere l'installazione, è necessario accedere a Grid Manager e configurare il nodo in sospeso come sostituzione del nodo guasto.
- Una volta configurato il nodo, il processo di installazione dell'appliance viene completato e l'appliance viene riavviata.

Fasi

1. Aprire un browser e immettere uno degli indirizzi IP per il dispositivo di servizi.

   `https://Controller_IP:8443`

   Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.



2. Per installare un nodo di amministrazione primario:

   a. Nella sezione questo nodo, per **Node Type**, selezionare **Primary Admin**.

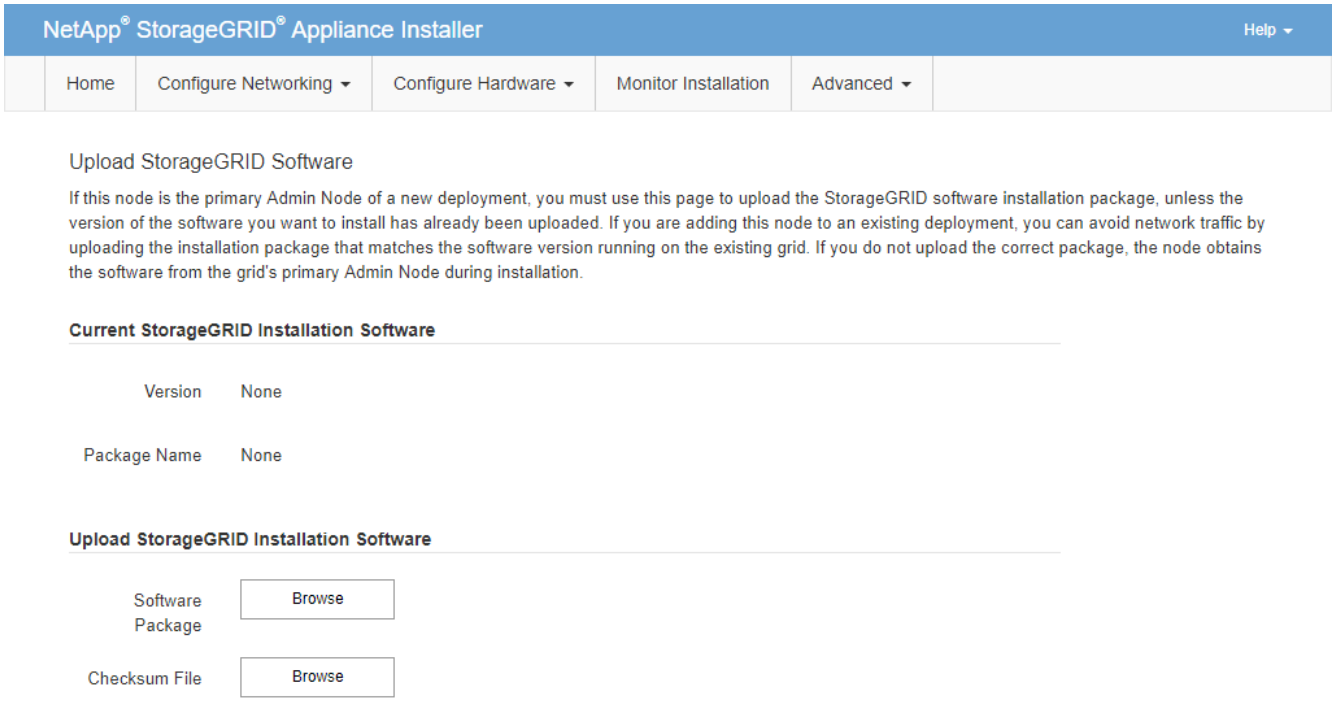
   b. Nel campo **Node Name** (Nome nodo), immettere lo stesso nome utilizzato per il nodo che si sta ripristinando e fare clic su **Save** (Salva).

   c. Nella sezione Installazione, controllare la versione del software elencata sotto Stato corrente

      Se la versione del software pronta per l'installazione è corretta, passare alla Fase di installazione.

   d. Per caricare una versione diversa del software, nel menu **Avanzate**, selezionare **carica software StorageGRID**.

      Viene visualizzata la pagina Caricamento del software StorageGRID.



a. Fare clic su **Browse** (Sfoglia) per caricare i file **pacchetto software** e **checksum file** per il software StorageGRID.

   I file vengono caricati automaticamente dopo averli selezionati.

b. Fare clic su **Home** per tornare alla home page del programma di installazione dell'appliance StorageGRID.

3. Per installare un nodo gateway o un nodo amministratore non primario:

   a. Nella sezione questo nodo, per **Node Type**, selezionare **Gateway** o **non-Primary Admin**, a seconda del tipo di nodo che si sta ripristinando.

   b. Nel campo **Node Name** (Nome nodo), immettere lo stesso nome utilizzato per il nodo che si sta ripristinando e fare clic su **Save** (Salva).

   c. Nella sezione Primary Admin Node Connection (connessione nodo amministratore primario), determinare se è necessario specificare l'indirizzo IP per il nodo amministratore primario.

      Il programma di installazione dell'appliance StorageGRID è in grado di rilevare automaticamente questo indirizzo IP, presupponendo che il nodo amministratore primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente nella stessa sottorete.

   d. Se questo indirizzo IP non viene visualizzato o se è necessario modificarlo, specificare l'indirizzo:

Opzione	Descrizione
Immissione manuale dell'IP	a. Deselezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Inserire l'indirizzo IP manualmente. c. Fare clic su **Save** (Salva). d. Attendere che lo stato della connessione del nuovo indirizzo IP diventi "pronto".

Opzione	Descrizione
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Dall'elenco degli indirizzi IP rilevati, selezionare il nodo di amministrazione principale per la griglia in cui verrà implementata l'appliance di servizi. c. Fare clic su **Save** (Salva). d. Attendere che lo stato della connessione del nuovo indirizzo IP diventi "pronto".

4. nella sezione Installation (Installazione), verificare che lo stato corrente sia Ready to start installation of node name (Pronto per avviare l'installazione del nome del nodo) e che il pulsante **Start Installation** (Avvia installazione) sia attivato.

   Se il pulsante **Avvia installazione** non è attivato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per istruzioni, consultare le istruzioni di manutenzione dell'apparecchio.

5. Dalla home page del programma di installazione dell'appliance StorageGRID, fare clic su **Avvia installazione**.

   Lo stato corrente cambia in "Installazione in corso" e viene visualizzata la pagina Installazione monitor.

   Per accedere manualmente alla pagina Installazione monitor, fare clic su **Installazione monitor** dalla barra dei menu.

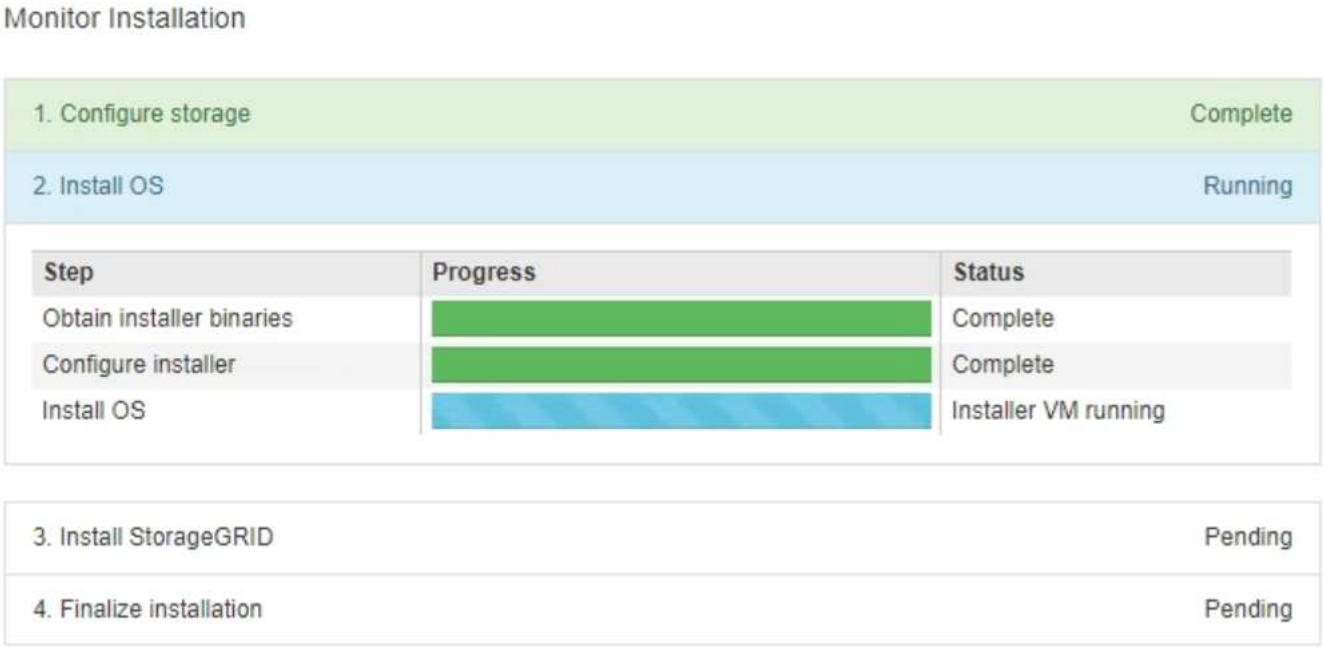
Monitorare l'installazione delle appliance di servizi

Il programma di installazione dell'appliance StorageGRID indica lo stato fino al completamento dell'installazione. Una volta completata l'installazione del software, l'appliance viene riavviata.

Fasi

1. Per monitorare l'avanzamento dell'installazione, fare clic su **Monitor Installation** (Installazione monitor) nella barra dei menu.

   La pagina Monitor Installation (Installazione monitor) mostra lo stato di avanzamento dell'installazione.



La barra di stato blu indica l'attività attualmente in corso. Le barre di stato verdi indicano le attività completate correttamente.

> Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si sta eseguendo nuovamente un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "saltato".

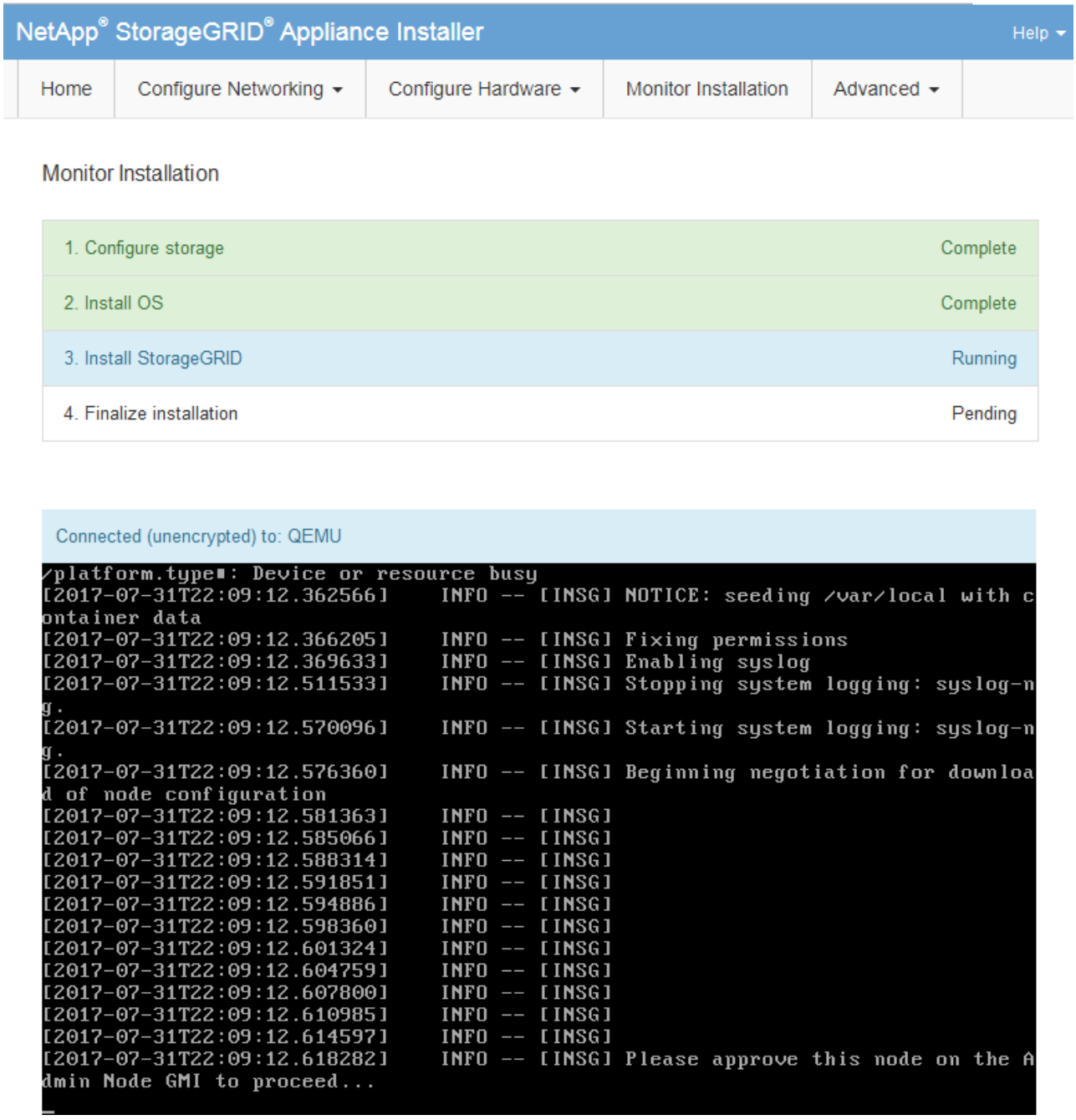
2. Esaminare i progressi delle prime due fasi dell'installazione.
   - **1. Configurare lo storage**

     Durante questa fase, il programma di installazione cancella qualsiasi configurazione esistente dai dischi e configura le impostazioni dell'host.

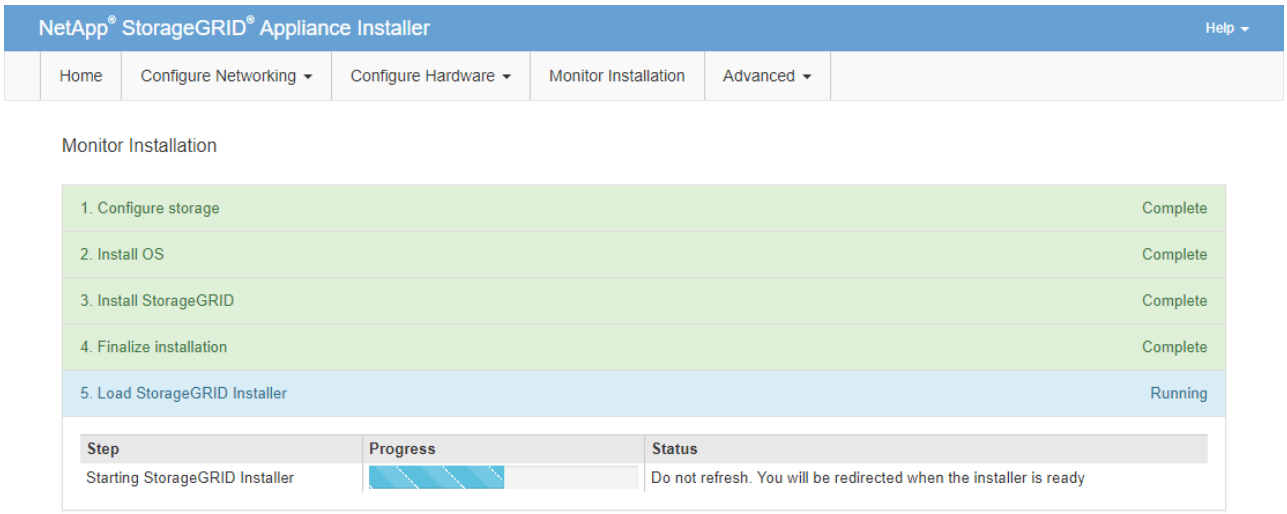
   - **2. Installare il sistema operativo**

     Durante questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID dal nodo di amministrazione primario all'appliance o installa il sistema operativo di base dal pacchetto di installazione per il nodo di amministrazione primario.

3. Continuare a monitorare l'avanzamento dell'installazione fino a quando non si verifica una delle seguenti condizioni:
   - Per i nodi gateway dell'appliance o i nodi di amministrazione dell'appliance non primaria, la fase **Install StorageGRID** (Installazione del nodo) viene sospesa e sulla console integrata viene visualizzato un messaggio che richiede di approvare questo nodo nel nodo di amministrazione utilizzando Gestione griglia.



- Per i nodi di amministrazione primari dell'appliance, viene visualizzata una quinta fase (carica programma di installazione StorageGRID). Se la quinta fase è in corso per più di 10 minuti, aggiornare la pagina manualmente.



4. Passare alla fase successiva del processo di ripristino per il tipo di nodo Grid dell'appliance che si sta ripristinando.

Tipo di ripristino	Riferimento
Nodo gateway	"Selezionare Avvia ripristino per configurare il nodo gateway"
Nodo amministrativo non primario	"Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario"
Nodo amministratore primario	"Configurare il nodo amministrativo primario sostitutivo"

Come il supporto tecnico recupera un sito

In caso di guasto di un intero sito StorageGRID o in caso di guasto di più nodi di storage, è necessario contattare il supporto tecnico. Il supporto tecnico valuterà la tua situazione, svilupperà un piano di recovery e ripristinerà i nodi o il sito guasti in modo da soddisfare gli obiettivi di business, ottimizzare i tempi di recovery e prevenire inutili perdite di dati.

Il ripristino del sito può essere eseguito solo dal supporto tecnico.

I sistemi StorageGRID sono resilienti a una vasta gamma di guasti e puoi eseguire molte procedure di ripristino e manutenzione autonomamente. Tuttavia, è difficile creare una procedura di ripristino del sito semplice e generalizzata, in quanto i passaggi dettagliati dipendono da fattori specifici della situazione. Ad esempio:

- **I tuoi obiettivi di business**: Dopo la perdita completa di un sito StorageGRID, dovresti valutare come soddisfare al meglio i tuoi obiettivi di business. Ad esempio, si desidera ricostruire il sito smarrito sul posto? Sostituire il sito StorageGRID perso in una nuova posizione? La situazione di ogni cliente è diversa e il tuo piano di recovery deve essere progettato per soddisfare le tue priorità.
- **Natura esatta del guasto**: Prima di iniziare un ripristino del sito, stabilire se i nodi del sito guasto sono intatti o se i nodi di storage contengono oggetti ripristinabili. Se si ricostruiscono nodi o volumi di storage che contengono dati validi, potrebbe verificarsi una perdita di dati non necessaria.

- **Criteri ILM attivi**: Il numero, il tipo e la posizione delle copie degli oggetti nella griglia sono controllati dai criteri ILM attivi. Le specifiche dei criteri ILM possono influire sulla quantità di dati ripristinabili e sulle tecniche specifiche necessarie per il ripristino.

  Se un sito contiene l'unica copia di un oggetto e il sito viene perso, l'oggetto viene perso.

- **Coerenza bucket (o contenitore)**: La coerenza applicata a un bucket (o contenitore) influisce sul fatto che StorageGRID replica completamente i metadati degli oggetti in tutti i nodi e siti prima di informare il client del successo dell'acquisizione degli oggetti. Se il valore di coerenza consente un'eventuale coerenza, alcuni metadati degli oggetti potrebbero essere andati persi nel guasto del sito. Ciò può influire sulla quantità di dati ripristinabili e potenzialmente sui dettagli della procedura di ripristino.
- **Cronologia delle modifiche recenti**: I dettagli della procedura di ripristino possono essere influenzati dall'eventuale presenza di procedure di manutenzione in corso al momento dell'errore o dall'eventuale modifica recente delle policy ILM. Prima di iniziare un ripristino del sito, il supporto tecnico deve valutare la cronologia recente del tuo grid e la sua situazione attuale.

Il ripristino del sito può essere eseguito solo dal supporto tecnico.

Di seguito viene fornita una panoramica generale del processo utilizzato dal supporto tecnico per il ripristino di un sito guasto:

1. Assistenza tecnica:
   a. Effettua una valutazione dettagliata del guasto.
   b. Collaborerà per esaminare gli obiettivi aziendali.
   c. Sviluppa un piano di ripristino personalizzato in base alla situazione.
2. Se il nodo amministrativo primario è guasto, il supporto tecnico lo ripristina.
3. Il supporto tecnico recupera tutti i nodi di storage, seguendo questa descrizione:
   a. Sostituire l'hardware o le macchine virtuali del nodo di storage secondo necessità.
   b. Ripristinare i metadati dell'oggetto nel sito guasto.
   c. Ripristinare i dati dell'oggetto nei nodi di storage ripristinati.

   La perdita di dati si verifica se vengono utilizzate le procedure di ripristino per un singolo nodo di storage guasto.

   In caso di guasto di un intero sito, il supporto tecnico utilizza comandi specializzati per ripristinare correttamente gli oggetti e i metadati degli oggetti.
4. Il supporto tecnico recupera altri nodi guasti.

   Una volta ripristinati i metadati e i dati degli oggetti, il supporto tecnico utilizza procedure standard per recuperare nodi Gateway guasti, nodi amministrativi non primari o nodi di archivio.

Informazioni correlate

"Decommissionare il sito"

Come abilitare StorageGRID nel tuo ambiente

Passare a. "Come abilitare StorageGRID nel tuo ambiente" Per scoprire come testare e abilitare le applicazioni nel tuo ambiente StorageGRID.

Il sito di documentazione **storagegrid-enable** fornisce esempi e libri di cucina che ampliano la documentazione del prodotto in questo sito e descrive alcuni passaggi successivi per la valutazione e l'integrazione con StorageGRID.

Alcune delle informazioni incluse:

- Elenco delle soluzioni di terze parti validate per le release StorageGRID precedenti e correnti.
- Guide alle funzionalità del prodotto. Ad esempio, queste guide forniscono tutte le informazioni necessarie per creare pool di storage cloud.
- Guide agli strumenti e alle applicazioni.
- Esempi di API per l'utilizzo di funzionalità StorageGRID come la crittografia S3 e il blocco oggetti S3.

Come gestire StorageGRID utilizzando NetApp Console

Vai a "Gestione StorageGRID tramite la console NetApp" per scoprire come gestire i sistemi StorageGRID dalla console NetApp utilizzando Grid Manager e utilizzare i servizi dati della console NetApp per backup, livelli di dati e altro ancora.

- BlueXP è ora NetApp Console*

NetApp Console, basata sulle fondamenta BlueXP migliorate e ristrutturate, offre una gestione centralizzata dello storage NetApp e dei NetApp Data Services in ambienti on-premise e cloud di livello aziendale, offrendo informazioni in tempo reale, flussi di lavoro più rapidi e un'amministrazione semplificata, il tutto in modo altamente sicuro e conforme.

Per i dettagli su cosa è cambiato, vedere il"Note sulla versione della console NetApp" .

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

https://library.netapp.com/ecm/ecm_download_file/ECMLP2886898

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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