



Documentazione del software StorageGRID 11.9

StorageGRID software

NetApp
December 03, 2025

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid-119/index.html> on December 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Documentazione del software StorageGRID 11.9	1
Dispositivi StorageGRID	2
Note di rilascio	3
Inizia 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 della griglia	11
Come StorageGRID gestisce i dati	23
Esplora StorageGRID	34
Linee guida per il networking	42
Linee guida per il networking	42
Tipi di rete StorageGRID	43
Esempi di topologia di rete	47
Requisiti di rete	54
Requisiti specifici della rete	56
Considerazioni sulla rete specifiche per l'implementazione	58
Installazione e provisioning della rete	61
Linee guida post-installazione	62
Riferimento porta di rete	62
Avvio rapido per StorageGRID	72
Installa, aggiorna e correggi StorageGRID	75
Dispositivi StorageGRID	75
Installa StorageGRID su Red Hat Enterprise Linux	75
Guida rapida all'installazione di StorageGRID su Red Hat Enterprise Linux	75
Pianificare e preparare l'installazione su Red Hat	76
Automatizza l'installazione StorageGRID su Red Hat Enterprise Linux	102
Distribuisci nodi di griglia virtuali (Red Hat)	105
Configurare la griglia e completare l'installazione (Red Hat)	128
Installazione REST API	141
Dove andare dopo	142
Risolvere i problemi di installazione	142
Esempio /etc/sysconfig/network-scripts	143
Installa StorageGRID su Ubuntu o Debian	145
Guida rapida all'installazione di StorageGRID su Ubuntu o Debian	145
Pianificare e preparare l'installazione su Ubuntu o Debian	146
Automatizzare l'installazione (Ubuntu o Debian)	173
Distribuisci nodi di griglia virtuali (Ubuntu o Debian)	175
Configurare la griglia e completare l'installazione (Ubuntu o Debian)	198
Installazione REST API	211
Dove andare dopo	212
Risolvere i problemi di installazione	213

Esempio /etc/network/interfaces	213
Installa StorageGRID su VMware	215
Guida rapida all'installazione di StorageGRID su VMware	215
Pianificare e preparare l'installazione su VMware	216
Automatizzare l'installazione (VMware)	225
Distribuisci nodi di griglia di macchine virtuali (VMware)	239
Configurare la griglia e completare l'installazione (VMware)	248
Installazione REST API	261
Dove andare dopo	262
Risolvere i problemi di installazione	263
Aggiorna il software StorageGRID	264
Aggiorna il software StorageGRID	264
Novità di StorageGRID 11.9	264
Funzionalità e capacità rimosse o deprecate	267
Modifiche all'API di gestione della griglia	269
Modifiche all'API di gestione degli inquilini	270
Pianificare e preparare l'aggiornamento	270
Aggiorna il software	278
Risolvere i problemi di aggiornamento	294
Applica l'hotfix StorageGRID	297
Procedura di hotfix di StorageGRID	297
Come viene influenzato il tuo sistema quando applichi un hotfix	298
Ottieni i materiali necessari per l'hotfix	299
Scarica il file hotfix	299
Controllare le condizioni del sistema prima di applicare l'hotfix	300
Applica hotfix	301
Configurare e gestire un sistema StorageGRID	305
Amministra StorageGRID	305
Amministra StorageGRID	305
Inizia con Grid Manager	305
Controlla l'accesso a StorageGRID	336
Utilizzare la federazione di griglia	384
Gestire la sicurezza	421
Gestire gli inquilini	488
Configurare le connessioni client	508
Gestire reti e connessioni	549
Utilizzare AutoSupport	568
Gestisci nodi di archiviazione	583
Gestisci nodi amministrativi	597
Gestire gli oggetti con ILM	600
Gestire gli oggetti con ILM	600
ILM e ciclo di vita degli oggetti	601
Creare e assegnare gradi di archiviazione	623
Utilizzare pool di archiviazione	626
Utilizzare i pool di archiviazione cloud	634

Gestisci i profili di codifica di cancellazione	654
Configurare le regioni (facoltativo e solo S3)	658
Crea regola ILM	659
Gestire le policy ILM	676
Lavorare con le policy e le regole ILM	692
Utilizzare il blocco oggetto S3	696
Esempio di regole e policy ILM	704
Rafforzamento del sistema	725
Considerazioni generali per il rafforzamento del sistema	725
Linee guida per il rafforzamento degli aggiornamenti software	726
Linee guida per il rafforzamento delle reti StorageGRID	727
Linee guida per il rafforzamento dei nodi StorageGRID	728
Linee guida per il rafforzamento di TLS e SSH	731
Altre linee guida per il rafforzamento	732
Configurare StorageGRID per FabricPool	733
Configurare StorageGRID per FabricPool	733
Informazioni necessarie per collegare StorageGRID come livello cloud	735
Utilizzare la procedura guidata di configurazione FabricPool	736
Configurare StorageGRID manualmente	750
Configurare ONTAP System Manager	760
Configurare il server DNS	762
Le migliori pratiche StorageGRID per FabricPool	763
Rimuovere i dati FabricPool da StorageGRID	767
Utilizzare i tenant e i client StorageGRID	769
Utilizzare un account tenant	769
Utilizzare un account tenant	769
Come accedere e uscire	770
Comprendere la dashboard di Tenant Manager	775
API di gestione degli inquilini	778
Utilizzare connessioni di federazione di rete	783
Gestisci gruppi e utenti	796
Gestisci le chiavi di accesso S3	816
Gestisci i bucket S3	822
Gestire i servizi della piattaforma S3	845
Utilizzare l'API REST S3	878
Versioni e aggiornamenti supportati dall'API REST S3	878
Riferimento rapido: richieste API S3 supportate	881
Testare la configurazione dell'API REST S3	900
Come StorageGRID implementa l'API REST S3	901
Supporto per l'API REST di Amazon S3	916
Operazioni personalizzate StorageGRID	966
Criteri di accesso a bucket e gruppi	987
Operazioni S3 tracciate nei registri di controllo	1014
Utilizzare Swift REST API (fine del ciclo di vita)	1015
Utilizzare Swift REST API	1015

Monitorare e risolvere i problemi di un sistema StorageGRID	1016
Monitorare il sistema StorageGRID	1016
Monitorare un sistema StorageGRID	1016
Visualizza e gestisci la dashboard	1016
Visualizza la pagina Nodi	1019
Informazioni da monitorare regolarmente	1053
Gestisci gli avvisi	1084
Riferimento ai file di registro	1122
Configurare le destinazioni dei messaggi di controllo e dei registri	1142
Utilizzare il monitoraggio SNMP	1156
Raccogli dati StorageGRID aggiuntivi	1167
Risoluzione dei problemi del sistema StorageGRID	1202
Risoluzione dei problemi di un sistema StorageGRID	1202
Risolvere i problemi relativi agli oggetti e all'archiviazione	1209
Risolvere i problemi relativi ai metadati	1238
Risolvere gli errori del certificato	1240
Risolvere i problemi relativi al nodo di amministrazione e all'interfaccia utente	1241
Risolvi i problemi di rete, hardware e piattaforma	1244
Risolvere i problemi di un server syslog esterno	1252
Esaminare i registri di controllo	1255
Messaggi e registri di controllo	1255
Flusso e conservazione dei messaggi di audit	1255
Accedi al file di registro di controllo	1258
Rotazione del file di registro di controllo	1259
Formato del file di registro di controllo	1259
Formato del messaggio di controllo	1272
Messaggi di audit e ciclo di vita degli oggetti	1277
Messaggi di controllo	1284
Espandi una griglia	1336
Tipi di espansione	1336
Pianifica l'espansione StorageGRID	1337
Aggiungere capacità di archiviazione	1337
Aggiungere capacità di metadati	1345
Aggiungi nodi di griglia per aggiungere funzionalità al tuo sistema	1347
Aggiungi un nuovo sito	1347
Raccogli i materiali richiesti	1348
Scarica ed estrai i file di installazione StorageGRID	1349
Verificare l'hardware e la rete	1355
Aggiungere volumi di archiviazione	1355
Aggiungere volumi di archiviazione ai nodi di archiviazione	1355
VMware: aggiungi volumi di archiviazione al nodo di archiviazione	1358
Linux: aggiungi volumi SAN o collegati direttamente al nodo di archiviazione	1359
Aggiungi nodi o siti della griglia	1363
Aggiungi nodi griglia al sito esistente o aggiungi un nuovo sito	1363
Aggiorna le subnet per Grid Network	1363

Distribuisci nuovi nodi della griglia	1365
Eseguire l'espansione	1370
Configurare il sistema espanso	1377
Fasi di configurazione dopo l'espansione	1377
Verificare che il nodo di archiviazione sia attivo	1379
Copia il database del nodo di amministrazione	1379
Copia le metriche di Prometheus	1381
Copia i registri di controllo	1382
Ribilancia i dati codificati tramite cancellazione dopo l'aggiunta di nodi di archiviazione	1384
Risoluzione dei problemi di espansione	1387
Mantenere un sistema StorageGRID	1389
Manutenzione della rete	1389
Prima di iniziare	1389
Procedure di manutenzione per gli elettrodomestici	1389
Scarica il pacchetto di ripristino	1389
Disattivare nodi o siti	1390
Dismettere il nodo o il sito	1390
Nodi dismessi	1390
Sito di dismissione	1409
Rinomina griglia, sito o nodo	1432
Utilizzare la procedura di rinomina	1432
Aggiungere o aggiornare i nomi visualizzati	1436
Procedure del nodo	1442
Procedure di manutenzione dei nodi	1442
Procedure del Server Manager	1443
Procedure di riavvio, spegnimento e accensione	1452
Procedure di rimappatura delle porte	1464
Procedure di rete	1468
Aggiorna le subnet per Grid Network	1468
Configurare gli indirizzi IP	1470
Aggiungi interfacce al nodo esistente	1487
Configurare i server DNS	1491
Modifica la configurazione DNS per un singolo nodo della griglia	1492
Gestire i server NTP	1494
Ripristinare la connettività di rete per i nodi isolati	1495
Procedure host e middleware	1497
Linux: Migrazione del nodo della griglia al nuovo host	1497
VMware: configurare la macchina virtuale per il riavvio automatico	1499
Recuperare o sostituire i nodi	1500
Avvertenze e considerazioni per il ripristino del nodo della griglia	1500
Prerequisiti per il recupero dei nodi della griglia	1500
Ordine di ripristino del nodo se un server che ospita più di un nodo della griglia fallisce	1501
Indirizzi IP per i nodi recuperati	1501
Raccogliere i materiali necessari per il recupero del nodo della griglia	1501
Scarica ed estrai i file di installazione StorageGRID	1502

Selezionare la procedura di ripristino del nodo	1508
Ripristino da guasti del nodo di archiviazione	1509
Ripristino da guasti del nodo di archiviazione	1509
Ripristina il nodo di archiviazione dell'appliance	1510
Ripristinare da un errore del volume di archiviazione in cui l'unità di sistema è intatta	1532
Ripristino da un errore dell'unità di sistema	1547
Ripristina i dati degli oggetti utilizzando Grid Manager	1565
Monitorare i lavori di riparazione dei dati	1568
Ripristino da errori del nodo di amministrazione	1570
Ripristino del nodo di amministrazione primario o non primario	1570
Ripristino da errori del nodo di amministrazione primario	1570
Ripristino da errori del nodo di amministrazione non primario	1579
Ripristino da guasti del nodo gateway	1587
Sostituisci nodo gateway	1587
Selezionare Avvia ripristino per configurare il nodo gateway	1588
Ripristino da errori del nodo di archivio	1589
Ripristino da errori del nodo di archivio	1589
Sostituisci nodo Linux	1589
Sostituisci nodo Linux	1589
Distribuisci nuovi host Linux	1590
Ripristina i nodi della griglia sull'host	1591
Prossimi passi: eseguire ulteriori passaggi di ripristino, se necessario	1595
Sostituisci nodo VMware	1597
Sostituisci il nodo non riuscito con l'appliance dei servizi	1598
Sostituisci il nodo non riuscito con l'appliance dei servizi	1598
Installa l'appliance dei servizi (solo cambio piattaforma)	1598
Preparare l'apparecchio per la reinstallazione (solo sostituzione della piattaforma)	1599
Avvia l'installazione del software sull'appliance dei servizi	1599
Installazione di apparecchiature di monitoraggio dei servizi	1603
Come il supporto tecnico recupera un sito	1606
Come abilitare StorageGRID nel tuo ambiente	1608
Come gestire StorageGRID utilizzando NetApp Console	1609
Note legali	1610
Copyright	1610
Marchi	1610
Brevetti	1610
Politica sulla riservatezza	1610
Open source	1610

Documentazione del software StorageGRID 11.9

Dispositivi StorageGRID

Vai a "[Documentazione dell'appliance StorageGRID](#)" per imparare come installare, configurare e gestire gli appliance di archiviazione e servizi StorageGRID .

Note di rilascio

Ottieni informazioni specifiche sulla versione, sui problemi risolti e sui problemi noti.

Accedi al sito di supporto NetApp per ["visualizza o scarica un file PDF"](#) contenente le note di rilascio StorageGRID 11.9.

Inizia con un sistema StorageGRID

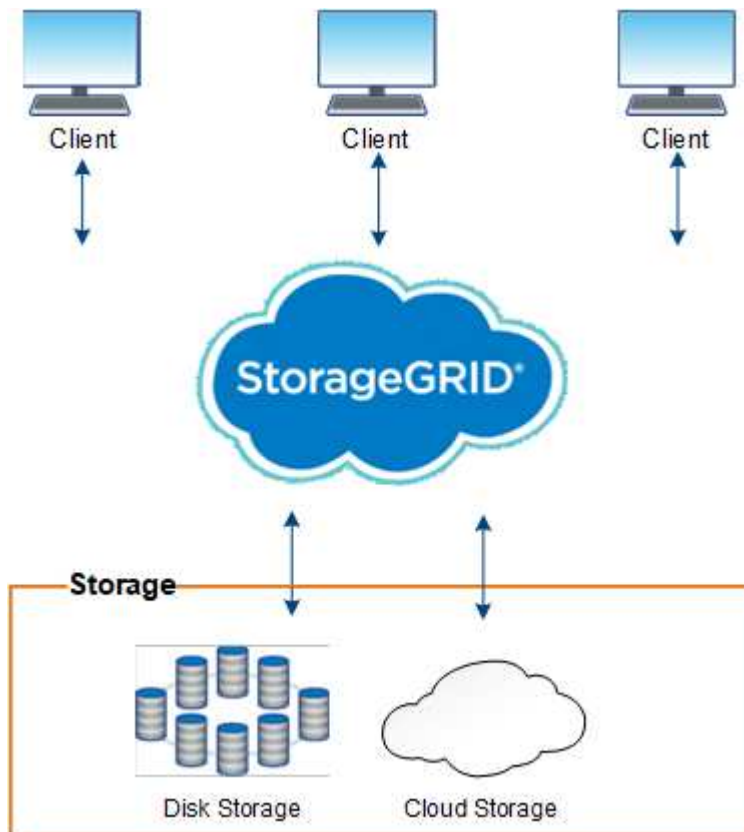
Scopri di più su StorageGRID

Che cos'è StorageGRID?

NetApp® StorageGRID® è una suite di storage di oggetti definiti dal software che supporta un'ampia gamma di casi d'uso in ambienti multicloud pubblici, privati e ibridi. StorageGRID offre supporto nativo per l'API Amazon S3 e offre innovazioni all'avanguardia nel settore, come la gestione automatizzata del ciclo di vita, per archiviare, proteggere, preservare e conservare dati non strutturati in modo conveniente per lunghi periodi.

StorageGRID fornisce un archivio sicuro e durevole per dati non strutturati su larga scala. Le policy di gestione del ciclo di vita integrate e basate sui metadati ottimizzano la posizione dei dati durante tutto il loro ciclo di vita. I contenuti vengono posizionati nel posto giusto, al momento giusto e nel livello di archiviazione giusto per ridurre i costi.

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



Il supporto per i nodi di archivio è stato rimosso. Lo spostamento di oggetti da un nodo di archivio a un sistema di archiviazione esterno tramite l'API S3 è stato sostituito da ["Pool di archiviazione cloud ILM"](#), che offrono maggiori funzionalità.

Vantaggi di StorageGRID

I vantaggi del sistema StorageGRID includono quanto segue:

- Un repository di dati distribuiti geograficamente, altamente scalabile e facile da usare, per dati non strutturati.
- Protocolli standard di archiviazione degli oggetti:
 - Servizio di archiviazione semplice di Amazon Web Services (S3)
 - OpenStack Swift



Il supporto per le applicazioni client Swift è stato deprecato e verrà rimosso in una versione futura.

- Abilitato per cloud ibrido. La gestione del ciclo di vita delle informazioni (ILM) basata su policy archivia gli oggetti nei cloud pubblici, tra cui Amazon Web Services (AWS) e Microsoft Azure. I servizi della piattaforma StorageGRID consentono la replicazione dei contenuti, la notifica degli eventi e la ricerca dei metadati degli oggetti archiviati nei cloud pubblici.
- Protezione flessibile dei dati per garantire durabilità e disponibilità. I dati possono essere protetti mediante replicazione e codifica di cancellazione a strati. La verifica dei dati a riposo e in volo garantisce l'integrità per la conservazione a lungo termine.
- Gestione dinamica del ciclo di vita dei dati per aiutare a gestire i costi di archiviazione. È possibile creare regole ILM che gestiscono il ciclo di vita dei dati a livello di oggetto, personalizzando la località, la durabilità, le prestazioni, i costi e il tempo di conservazione dei dati.
- Elevata disponibilità di archiviazione dati e alcune funzioni di gestione, con bilanciamento del carico integrato per ottimizzare il carico dati tra le risorse StorageGRID .
- Supporto per più account tenant di archiviazione per separare gli oggetti archiviati sul sistema da entità diverse.
- Numerosi strumenti per monitorare lo stato del sistema StorageGRID , tra cui un sistema di avvisi completo, una dashboard grafica e stati dettagliati per tutti i nodi e i siti.
- Supporto per la distribuzione basata su software o hardware. È possibile distribuire StorageGRID su uno qualsiasi dei seguenti dispositivi:
 - Macchine virtuali in esecuzione in VMware.
 - Motori di container su host Linux.
 - Apparecchiature progettate da StorageGRID .
 - Gli apparecchi di archiviazione forniscono archiviazione di oggetti.
 - Gli apparecchi di servizio forniscono servizi di amministrazione della rete e di bilanciamento del carico.
- Conforme ai requisiti di conservazione pertinenti di queste normative:
 - Securities and Exchange Commission (SEC) nel 17 CFR § 240.17a-4(f), che regola i membri della borsa, i broker o i dealer.
 - Regola 4511(c) della Financial Industry Regulatory Authority (FINRA), che rimanda ai requisiti di formato e media della Regola 17a-4(f) della SEC.
 - Commodity Futures Trading Commission (CFTC) nel regolamento 17 CFR § 1.31(c)-(d), che regola il commercio di future sulle materie prime.
- Operazioni di aggiornamento e manutenzione senza interruzioni. Mantenere l'accesso ai contenuti durante

le procedure di aggiornamento, espansione, dismissione e manutenzione.

- Gestione federata delle identità. Si integra con Active Directory, OpenLDAP o Oracle Directory Service per l'autenticazione degli utenti. Supporta l'accesso Single Sign-On (SSO) tramite lo standard Security Assertion Markup Language 2.0 (SAML 2.0) per lo scambio di dati di autenticazione e autorizzazione tra StorageGRID e Active Directory Federation Services (AD FS).

Cloud ibridi con StorageGRID

Utilizza StorageGRID in una configurazione cloud ibrida implementando la gestione dei dati basata su policy per archiviare oggetti in Cloud Storage Pool, sfruttando i servizi della piattaforma StorageGRID e suddividendo i dati da ONTAP a StorageGRID con NetApp FabricPool.

Pool di archiviazione cloud

I pool di archiviazione cloud consentono di archiviare oggetti al di fuori del sistema StorageGRID. Ad esempio, potresti voler spostare gli oggetti a cui si accede raramente su un archivio cloud più economico, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o il livello di accesso Archive nell'archivio BLOB di Microsoft Azure. In alternativa, potresti voler mantenere un backup cloud degli oggetti StorageGRID, che può essere utilizzato per recuperare i dati persi a causa di un errore del volume di archiviazione o del nodo di archiviazione.

È supportato anche lo storage di partner terzi, inclusi storage su disco e nastro.



L'utilizzo di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva necessaria per recuperare un oggetto dalla destinazione di Cloud Storage Pool.

Servizi della piattaforma S3

I servizi della piattaforma S3 offrono la possibilità di utilizzare servizi remoti come endpoint per la replicazione 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 singoli bucket S3. Sono supportati i seguenti servizi:

- Il servizio di replica CloudMirror esegue automaticamente il mirroring degli oggetti specificati su un bucket S3 di destinazione, che può trovarsi su Amazon S3 o su un secondo sistema StorageGRID.
- Il servizio di notifica eventi invia messaggi sulle azioni specificate 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 Elasticsearch esterno, consentendo la ricerca, la visualizzazione e l'analisi dei metadati tramite strumenti di terze parti.

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

Livelli di dati ONTAP tramite FabricPool

È possibile ridurre i costi di archiviazione ONTAP suddividendo i dati in livelli su StorageGRID tramite FabricPool. FabricPool consente il tiering automatico dei dati su livelli di archiviazione di oggetti a basso costo, sia in sede che fuori sede.

A differenza delle soluzioni di suddivisione in livelli manuale, FabricPool riduce il costo totale di proprietà automatizzando la suddivisione in livelli dei dati per abbassare i costi di archiviazione. Offre i vantaggi

dell'economia del cloud tramite la suddivisione in livelli tra cloud pubblici e privati, tra cui StorageGRID.

Informazioni correlate

- ["Che cos'è 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 di griglia in uno o più siti di data center.

Vedi il ["descrizioni dei tipi di nodi della griglia"](#) .

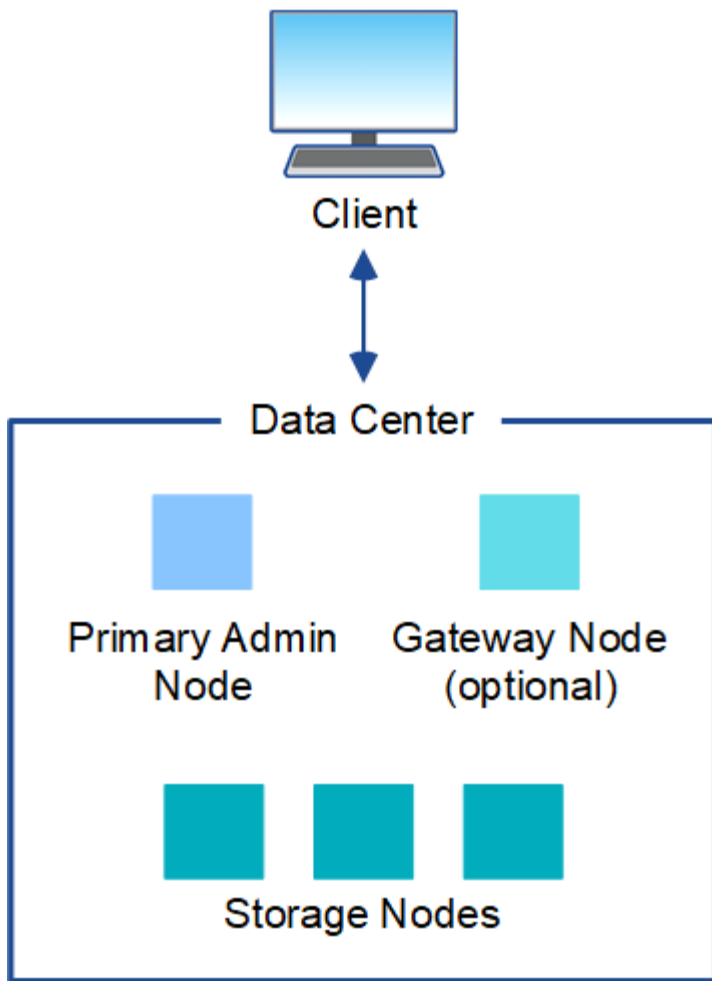
Per ulteriori informazioni sulla topologia di rete StorageGRID , sui requisiti e sulle comunicazioni di rete, vedere ["Linee guida per il networking"](#) .

Topologie di distribuzione

Il sistema StorageGRID può essere distribuito in un singolo sito di data center o in più siti di data center.

Sito singolo

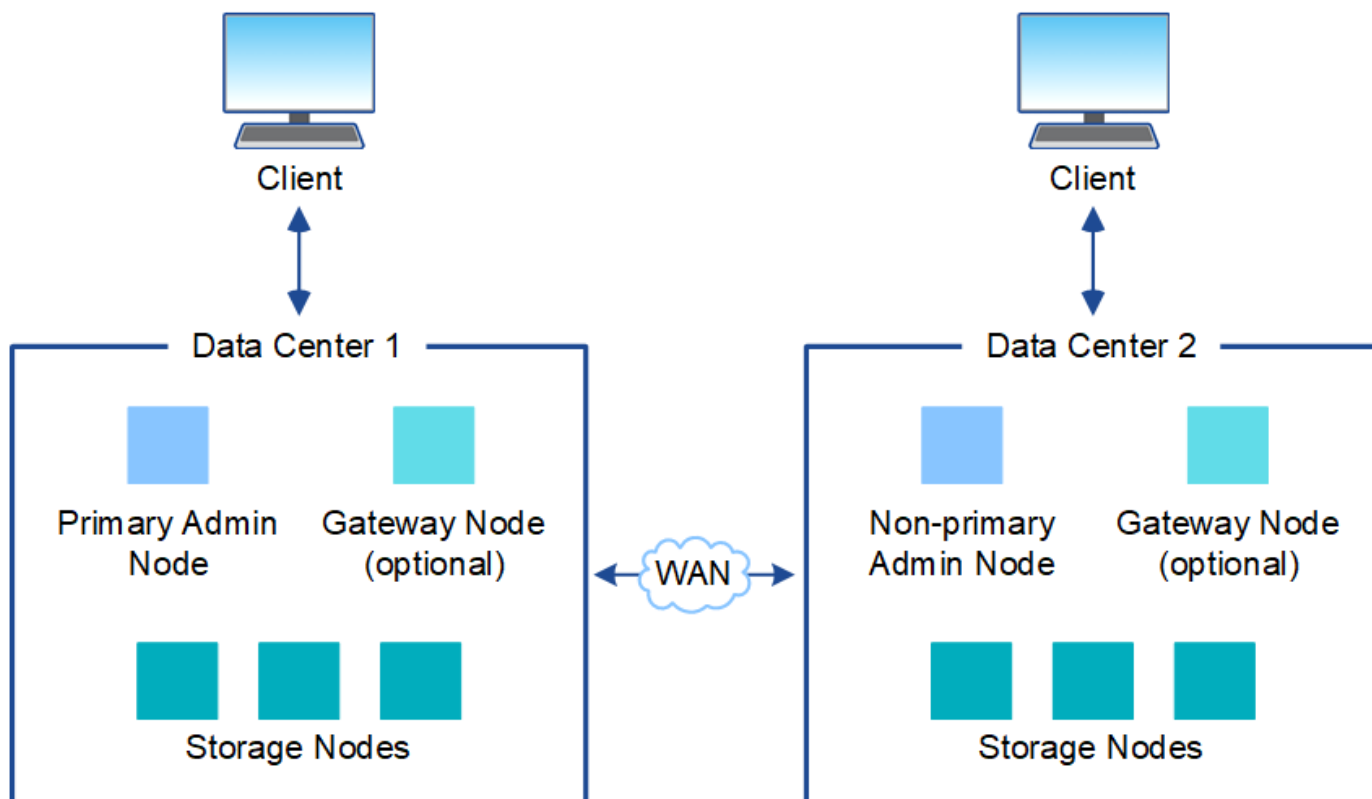
In una distribuzione con un singolo sito, l'infrastruttura e le operazioni del sistema StorageGRID sono centralizzate.



Siti multipli

In una distribuzione con più siti, è possibile installare in ciascun sito diversi tipi e numeri di risorse StorageGRID. Ad esempio, potrebbe essere necessario più spazio di archiviazione in un data center rispetto a un altro.

Spesso siti diversi si trovano in posizioni geografiche diverse, in domini di guasto diversi, come una faglia sismica o una pianura alluvionale. La condivisione dei dati e il ripristino in caso di disastro vengono ottenuti mediante la distribuzione automatizzata dei dati ad altri siti.



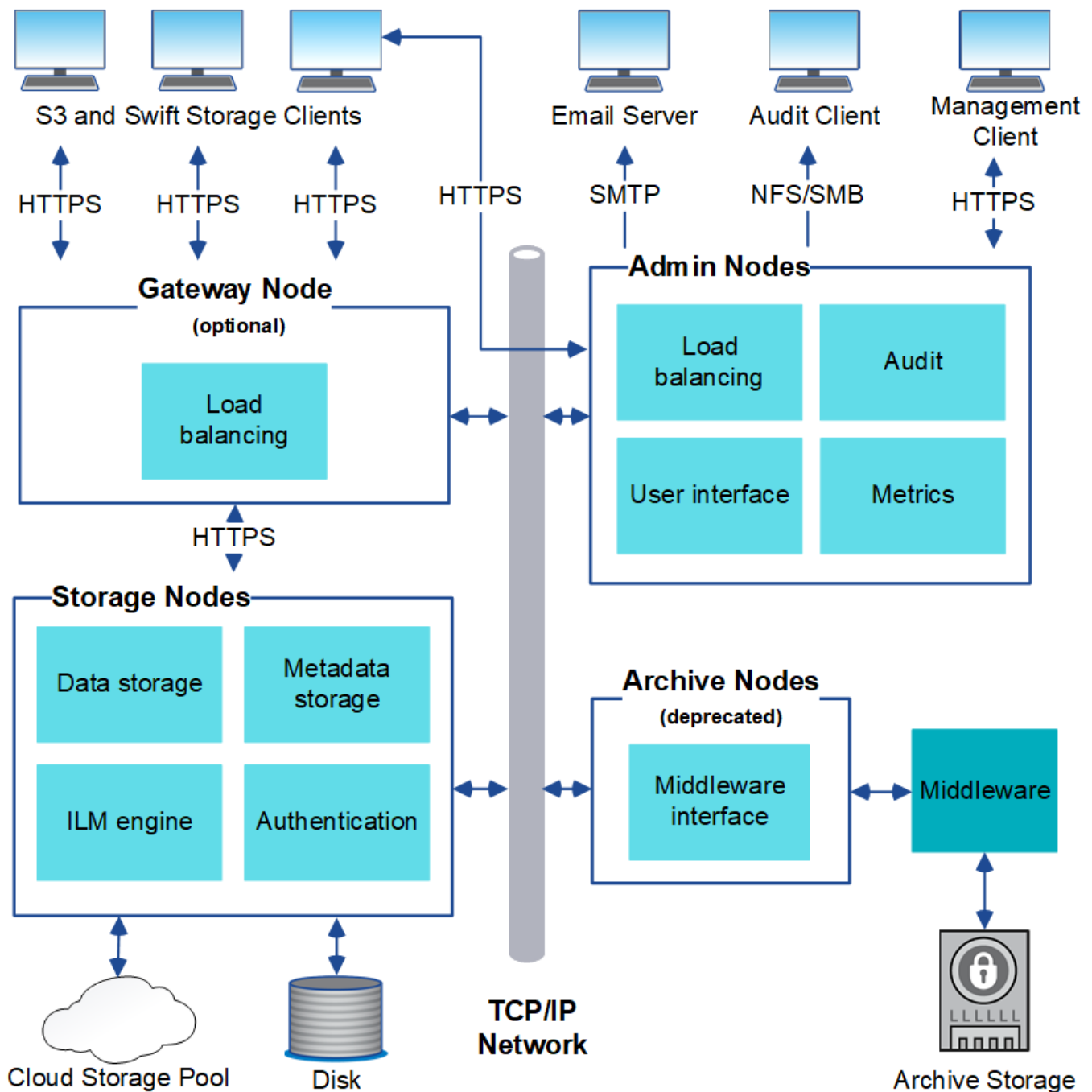
All'interno di un singolo data center possono esistere anche più siti logici per consentire l'uso della replica distribuita e della codifica di cancellazione per aumentare la disponibilità e la resilienza.

Ridondanza dei nodi della griglia

In una distribuzione a sito singolo o multi-sito, è possibile includere facoltativamente più di un nodo di amministrazione o nodo gateway per ridondanza. Ad esempio, è possibile installare più di un nodo di amministrazione in un singolo sito o in più siti. Tuttavia, ogni sistema StorageGRID può avere un solo nodo amministrativo primario.

Architettura del sistema

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



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

I client S3 possono connettersi a un nodo gateway o a un nodo di amministrazione per utilizzare l'interfaccia di bilanciamento del carico per i nodi di archiviazione. In alternativa, i client S3 possono connettersi direttamente ai nodi di archiviazione tramite HTTPS.

Gli oggetti possono essere archiviati in StorageGRID su nodi di archiviazione basati su software o hardware oppure in pool di archiviazione cloud, costituiti da bucket S3 esterni o contenitori di archiviazione BLOB di Azure.

Nodi e servizi della griglia

Nodi e servizi della griglia

L'elemento costitutivo di base di un sistema StorageGRID è il nodo griglia. I nodi contengono servizi, ovvero moduli software che forniscono un insieme di funzionalità a un nodo della griglia.

Tipi di nodi della griglia

Il sistema StorageGRID utilizza quattro tipi di nodi di griglia:

Nodi amministrativi

Fornire servizi di gestione quali configurazione del sistema, monitoraggio e registrazione. Quando accedi a Grid Manager, ti connetti a un nodo di amministrazione. Ogni griglia deve avere un nodo amministrativo primario e potrebbe avere nodi amministrativi non primari aggiuntivi per ridondanza. È possibile connettersi a qualsiasi nodo di amministrazione e ogni nodo di amministrazione visualizza una vista simile del sistema StorageGRID. Tuttavia, le procedure di manutenzione devono essere eseguite utilizzando il nodo di amministrazione primario.

I nodi amministrativi possono essere utilizzati anche per bilanciare il carico del traffico client S3.

Vedere ["Che cos'è un nodo amministrativo?"](#)

Nodi di archiviazione

Gestire e archiviare dati e metadati degli oggetti. Ogni sito nel sistema StorageGRID deve avere almeno tre nodi di archiviazione.

Vedere ["Che cos'è un nodo di archiviazione?"](#)

Nodi gateway (facoltativo)

Fornire un'interfaccia di bilanciamento del carico che le applicazioni client possono utilizzare per connettersi a StorageGRID. Un bilanciatore del carico indirizza senza soluzione di continuità i client verso un nodo di archiviazione ottimale, in modo che il guasto dei nodi o persino di un intero sito sia trasparente.

Vedere ["Che cos'è un nodo gateway?"](#)

Nodi hardware e software

I nodi StorageGRID possono essere distribuiti come nodi di appliance StorageGRID o come nodi basati su software.

Nodi dell'appliance StorageGRID

Gli apparecchi hardware StorageGRID sono progettati specificamente per l'uso in un sistema StorageGRID. Alcuni dispositivi possono essere utilizzati come nodi di archiviazione. Altri dispositivi possono essere utilizzati come nodi amministrativi o nodi gateway. È possibile combinare nodi appliance con nodi basati su software oppure distribuire griglie completamente progettate e composte da tutte le appliance, che non dipendono da hypervisor esterni, storage o hardware di elaborazione.

Per conoscere gli elettrodomestici disponibili, vedere quanto segue:

- ["Documentazione dell'appliance StorageGRID"](#)

- ["Hardware Universe NetApp"](#)

Nodi basati su software

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

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

Utilizzare il ["Strumento matrice di interoperabilità NetApp \(IMT\)"](#) per determinare le versioni supportate.

Durante l'installazione iniziale di un nuovo nodo di archiviazione basato su software è possibile specificare che venga utilizzato solo per ["memorizzare i metadati"](#) .

Servizi StorageGRID

Di seguito è riportato un elenco completo dei servizi StorageGRID .

Servizio	Descrizione	Posizione
Spedizioniere di servizi di account	Fornisce un'interfaccia per il servizio Load Balancer per interrogare il servizio account sugli host remoti e fornisce notifiche delle modifiche alla configurazione dell'endpoint Load Balancer al servizio Load Balancer.	Servizio di bilanciamento del carico sui nodi amministrativi e sui nodi gateway
ADC (Administrative Domain Controller)	Gestisce le informazioni sulla topologia, fornisce servizi di autenticazione e risponde alle query dei servizi LDR e CMN.	Almeno tre nodi di archiviazione contenenti il servizio ADC in ogni sito
AMS (Sistema di gestione degli audit)	Monitora e registra tutti gli eventi e le transazioni di sistema controllati in un file di registro di testo.	Nodi amministrativi
Cassandra Reaper	Esegue riparazioni automatiche dei metadati degli oggetti.	Nodi di archiviazione
Servizio Chunk	Gestisce i dati codificati in modo cancellabile e i frammenti di parità.	Nodi di archiviazione
CMN (Nodo di gestione della configurazione)	Gestisce le configurazioni a livello di sistema e le attività della griglia. Ogni griglia ha un servizio CMN.	Nodo di amministrazione primario
DDS (archivio dati distribuito)	Si interfaccia con il database Cassandra per gestire i metadati degli oggetti.	Nodi di archiviazione

Servizio	Descrizione	Posizione
DMV (Data Mover)	Sposta i dati verso gli endpoint cloud.	Nodi di archiviazione
IP dinamico (dynip)	Monitora la griglia per rilevare modifiche IP dinamiche e aggiorna le configurazioni locali.	Tutti i nodi
Grafana	Utilizzato per la visualizzazione delle metriche in Grid Manager.	Nodi amministrativi
Alta disponibilità	Gestisce gli IP virtuali ad alta disponibilità sui nodi configurati nella pagina Gruppi ad alta disponibilità. Questo servizio è noto anche come servizio keepalived.	Nodi di amministrazione e gateway
Identità (idnt)	Federa le identità utente da LDAP e Active Directory.	Nodi di archiviazione che utilizzano il servizio ADC
Arbitro Lambda	Gestisce le richieste S3 Select SelectObjectContent.	Tutti i nodi
Bilanciatore del carico (nginx-gw)	Fornisce il bilanciamento del carico del traffico S3 dai client ai nodi di archiviazione. Il servizio Load Balancer può essere configurato tramite la pagina di configurazione degli endpoint del Load Balancer. Questo servizio è noto anche come servizio nginx-gw.	Nodi di amministrazione e gateway
LDR (Router di distribuzione locale)	Gestisce l'archiviazione e il trasferimento dei contenuti all'interno della griglia.	Nodi di archiviazione
MISCd Information Service Control Daemon	Fornisce un'interfaccia per interrogare e gestire i servizi su altri nodi e per gestire le configurazioni ambientali sul nodo, ad esempio interrogando lo stato dei servizi in esecuzione su altri nodi.	Tutti i nodi
nginx	Funziona come meccanismo di autenticazione e comunicazione sicura per vari servizi di griglia (come Prometheus e Dynamic IP) per poter comunicare con i servizi su altri nodi tramite API HTTPS.	Tutti i nodi
nginx-gw	Alimenta il servizio Load Balancer.	Nodi di amministrazione e gateway
NMS (Sistema di gestione della rete)	Alimenta le opzioni di monitoraggio, reporting e configurazione visualizzate tramite Grid Manager.	Nodi amministrativi

Servizio	Descrizione	Posizione
Persistenza	Gestisce i file sul disco radice che devono rimanere memorizzati anche dopo un riavvio.	Tutti i nodi
Prometeo	Raccoglie metriche di serie temporali dai servizi su tutti i nodi.	Nodi amministrativi
RSM (macchina a stati replicati)	Assicura che le richieste di servizio della piattaforma vengano inviate ai rispettivi endpoint.	Nodi di archiviazione che utilizzano il servizio ADC
SSM (monitoraggio dello stato del server)	Monitora le condizioni dell'hardware e invia segnalazioni al servizio NMS.	Un'istanza è presente su ogni nodo della griglia
Collettore di tracce	Esegue la raccolta di tracce per raccogliere informazioni da utilizzare da parte del supporto tecnico. Il servizio di raccolta delle tracce utilizza il software open source Jaeger.	Nodi amministrativi

Che cos'è un nodo amministrativo?

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

Differenze tra nodi amministrativi primari e non primari

Quando accedi a Grid Manager o a Tenant Manager, ti stai connettendo a un nodo di amministrazione. È possibile connettersi a qualsiasi nodo di amministrazione e ogni nodo di amministrazione visualizza una vista simile del sistema StorageGRID. Tuttavia, il nodo amministrativo primario offre 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.

Capacità	Nodo di amministrazione primario	Nodo amministratore non primario
Include il AMS servizio	Sì	Sì
Include il CMN servizio	Sì	NO
Include il NMS servizio	Sì	Sì
Include il Prometeo servizio	Sì	Sì

Capacità	Nodo di amministrazione primario	Nodo amministratore non primario
Include ilSSM servizio	Sì	Sì
Include ilBilanciatore del carico EAlta disponibilità servizi	Sì	Sì
Supporta illInterfaccia di programmazione dell'applicazione di gestione (mgmt-api)	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 di archiviazione	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 ilmittente preferito .	Sì. Funziona come mittente in standby.

Mittente preferito Nodo amministratore

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 informazioni SNMP.

Durante il normale funzionamento del sistema, solo il mittente preferito invia le notifiche. Tuttavia, tutti gli altri nodi amministrativi monitorano il mittente preferito. Se viene rilevato un problema, altri nodi amministrativi agiscono come *mittenti in standby*.

Nei seguenti casi potrebbero essere inviate più notifiche:

- Se i nodi di amministrazione diventano "isolati" 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 tal caso, potrebbero essere inviate notifiche duplicate. Il mittente in standby interromperà l'invio di notifiche quando non rileverà più errori sul mittente preferito.



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

Servizi primari per i nodi amministrativi

Nella tabella seguente sono riportati i servizi principali per i nodi di amministrazione; tuttavia, questa tabella non elenca tutti i servizi del nodo.

Servizio	Funzione chiave
Sistema di gestione degli audit (AMS)	Tiene traccia dell'attività e degli eventi del sistema.
Nodo di gestione della configurazione (CMN)	Gestisce la configurazione dell'intero sistema.
[[alta disponibilità]]Alta disponibilità	Gestisce indirizzi IP virtuali ad alta disponibilità per gruppi di nodi amministrativi e nodi gateway. Nota: questo servizio è disponibile anche sui Gateway Nodes.
[[bilanciamento del carico]]Bilanciamento del carico	Fornisce il bilanciamento del carico del traffico S3 dai client ai nodi di archiviazione. Nota: questo servizio è disponibile anche sui Gateway Nodes.
Interfaccia di programmazione dell'applicazione di gestione (mgmt-api)	Elabora le richieste provenienti dall'API di gestione della griglia e dall'API di gestione degli inquilini.
Sistema di gestione della rete (NMS)	Fornisce funzionalità per Grid Manager.
Prometeo	Raccoglie e memorizza le metriche delle serie temporali dai servizi su tutti i nodi.
Monitoraggio dello stato del server (SSM)	Monitora il sistema operativo e l'hardware sottostante.

Che cos'è un nodo di archiviazione?

I nodi di archiviazione gestiscono e archiviano dati e metadati degli oggetti. I nodi di archiviazione includono i servizi e i processi necessari per archiviare, spostare, verificare e recuperare dati e metadati degli oggetti su disco.

Ogni sito nel sistema StorageGRID deve avere almeno tre nodi di archiviazione.

Tipi di nodi di archiviazione

Durante l'installazione, è possibile selezionare il tipo di nodo di archiviazione che si desidera installare. Questi tipi sono disponibili per i nodi di archiviazione basati su software e per i nodi di archiviazione basati su appliance che supportano la funzionalità:

- Nodo di archiviazione di dati e metadati combinati
- Nodo di archiviazione solo metadati
- Nodo di archiviazione solo dati

È possibile selezionare il tipo di nodo di archiviazione nelle seguenti situazioni:

- Quando si installa inizialmente un nodo di archiviazione
- Quando si aggiunge un nodo di archiviazione durante l'espansione del sistema StorageGRID



Non è possibile modificare il tipo una volta completata l'installazione del nodo di archiviazione.

Nodo di archiviazione dati e metadati (combinato)

Per impostazione predefinita, tutti i nuovi nodi di archiviazione memorizzeranno sia i dati degli oggetti che i metadati. Questo tipo di nodo di archiviazione è chiamato nodo di archiviazione *combinato*.

Nodo di archiviazione solo metadati

Utilizzare un nodo di archiviazione esclusivamente per i metadati può avere senso se la griglia memorizza un numero molto elevato di piccoli oggetti. L'installazione di una capacità dedicata per i metadati garantisce un migliore equilibrio tra lo spazio necessario per un numero molto elevato di piccoli oggetti e lo spazio necessario per i metadati di tali oggetti. Inoltre, i nodi di archiviazione basati solo su metadati ospitati su appliance ad alte prestazioni possono aumentare le prestazioni.

I nodi di archiviazione solo metadati hanno requisiti hardware specifici:

- Quando si utilizzano appliance StorageGRID, i nodi solo metadati possono essere configurati solo su appliance SGF6112 con dodici unità da 1,9 TB o dodici unità da 3,8 TB.
- Quando si utilizzano nodi basati su software, le risorse dei nodi solo metadati devono corrispondere alle risorse dei nodi di archiviazione esistenti. Per esempio:
 - Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo su software devono soddisfare i seguenti requisiti minimi:
 - 128 GB di RAM
 - CPU a 8 core
 - SSD da 8 TB o spazio di archiviazione equivalente per il database Cassandra (rangedb/0)
 - Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuali con 24 GB di RAM, CPU a 8 core e 3 TB o 4 TB di spazio di archiviazione dei metadati, i nodi basati solo su software devono utilizzare risorse simili (24 GB di RAM, CPU a 8 core e 4 TB di spazio di archiviazione dei metadati (rangedb/0).
- Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve corrispondere almeno ai siti StorageGRID esistenti e le risorse del nuovo sito devono corrispondere ai nodi di archiviazione nei siti StorageGRID esistenti.

Quando si installano nodi solo metadati, la griglia deve contenere anche un numero minimo di nodi per l'archiviazione dei dati:

- Per una griglia a sito singolo, configurare almeno due nodi di archiviazione combinati o solo dati.
- Per una griglia multi-sito, configurare almeno un nodo di archiviazione combinato o solo dati *per sito*.



Sebbene i nodi di archiviazione solo metadati contengano [Servizio LDR](#) e può elaborare le richieste del client S3, le prestazioni StorageGRID potrebbero non aumentare.

Nodo di archiviazione solo dati

Utilizzare un nodo di archiviazione esclusivamente per i dati può avere senso se i nodi di archiviazione hanno caratteristiche prestazionali diverse. Ad esempio, per aumentare potenzialmente le prestazioni, è possibile disporre di nodi di archiviazione con dischi rotanti ad alta capacità e solo dati, accompagnati da nodi di archiviazione ad alte prestazioni solo metadati.

Quando si installano nodi solo dati, la griglia deve contenere quanto segue:

- Un minimo di due nodi di archiviazione combinati o solo dati *per griglia*
- Almeno un nodo di archiviazione combinato o solo dati *per sito*
- Un minimo di tre nodi di archiviazione combinati o solo metadati *per sito*

Servizi primari per i nodi di archiviazione

Nella tabella seguente sono riportati i servizi principali per i nodi di archiviazione; tuttavia, questa tabella non elenca tutti i servizi dei nodi.



Alcuni servizi, come il servizio ADC e il servizio RSM, in genere sono presenti solo su tre nodi di archiviazione in ogni sito.

Servizio	Funzione chiave
Conto (account)	Gestisce i conti degli inquilini.

Servizio	Funzione chiave
Controller di dominio amministrativo (ADC)	Mantiene la topologia e la configurazione dell'intera griglia. Nota: i nodi di archiviazione solo dati non ospitano il servizio ADC. Dettagli Il servizio Administrative Domain Controller (ADC) autentica i nodi della griglia e le loro connessioni reciproche. Il servizio ADC è ospitato su un minimo di tre nodi di archiviazione in un sito. Il servizio ADC gestisce le informazioni sulla topologia, tra cui 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 bundle di configurazione della distribuzione StorageGRID , consentendo a qualsiasi nodo della griglia di recuperare le informazioni di configurazione correnti. Per facilitare le operazioni distribuite e in isola, ogni 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 della griglia mantengono una connessione ad almeno un servizio ADC. Ciò garantisce che i nodi della griglia accedano sempre alle informazioni più recenti. Quando i nodi della griglia si connettono, memorizzano nella cache i certificati degli altri nodi della griglia, consentendo ai sistemi di continuare a funzionare con i nodi della griglia noti anche quando un servizio ADC non è disponibile. I nuovi nodi della griglia possono stabilire connessioni solo tramite un servizio ADC. La connessione di ciascun nodo della griglia consente al servizio ADC di raccogliere informazioni sulla topologia. Le informazioni sul nodo della griglia includono il carico della CPU, lo spazio disponibile su disco (se dispone di spazio di archiviazione), 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 query con le informazioni più recenti ricevute dal sistema StorageGRID .
Cassandra	Memorizza e protegge i metadati degli oggetti. Nota: i nodi di archiviazione solo dati non ospitano il servizio Cassandra.
Cassandra Reaper	Esegue riparazioni automatiche dei metadati degli oggetti. Nota: i nodi di archiviazione solo dati non ospitano il servizio Cassandra Reaper.
Pezzo	Gestisce i dati codificati in modo cancellabile e i frammenti di parità.

Servizio	Funzione chiave
Spostamento dati (DMV)	Sposta i dati nei pool di archiviazione cloud.
Archivio dati distribuito (DDS)	Monitora l'archiviazione dei metadati degli oggetti. Dettagli Ogni nodo di archiviazione include il servizio Distributed Data Store (DDS). 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 ingeriti nel sistema StorageGRID , nonché del numero totale di oggetti ingeriti tramite ciascuna delle interfacce supportate dal sistema (S3).
Identità (idnt)	Federa le identità utente da LDAP e Active Directory.

Servizio	Funzione chiave
Router di distribuzione locale (LDR)	Elabora le richieste del protocollo di archiviazione degli oggetti e gestisce i dati degli oggetti su disco.

Servizio	Funzione chiave
Macchina a stati replicati (RSM)	Garantisce che le richieste dei servizi della piattaforma S3 vengano inviate ai rispettivi endpoint.
Monitoraggio dello stato del server (SSM)	Monitora il sistema operativo e l'hardware sottostante.

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

Che cos'è un nodo gateway?

Il servizio LDR gestisce le seguenti attività:
 I nodi gateway forniscono un'interfaccia di bilanciamento del carico dedicata che le applicazioni client S3 possono utilizzare per connettersi a StorageGRID. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo il carico di lavoro su più nodi di archiviazione. I nodi gateway sono facoltativi.

Il servizio StorageGRID Load Balancer gestisce tutti i nodi amministrativi e su tutti i nodi gateway. Esegue la terminazione Transport Layer Security (TLS) delle richieste client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di archiviazione. Il servizio Load Balancer indirizza senza soluzione di continuità i client verso un nodo di archiviazione ottimale, in modo che il guasto dei nodi o addirittura di un intero sito sia trasparente.

È possibile configurare uno o più endpoint del bilanciatore del carico per definire la porta e il protocollo di rete (HTTPS o HTTP) che le richieste client in entrata e in uscita utilizzeranno per accedere ai servizi del bilanciatore del carico sui nodi gateway e amministrativi. L'endpoint del bilanciatore del carico definisce anche il tipo di client (S3), la modalità di associazione e, facoltativamente, un elenco di tenant consentiti o bloccati.

Vedere ["Considerazioni sul bilanciamento del carico"](#).

Se necessario, è possibile raggruppare le interfacce di rete di più nodi gateway e nodi amministrativi in un gruppo ad alta disponibilità (HA). Se l'interfaccia attiva nel gruppo HA non funziona, un'interfaccia di backup può gestire il carico di lavoro dell'applicazione client. Vedere ["Gestire gruppi ad alta disponibilità \(HA\)"](#).

Servizi primari per i nodi gateway

Nella tabella seguente sono riportati i servizi principali per i nodi gateway; tuttavia, questa tabella non elenca tutti i servizi del nodo.

Servizio	Funzione chiave
Alta disponibilità	Gestisce indirizzi IP virtuali ad alta disponibilità per gruppi di nodi amministrativi e nodi gateway. Nota: questo servizio è disponibile anche sui nodi amministrativi.
Bilanciatore del carico	Fornisce il bilanciamento del carico di livello 7 del traffico S3 dai client ai nodi di archiviazione. Questo è il meccanismo di bilanciamento del carico consigliato. Nota: questo servizio è disponibile anche sui nodi amministrativi.
Monitoraggio dello stato del server (SSM)	Monitora il sistema operativo e l'hardware sottostante.

maggiori dettagli, vedere ["Gestire l'archiviazione dei metadati degli oggetti"](#).

Che cos'è un nodo archivio?

Il supporto per i nodi di archivio è stato rimosso.

Per informazioni sui nodi di archivio, vedere ["Che cos'è un nodo di archivio \(sito di documentazione StorageGRID 11.8\)"](#).

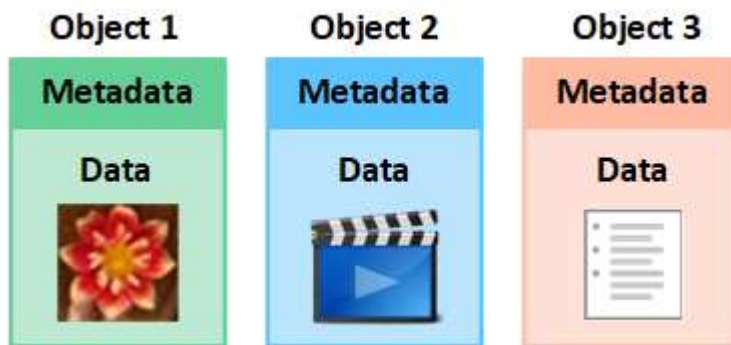
Come StorageGRID gestisce i dati

Che cosa è un oggetto

Con l'archiviazione di oggetti, l'unità di archiviazione è un oggetto, anziché un file o un blocco. A differenza della gerarchia ad albero di un file system o di un archivio a blocchi, l'archiviazione a oggetti organizza i dati in un layout piatto e non strutturato.

L'archiviazione di oggetti separa la posizione fisica dei dati dal metodo utilizzato per archiviare e recuperare tali dati.

Ogni oggetto in un sistema di archiviazione basato su oggetti è costituito da due parti: dati dell'oggetto e metadati dell'oggetto.



Cosa sono i dati oggetto?

I dati oggetto possono essere qualsiasi cosa, ad esempio una fotografia, un filmato o una cartella clinica.

Cosa sono i metadati degli oggetti?

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

I metadati degli oggetti includono informazioni come le seguenti:

- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3 o del contenitore 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 in cui l'oggetto è stato modificato per l'ultima volta.
- Posizione di archiviazione corrente di ogni copia dell'oggetto o frammento codificato per la cancellazione.
- Tutti i metadati utente associati all'oggetto.

I metadati degli oggetti sono personalizzabili ed espandibili, il che li rende flessibili per l'utilizzo da parte delle

applicazioni.

Per informazioni dettagliate su come e dove StorageGRID memorizza i metadati degli oggetti, visitare ["Gestire l'archiviazione dei metadati degli oggetti"](#).

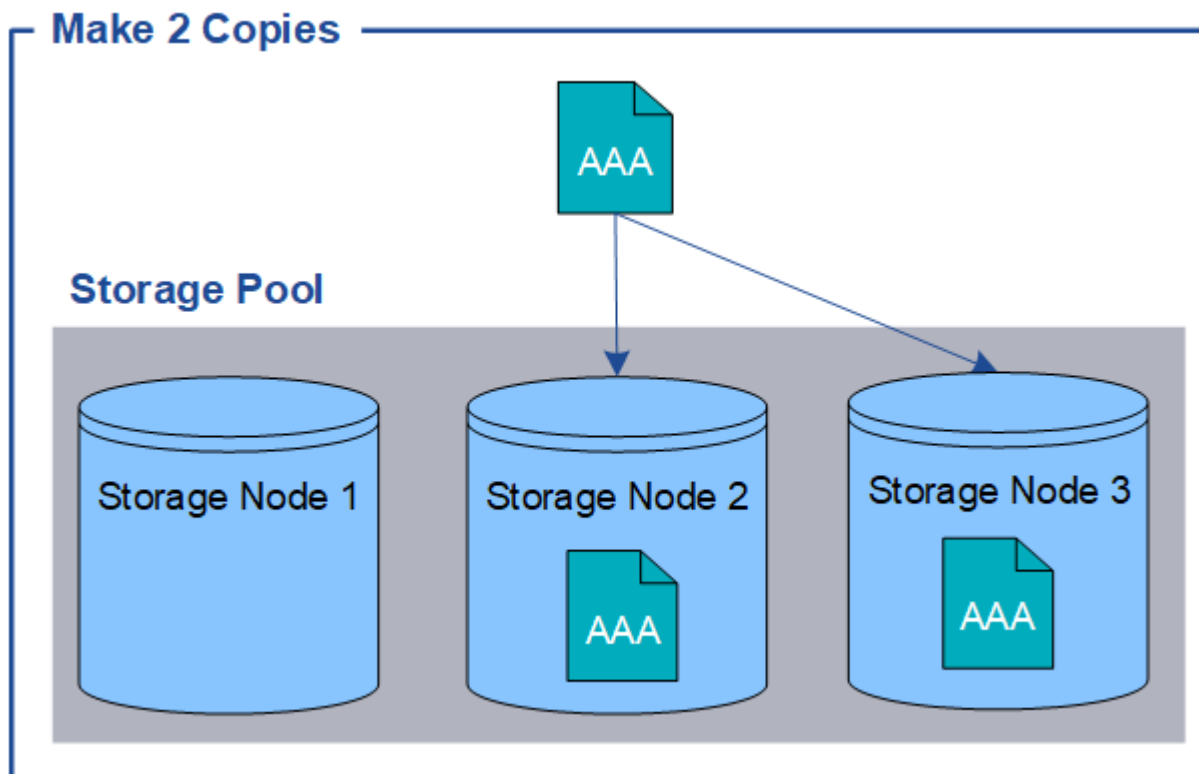
Come vengono protetti i dati degli oggetti?

Il sistema StorageGRID fornisce due meccanismi per proteggere i dati degli oggetti dalla perdita: la replicazione e la codifica di cancellazione.

Replicazione

Quando StorageGRID abbina gli oggetti a una regola di gestione del ciclo di vita delle informazioni (ILM) configurata per creare copie replicate, il sistema crea copie esatte dei dati degli oggetti e le archivia su nodi di archiviazione o pool di archiviazione cloud. Le regole ILM stabiliscono il numero di copie effettuate, dove tali copie vengono archiviate e per quanto tempo vengono conservate dal sistema. Se una copia viene persa, ad esempio a causa della perdita di un nodo di archiviazione, l'oggetto è comunque disponibile se ne esiste una copia altrove nel sistema StorageGRID.

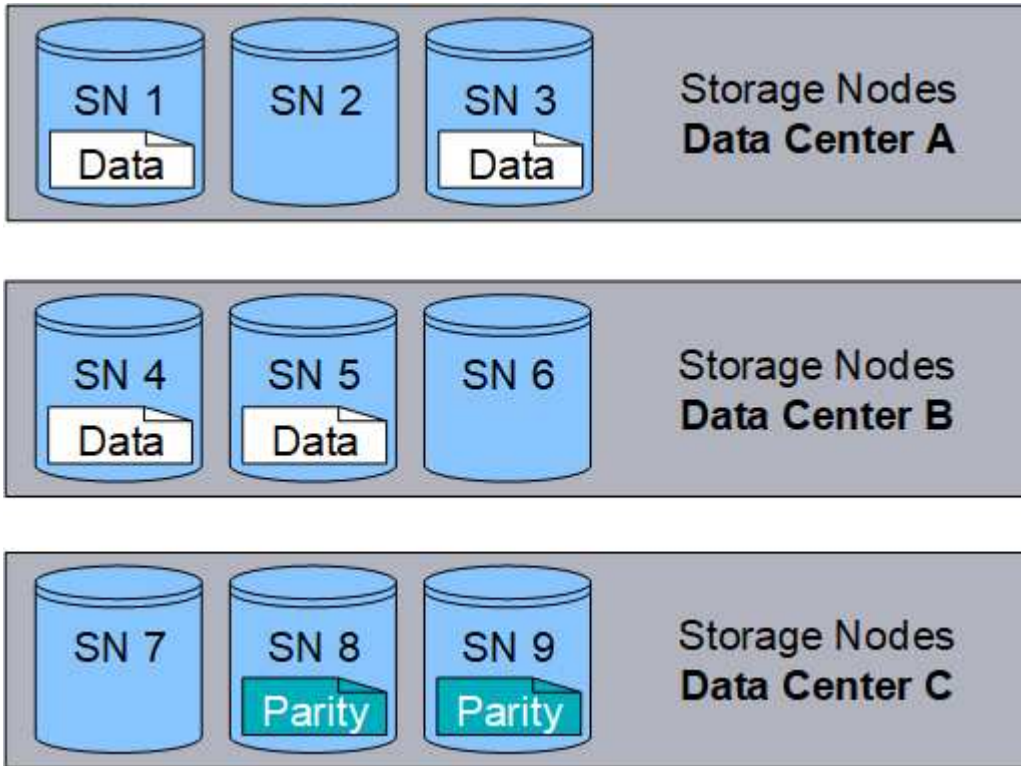
Nell'esempio seguente, la regola Crea 2 copie specifica che due copie replicate di ciascun oggetto devono essere inserite in un pool di archiviazione contenente tre nodi di archiviazione.



Codifica di cancellazione

Quando StorageGRID abbina gli oggetti a una regola ILM configurata per creare copie con codice di cancellazione, suddivide i dati dell'oggetto in frammenti di dati, calcola frammenti di parità aggiuntivi e archivia ciascun frammento su un diverso nodo di archiviazione. Quando si accede a un oggetto, questo viene riassembleato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità si danneggia o viene perso, l'algoritmo di codifica di cancellazione può ricreare quel frammento utilizzando un sottoinsieme dei dati e dei frammenti di parità rimanenti. Le regole ILM e i profili di codifica della cancellazione determinano lo schema di codifica della cancellazione utilizzato.

L'esempio seguente illustra l'uso della codifica di cancellazione sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di codifica di cancellazione 4+2. Ogni oggetto viene suddiviso in quattro frammenti di dati uguali e dai dati dell'oggetto vengono calcolati due frammenti di parità. Ciascuno dei sei frammenti viene archiviato su un diverso nodo di archiviazione in tre data center per garantire la protezione dei dati in caso di guasti dei nodi o perdite del sito.



Informazioni correlate

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

La vita di un oggetto

La vita di un oggetto è composta da varie fasi. Ogni fase rappresenta le operazioni che si verificano sull'oggetto.

La vita di un oggetto comprende le operazioni di acquisizione, gestione delle copie, recupero ed eliminazione.

- **Ingest:** il processo di un'applicazione client S3 che salva un oggetto tramite HTTP nel sistema StorageGRID. In questa fase, il sistema StorageGRID inizia a gestire l'oggetto.
- **Gestione delle copie:** il processo di gestione delle copie replicate e con codice di cancellazione in StorageGRID, come descritto dalle regole ILM nelle policy ILM attive. Durante la fase di gestione delle copie, StorageGRID protegge i dati degli oggetti dalla perdita creando e gestendo il numero e il tipo specificati di copie degli oggetti sui nodi di archiviazione o in un pool di archiviazione cloud.
- **Recupera:** il processo di un'applicazione client che accede a un oggetto archiviato dal sistema StorageGRID. Il client legge l'oggetto, che viene recuperato da un nodo di archiviazione o da un pool di archiviazione cloud.
- **Elimina:** il processo di rimozione di tutte le copie degli oggetti dalla griglia. Gli oggetti possono essere eliminati tramite l'invio di una richiesta di eliminazione da parte dell'applicazione client al sistema StorageGRID oppure tramite un processo automatico eseguito da StorageGRID alla scadenza del ciclo di

vita dell'oggetto.



Informazioni correlate

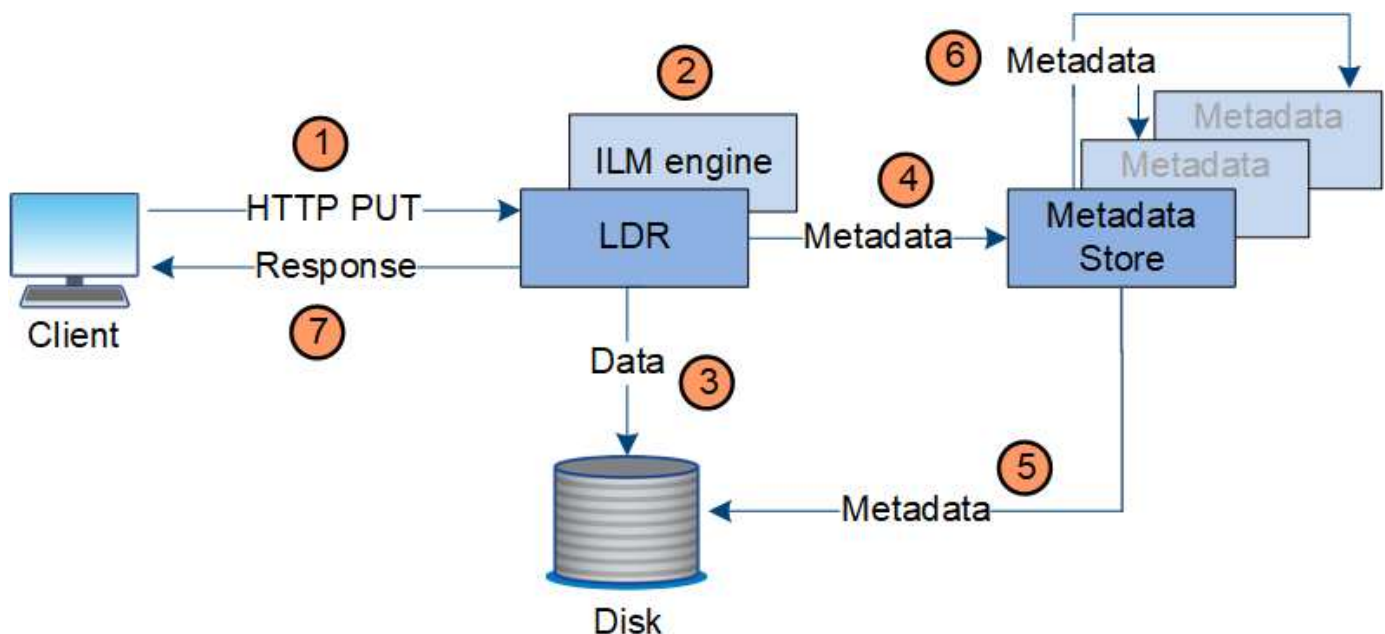
- ["Gestire gli oggetti con ILM"](#)
- ["Utilizzare la gestione del ciclo di vita delle informazioni"](#)

Flusso di dati di acquisizione

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 inserisce un oggetto nel sistema StorageGRID , il servizio LDR sui nodi di archiviazione 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 alla politica ILM del sistema.
3. Il servizio LDR salva i dati dell'oggetto come copia replicata o come copia con codice di cancellazione. (Il diagramma mostra una versione semplificata dell'archiviazione di una copia replicata su disco.)
4. Il servizio LDR invia i metadati dell'oggetto all'archivio metadati.
5. L'archivio metadati salva i metadati dell'oggetto su disco.
6. L'archivio metadati propaga copie dei metadati degli oggetti ad altri nodi di archiviazione. Queste copie vengono salvate anche su disco.

7. Il servizio LDR restituisce al client una risposta HTTP 200 OK 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 creano copie replicate o con codice di cancellazione per proteggere i dati degli oggetti dalla perdita.

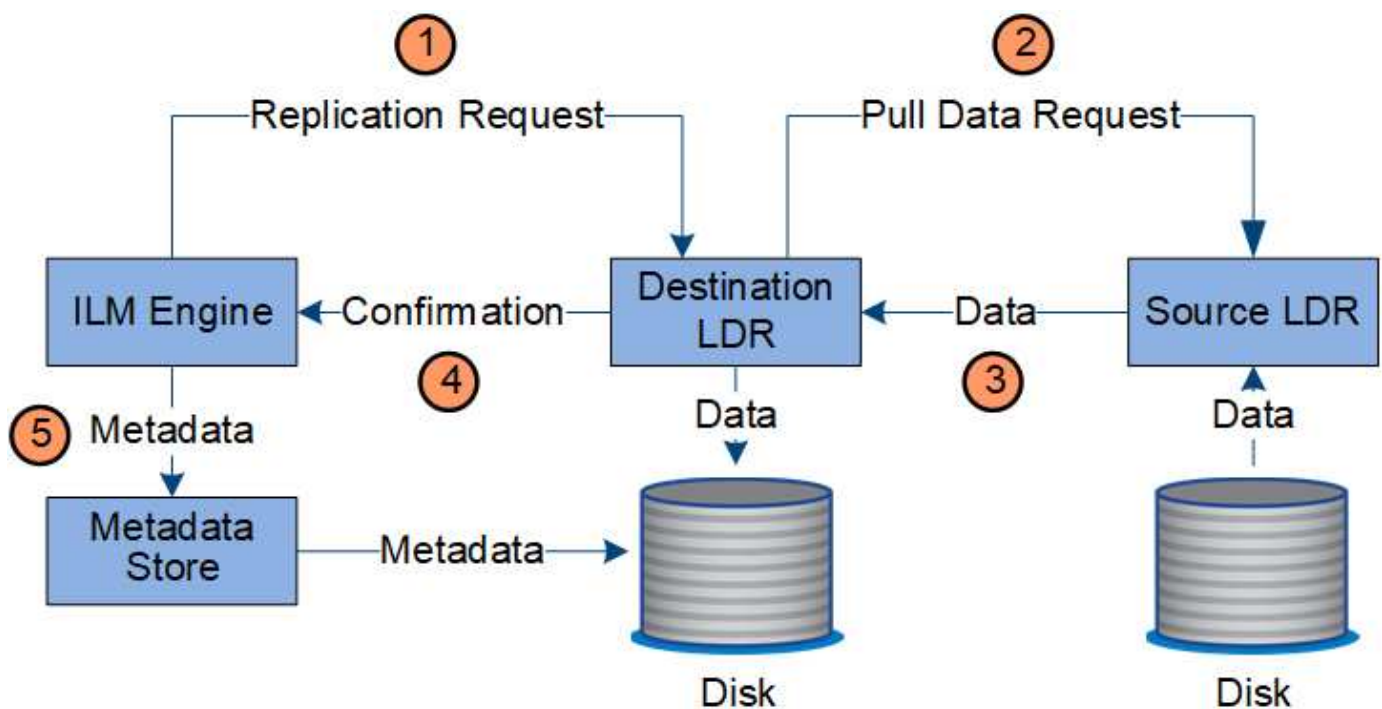
Potrebbero essere necessari tipi o posizioni diverse di copie di oggetti in momenti diversi della vita dell'oggetto. Le regole ILM vengono valutate periodicamente per garantire che gli oggetti vengano posizionati come richiesto.

I dati degli oggetti sono gestiti dal servizio LDR.

Protezione del contenuto: replicazione

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

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



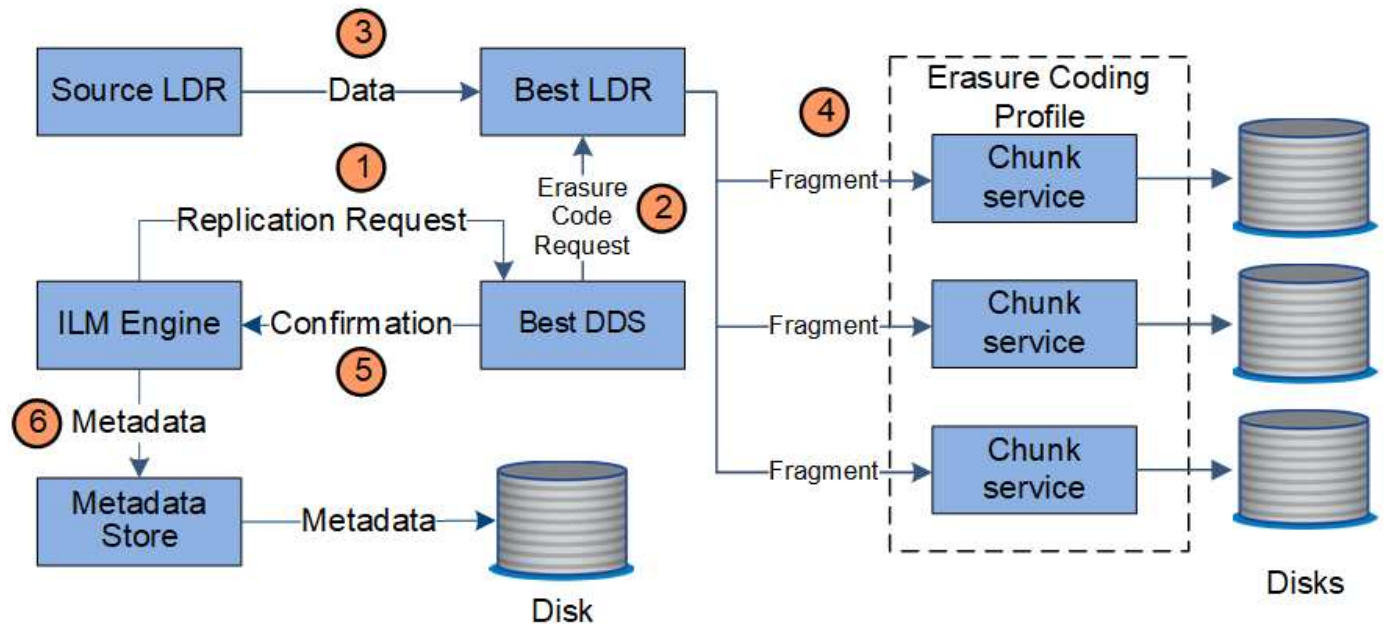
1. Il motore ILM interroga il servizio ADC per determinare il miglior servizio LDR di destinazione all'interno del pool di archiviazione specificato dalla regola ILM. Invia quindi al servizio LDR un comando per avviare la replica.
2. Il servizio LDR di destinazione interroga il servizio ADC per individuare la posizione di origine migliore. Invia quindi 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 archiviati.
5. Il motore ILM aggiorna l'archivio dei metadati con i metadati sulla posizione degli oggetti.

Protezione dei contenuti: codifica di cancellazione

Se una regola ILM include istruzioni per creare copie con codifica di cancellazione dei dati dell'oggetto, lo schema di codifica di cancellazione applicabile suddivide i dati dell'oggetto in frammenti di dati e di parità e distribuisce tali frammenti tra i nodi di archiviazione configurati nel profilo di codifica di cancellazione.

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

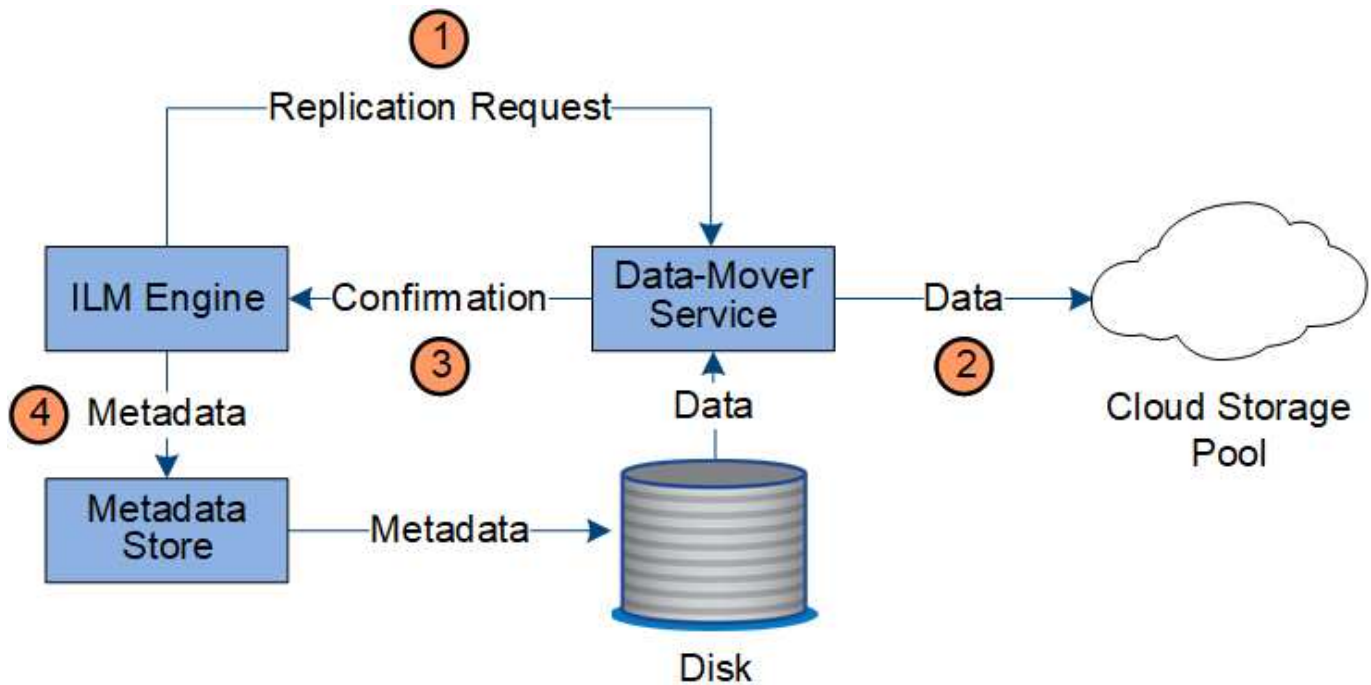


1. Il motore ILM interroga il servizio ADC per determinare quale servizio DDS può eseguire al meglio l'operazione di codifica di cancellazione. Una volta determinato, il motore ILM invia una richiesta di "avvio" a quel servizio.
2. Il servizio DDS istruisce un LDR a cancellare il codice dei dati dell'oggetto.
3. Il servizio LDR di origine invia una copia al servizio LDR selezionato per la codifica di cancellazione.
4. Dopo aver creato il numero appropriato di frammenti di parità e di dati, il servizio LDR distribuisce tali frammenti tra i nodi di archiviazione (servizi Chunk) che costituiscono il pool di archiviazione del profilo di codifica di cancellazione.
5. Il servizio LDR notifica al motore ILM la corretta distribuzione dei dati dell'oggetto.
6. Il motore ILM aggiorna l'archivio dei metadati con i metadati sulla posizione degli oggetti.

Protezione dei contenuti: Cloud Storage Pool

Se le istruzioni di posizionamento del contenuto di una regola ILM richiedono che una copia replicata dei dati dell'oggetto venga archiviata in un Cloud Storage Pool, i dati dell'oggetto vengono duplicati nel bucket S3 esterno o nel contenitore di archiviazione BLOB di Azure 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 archiviati.
4. Il motore ILM aggiorna l'archivio dei metadati con i metadati sulla posizione degli oggetti.

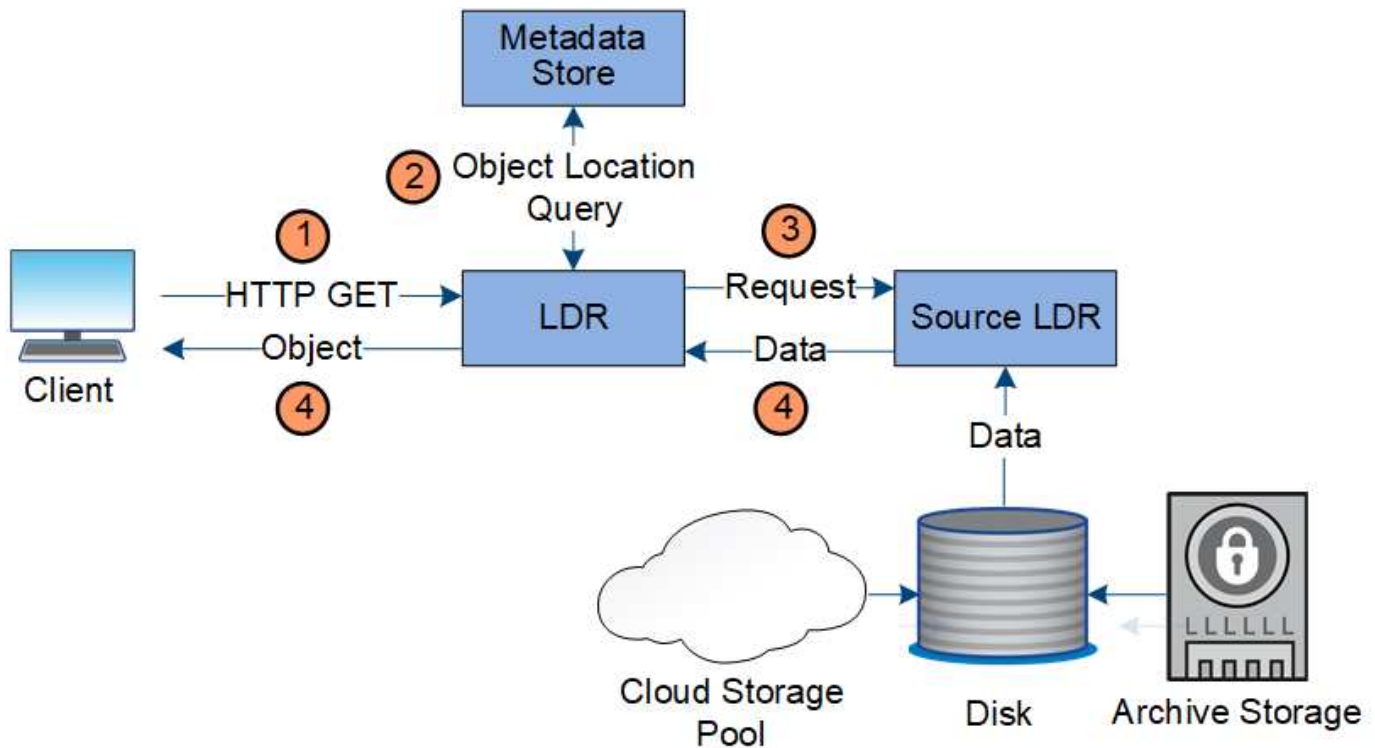
Recupera il flusso di dati

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

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



Se l'unica copia dell'oggetto si trova nello storage AWS Glacier o nel livello Azure Archive, l'applicazione client deve inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel Cloud Storage Pool.



1. Il servizio LDR riceve una richiesta di recupero dall'applicazione client.
2. Il servizio LDR interroga l'archivio metadati per conoscere 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.

Elimina flusso di dati

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

Gerarchia di eliminazione

StorageGRID fornisce diversi metodi per controllare quando gli oggetti vengono conservati o eliminati. Gli oggetti possono essere eliminati su richiesta del client o automaticamente. StorageGRID dà sempre priorità alle impostazioni di blocco degli oggetti S3 rispetto alle richieste di eliminazione del client, che a loro volta hanno priorità sul ciclo di vita del bucket S3 e sulle istruzioni di posizionamento ILM.

- **Blocco oggetto S3:** se l'impostazione globale Blocco oggetto S3 è abilitata per la griglia, i client S3 possono creare bucket con Blocco oggetto S3 abilitato e quindi utilizzare l'API REST S3 per specificare le impostazioni di conservazione fino alla data di scadenza e di conservazione legale per ogni versione dell'oggetto aggiunta a tale bucket.
 - Una versione di un oggetto sottoposta a conservazione legale non può essere eliminata con alcun metodo.
 - Prima che venga raggiunta la data di conservazione di una versione di un oggetto, tale versione non può essere eliminata con alcun metodo.

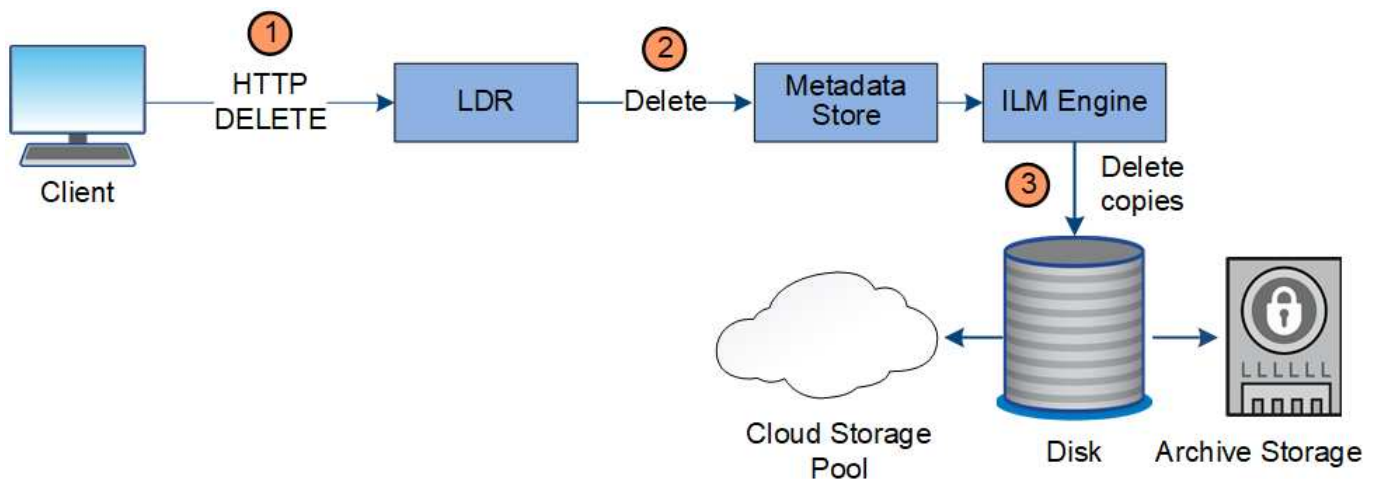
- Gli oggetti nei bucket con S3 Object Lock abilitato vengono conservati da ILM "per sempre". Tuttavia, una volta raggiunta la data di conservazione, una versione dell'oggetto può essere eliminata da una richiesta del client o dalla scadenza del ciclo di vita del bucket.
- Se i client S3 applicano una retain-until-date predefinita al bucket, non è necessario specificare una retain-until-date per ciascun oggetto.
- **Richiesta di eliminazione del client:** un client S3 può inviare una richiesta di eliminazione di un oggetto. Quando un client elimina un oggetto, tutte le copie dell'oggetto vengono rimosse dal sistema StorageGRID .
- **Elimina oggetti nel bucket:** gli utenti Tenant Manager possono utilizzare questa opzione per rimuovere definitivamente tutte le copie degli oggetti e le versioni degli oggetti nei bucket selezionati dal sistema StorageGRID .
- **Ciclo di vita del bucket S3:** i client S3 possono aggiungere ai propri bucket una configurazione del ciclo di vita che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID elimina automaticamente tutte le copie di un oggetto quando vengono raggiunti la data o il numero di giorni specificati nell'azione Scadenza, a meno che il client non elimini prima l'oggetto.
- **Istruzioni per il posizionamento ILM:** presupponendo che il bucket non abbia abilitato S3 Object Lock e che non vi sia alcun ciclo di vita del bucket, StorageGRID elimina automaticamente un oggetto quando termina l'ultimo periodo di tempo nella regola ILM e non sono specificati ulteriori posizionamenti per l'oggetto.



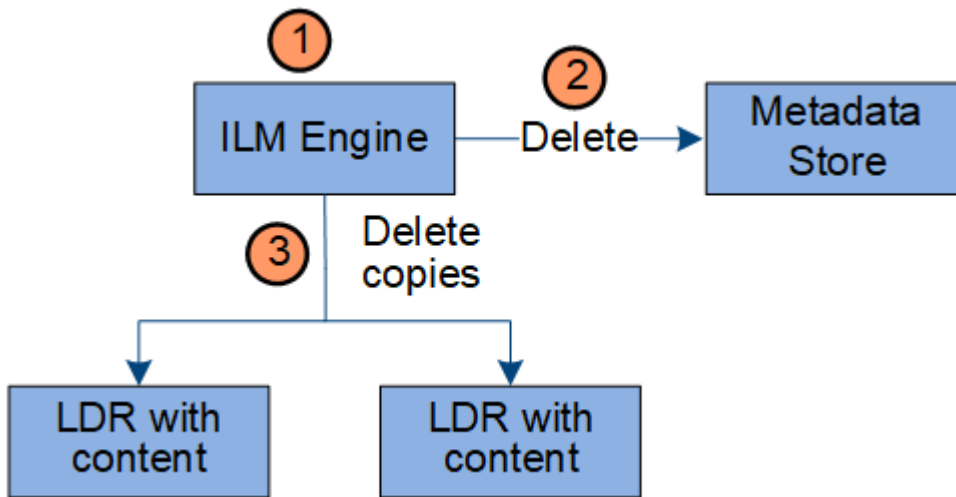
Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti che corrispondono al filtro del ciclo di vita. Di conseguenza, un oggetto potrebbe essere mantenuto sulla griglia anche dopo che sono scadute tutte le istruzioni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

Vedere ["Come vengono eliminati gli oggetti"](#) per maggiori informazioni.

Flusso di dati per le eliminazioni dei client



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



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

Gestione del ciclo di vita delle informazioni

È possibile utilizzare 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 archivia gli oggetti nel tempo. È possibile configurare una o più regole ILM e quindi aggiungerle a un criterio ILM. Una griglia può avere più di una policy attiva contemporaneamente.

Le regole ILM definiscono:

- Quali oggetti dovrebbero essere conservati. Una regola può essere applicata a tutti gli oggetti oppure è possibile specificare dei 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 contenitori Swift oppure a specifici valori di metadati.
- Tipo e posizione di archiviazione. Gli oggetti possono essere archiviati su nodi di archiviazione o in pool di archiviazione cloud.
- Il tipo di copie dell'oggetto realizzate. Le copie possono essere replicate o codificate in modo da essere cancellate.
- Per le copie replicate, il numero di copie realizzate.
- Per le copie con codice di cancellazione, viene utilizzato lo schema di codifica di cancellazione.
- Le modifiche nel tempo alla posizione di archiviazione di un oggetto e al tipo di copie.
- Modalità di protezione dei dati degli oggetti quando gli oggetti vengono inseriti 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 archiviati in un database Cassandra, in quello che è noto come archivio di metadati. In ogni sito vengono conservate automaticamente tre copie dei metadati degli oggetti per proteggere i dati da eventuali perdite.

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applica solo agli oggetti appartenenti all'inquilino A.
- Realizza due copie replicate di quegli oggetti e conserva ciascuna copia in un luogo diverso.
- Conservare le due copie "per sempre", il che significa che StorageGRID non le eliminerà automaticamente. StorageGRID conserverà invece questi oggetti finché non verranno eliminati da una richiesta di eliminazione del client o dalla scadenza del ciclo di vita di un bucket.
- Utilizzare l'opzione Bilanciato per il comportamento di acquisizione: l'istruzione di posizionamento su due siti viene applicata non appena il Tenant A salva un oggetto in StorageGRID, a meno che non sia possibile effettuare 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 provvisorie sui nodi di archiviazione del sito 1. Non appena il Sito 2 sarà disponibile, StorageGRID effettuerà la copia richiesta in quel sito.

Come una policy ILM valuta gli oggetti

I criteri ILM attivi per il sistema StorageGRID controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti.

Quando i client salvano oggetti in StorageGRID, gli oggetti vengono valutati in base al set ordinato di regole ILM nella policy attiva, come segue:

1. Se i filtri per la prima regola nel criterio corrispondono a un oggetto, l'oggetto viene acquisito in base al comportamento di acquisizione di quella regola e archiviato in base alle istruzioni di posizionamento di quella regola.
2. Se i filtri per la prima regola non corrispondono all'oggetto, l'oggetto viene valutato rispetto a ogni regola successiva nel criterio finché non viene trovata una corrispondenza.
3. Se nessuna regola corrisponde a un oggetto, vengono applicate le istruzioni di posizionamento e comportamento di acquisizione per la 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.

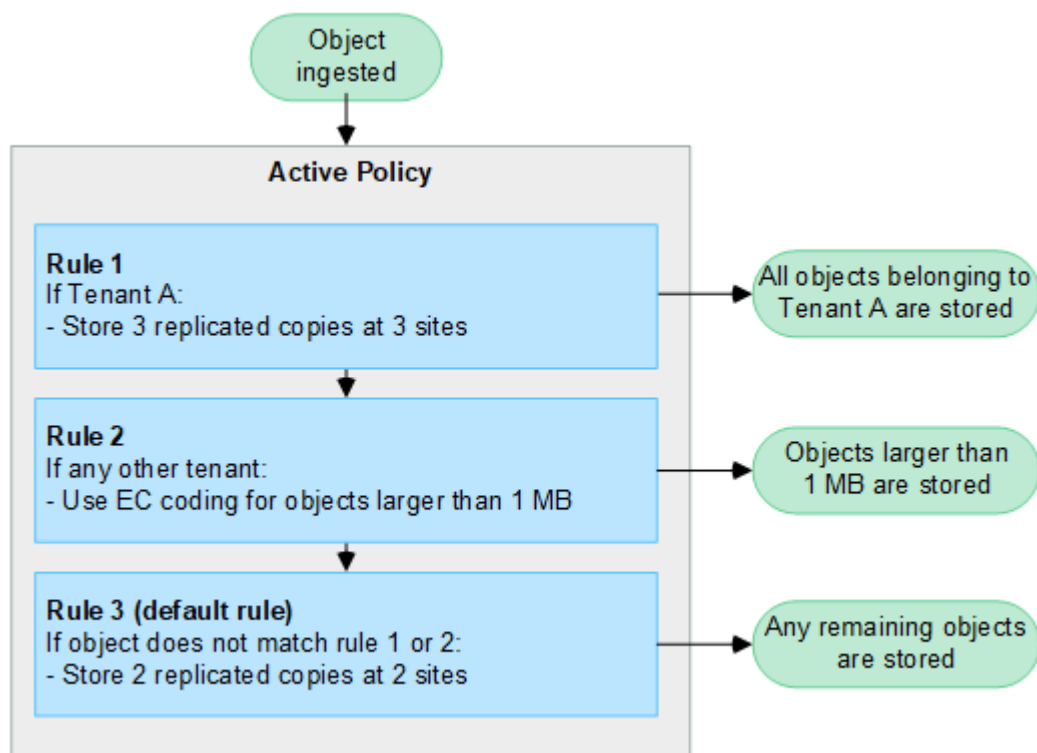
Esempio di politica ILM

Ad esempio, una policy ILM potrebbe contenere tre regole ILM che specificano quanto segue:

- **Regola 1: Copie replicate per l'inquilino A**
 - Abbina tutti gli oggetti appartenenti all'inquilino A.
 - Conservare questi oggetti in tre copie replicate in tre siti.
 - Gli oggetti appartenenti ad altri tenant non sono soggetti alla Regola 1, pertanto vengono valutati in base alla Regola 2.
- **Regola 2: Codifica di cancellazione per oggetti di dimensioni superiori a 1 MB**
 - Corrisponde a tutti gli oggetti degli altri tenant, ma solo se sono maggiori di 1 MB. Questi oggetti di grandi dimensioni 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** (predefinita)

- È l'ultima regola predefinita della policy. Non utilizza filtri.
- Eseguire 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 agli screenshot di esempio presenti in questa pagina.

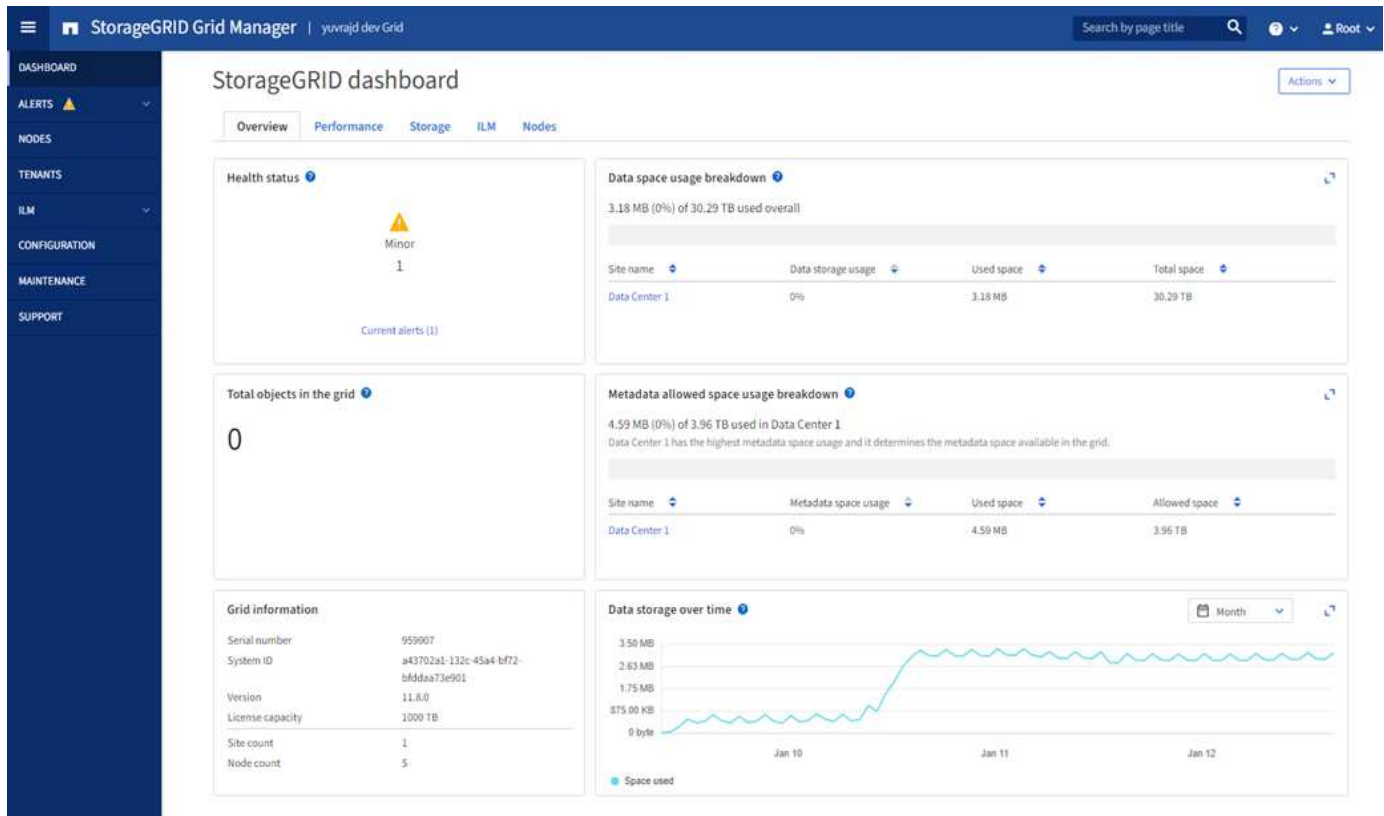
Quando accedi a Grid Manager, ti connetti a un nodo di amministrazione. Ogni sistema StorageGRID include un nodo amministrativo primario e un numero qualsiasi di nodi amministrativi non primari. È possibile connettersi a qualsiasi nodo di amministrazione e ogni nodo di amministrazione visualizza una vista simile del sistema StorageGRID.

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

Dashboard di Grid Manager

Quando accedi per la prima volta a Grid Manager, puoi utilizzare la dashboard per ["monitorare le attività del sistema"](#) a colpo d'occhio.

La dashboard contiene informazioni sullo stato e sulle prestazioni del sistema, sull'utilizzo dello storage, sui processi ILM, sulle operazioni S3 e sui nodi nella griglia. Puoi [configurare la dashboard](#) selezionando da una raccolta di schede che contengono le informazioni necessarie per monitorare efficacemente il tuo sistema.



Per una spiegazione delle informazioni mostrate su ogni scheda, seleziona l'icona della guida per quella carta.

Campo di ricerca

Il campo **Cerca** nella barra dell'interfaccia consente di navigare rapidamente verso una pagina specifica all'interno di Grid Manager. Ad esempio, puoi immettere **km** per accedere alla pagina del server di gestione delle chiavi (KMS).

È possibile utilizzare **Cerca** per trovare voci nella barra laterale di Grid Manager e nei menu Configurazione, Manutenzione e Supporto. È anche possibile cercare per nome elementi come nodi della griglia e account tenant.

Menu di aiuto

Il menu di aiuto fornisce accesso a:

- IL ["FabricPool"](#) E ["Configurazione 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 StorageGRID .

Dal menu Avvisi, puoi fare quanto segue per ["gestire gli avvisi"](#) :

- Rivedi gli avvisi attuali
- Esamina gli avvisi risolti
- Configura i silenzi per sopprimere le notifiche di avviso
- Definisci regole di avviso per le condizioni che attivano gli avvisi
- Configurare il server di posta elettronica per le notifiche di avviso

Pagina dei nodi

IL ["Pagina dei nodi"](#) visualizza informazioni sull'intera griglia, su ciascun sito nella griglia e su ciascun nodo in un sito.

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

Nodes

View the list and status of sites and grid nodes.

Total node count: 14

Name ?	Type	Object data used ?	Object metadata used ?	CPU usage ?
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

Pagina degli inquilini

IL ["Pagina degli inquilini"](#) ti permette di ["creare e monitorare gli account dei tenant di storage"](#) per il tuo sistema StorageGRID . È necessario creare almeno un account tenant per specificare chi può archiviare e recuperare oggetti e quali funzionalità sono a sua disposizione.

La pagina Inquilini fornisce anche dettagli sull'utilizzo per ciascun inquilino, tra cui la quantità di spazio di archiviazione utilizzato e il numero di oggetti. Se imposti una quota quando crei il tenant, puoi vedere quanta di quella quota è stata utilizzata.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#) [Export to CSV](#) [Actions](#)

Displaying 2 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	S3 Tenant	0 bytes	0%	100.00 GB	0	→ 📄
☐	Swift Tenant	0 bytes	0%	100.00 GB	0	→ 📄

← Previous 1 Next →

Menù ILM

IL "Menù ILM" ti permette di [configurare le regole e le policy di gestione del ciclo di vita delle informazioni \(ILM\)](#) che regolano la durabilità e la disponibilità dei dati. È anche possibile immettere un identificatore di oggetto per visualizzare i metadati di tale oggetto.

Dal menu ILM è possibile visualizzare e gestire ILM:

- Regole
- Politiche
- Tag di policy
- Pool di stoccaggio
- Gradi di stoccaggio
- Regioni
- Ricerca metadati oggetto

Menu di configurazione

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

Attività di rete

Le attività di rete includono:

- ["Gestione di gruppi ad alta disponibilità"](#)
- ["Gestione degli endpoint del bilanciatore del carico"](#)
- ["Configurazione dei nomi di dominio degli endpoint S3"](#)
- ["Gestione delle politiche di classificazione del traffico"](#)
- ["Configurazione delle interfacce VLAN"](#)

Compiti di sicurezza

I compiti di sicurezza includono:

- "Gestione dei certificati di sicurezza"
- "Gestione dei controlli del firewall interno"
- "Configurazione dei server di gestione delle chiavi"
- Configurazione delle impostazioni di sicurezza, incluso il "Politica TLS e SSH" , "opzioni di sicurezza di rete e oggetti" , E "impostazioni di sicurezza dell'interfaccia" .
- Configurazione delle impostazioni per un "proxy di archiviazione" o un "proxy amministratore"

Attività di sistema

Le attività di sistema includono:

- Utilizzando "federazione di rete" per clonare le informazioni dell'account tenant e replicare i dati degli oggetti tra due sistemi StorageGRID .
- Facoltativamente, abilitando il "Comprimi gli oggetti memorizzati" opzione.
- "Gestione del blocco degli oggetti S3"
- Comprendere le opzioni di archiviazione come "segmentazione degli oggetti" E "filigrane del volume di archiviazione" .
- "Gestisci i profili di codifica di cancellazione" .

Attività di monitoraggio

Le attività di monitoraggio includono:

- "Configurazione dei messaggi di controllo e delle destinazioni dei registri"
- "Utilizzo del monitoraggio SNMP"

Attività di controllo degli accessi

Le attività di controllo degli accessi includono:

- "Gestione dei gruppi di amministrazione"
- "Gestione degli utenti amministratori"
- Cambiando il "passphrase di provisioning" O "password della console del nodo"
- "Utilizzo della federazione delle identità"
- "Configurazione SSO"

Menu di manutenzione

Il menu Manutenzione consente di eseguire attività di manutenzione, manutenzione del sistema e manutenzione della rete.

Compiti

Le attività di manutenzione includono:

- ["Operazioni di dismissione"](#) per rimuovere nodi e siti della griglia non utilizzati
- ["Operazioni di espansione"](#) per aggiungere nuovi nodi e siti della griglia
- ["Procedure di ripristino del nodo della griglia"](#) per sostituire un nodo guasto e ripristinare i dati
- ["Rinominare le procedure"](#) per modificare i nomi visualizzati della griglia, dei siti e dei nodi
- ["Operazioni di controllo dell'esistenza dell'oggetto"](#) per verificare l'esistenza (anche se non la correttezza) dei dati dell'oggetto
- Esecuzione di un ["riavvio progressivo"](#) per riavviare più nodi della griglia
- ["Operazioni di ripristino del volume"](#)

Sistema

Le attività di manutenzione del sistema che puoi eseguire includono:

- ["Visualizzazione delle informazioni sulla licenza StorageGRID"](#) o ["aggiornamento delle informazioni sulla licenza"](#)
- Generazione e download del ["Pacchetto di recupero"](#)
- Esecuzione di aggiornamenti software StorageGRID , inclusi aggiornamenti software, hotfix e aggiornamenti al software SANtricity OS su appliance selezionate
 - ["Procedura di aggiornamento"](#)
 - ["Procedura di hotfix"](#)
 - ["Aggiornare il sistema operativo SANtricity sui controller di archiviazione SG6000 utilizzando Grid Manager"](#)
 - ["Aggiornare il sistema operativo SANtricity sui controller di archiviazione SG5700 utilizzando Grid Manager"](#)

Rete

Le attività di manutenzione della rete che puoi eseguire includono:

- ["Configurazione dei server DNS"](#)
- ["Aggiornamento delle subnet della rete Grid"](#)
- ["Gestione dei server NTP"](#)

Menu di supporto

Il menu Supporto fornisce opzioni che aiutano il supporto tecnico ad analizzare e risolvere i problemi del sistema.

Utensili

Dalla sezione Strumenti del menu Supporto, puoi:

- ["Configura AutoSupport"](#)
- ["Eseguire la diagnostica"](#) sullo stato attuale della rete
- ["Accedi all'albero della topologia della griglia"](#) per visualizzare informazioni dettagliate sui nodi, sui servizi e sugli attributi della griglia

- ["Raccogli file di registro e dati di sistema"](#)
- ["Esaminare le metriche di supporto"](#)



Gli strumenti disponibili nell'opzione **Metriche** sono destinati all'uso da parte del supporto tecnico. Alcune funzionalità e voci di menu di questi strumenti sono intenzionalmente non funzionali.

Allarmi (legacy)

Le informazioni sugli allarmi legacy sono state rimosse da questa versione della documentazione. Fare riferimento a ["Gestire avvisi e allarmi \(documentazione StorageGRID 11.8\)"](#).

Altro

Dalla sezione Altro del menu Supporto, puoi:

- Maneggio ["costo del collegamento"](#)
- Visualizzazione ["Sistema di gestione della rete \(NMS\)"](#) voci
- Maneggio ["filigrane di archiviazione"](#)

Esplora il Tenant Manager

IL ["Responsabile degli inquilini"](#) è l'interfaccia grafica basata sul browser a cui gli utenti tenant accedono per configurare, gestire e monitorare i propri account di archiviazione.



Tenant Manager viene aggiornato a ogni versione e potrebbe non corrispondere agli screenshot di esempio in questa pagina.

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

Dashboard del gestore degli inquilini

Dopo che un amministratore di rete crea un account tenant utilizzando Grid Manager o Grid Management API, gli utenti tenant possono accedere a Tenant Manager.

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

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

Dashboard

16**Buckets**[View buckets](#)**2****Platform services****endpoints**[View endpoints](#)**0****Groups**[View groups](#)**1****User**[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details [?](#)

Name: Tenant02

ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Menù di archiviazione (S3)

Il menu 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 bucket, gestire gli endpoint dei servizi della piattaforma e visualizzare tutte le connessioni di federazione della griglia che sono autorizzati a utilizzare.

Le mie chiavi di accesso

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 inoltre l'accesso completo ai bucket e agli oggetti del tenant, a meno che non siano disabilitate esplicitamente da una policy sui bucket.



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

Secchi

Gli utenti tenant S3 con le autorizzazioni appropriate possono eseguire le seguenti attività per i propri bucket:

- Crea bucket

- Abilita S3 Object Lock per un nuovo bucket (presuppone che S3 Object Lock sia abilitato per il sistema StorageGRID)
- Aggiorna i valori di coerenza
- Abilita e disabilita gli aggiornamenti dell'ultimo orario di accesso
- Abilita o sospendi il controllo delle versioni degli oggetti
- Aggiorna la conservazione predefinita del blocco degli oggetti S3
- Configurare la condivisione delle risorse tra origini (CORS)
- Elimina tutti gli oggetti in un bucket
- Elimina i bucket vuoti
- Utilizzare il ["Consolle S3"](#) per gestire gli oggetti bucket

Se un amministratore di rete ha abilitato l'utilizzo dei servizi della piattaforma per l'account tenant, un utente tenant S3 con le autorizzazioni appropriate può anche eseguire 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 su un bucket S3 esterno.
- Configura l'integrazione della ricerca, che invia i metadati degli oggetti a un indice di ricerca di destinazione ogni volta che un oggetto viene creato, eliminato o i suoi metadati o tag vengono aggiornati.

Endpoint dei servizi della piattaforma

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

Connessioni di federazione della rete

Se un amministratore di griglia ha abilitato l'uso di una connessione di federazione di griglia per l'account tenant, un utente tenant S3 con autorizzazione di accesso Root può visualizzare il nome della connessione, accedere alla pagina dei dettagli del bucket per ciascun bucket con replica tra griglie abilitata e visualizzare l'errore più recente verificatosi durante la replica dei dati del bucket sull'altra griglia nella connessione. Vedere ["Visualizza le connessioni della federazione di griglia"](#) .

Menu Gestione accessi

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

Linee guida per il networking

Linee guida per il networking

Utilizzare queste linee guida per apprendere informazioni sull'architettura e sulle topologie di rete StorageGRID e per apprendere i requisiti per la configurazione e il provisioning della rete.

Informazioni su queste istruzioni

Queste linee guida forniscono informazioni utili per creare l'infrastruttura di rete StorageGRID prima di distribuire 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 e i servizi esterni devono connettersi alle reti StorageGRID per eseguire funzioni come le seguenti:

- Memorizzare e recuperare i dati degli oggetti
- Ricevi notifiche via email
- Accedi all'interfaccia di gestione StorageGRID (Grid Manager e Tenant Manager)
- Accedi alla condivisione di controllo (facoltativo)
- Fornire servizi quali:
 - Protocollo di tempo di rete (NTP)
 - Sistema dei nomi di dominio (DNS)
 - 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 elevato livello di esperienza con la commutazione Ethernet, la rete TCP/IP, le subnet, il routing di rete e i 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 tali reti saranno configurate, è possibile installare e configurare i nodi StorageGRID seguendo le istruzioni appropriate.

Installare i nodi dell'appliance

- ["Installare l'hardware dell'apparecchio"](#)

Installare nodi basati su software

- ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
- ["Installa StorageGRID su Ubuntu o Debian"](#)
- ["Installa StorageGRID su VMware"](#)

Configurare e amministrare il software StorageGRID

- ["Amministra StorageGRID"](#)
- ["Note di rilascio"](#)

Tipi di rete StorageGRID

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

Tipi di traffico

Tipo di traffico	Descrizione	Tipo di rete
Traffico in griglia	Il traffico StorageGRID interno che viaggia tra tutti i nodi della griglia. Tutti i nodi della griglia devono essere in grado di comunicare con tutti gli altri nodi della griglia tramite questa rete.	Rete di griglia (obbligatorio)
Traffico amministrativo	Traffico utilizzato per l'amministrazione e la manutenzione del sistema.	Rete di amministrazione (facoltativa), Rete VLAN (facoltativa)
Traffico clienti	Il traffico che viaggia tra le applicazioni client esterne e la griglia, incluse tutte le richieste di archiviazione di oggetti dai client S3.	Rete client (facoltativa), Rete VLAN (facoltativa)

È possibile configurare la rete nei seguenti modi:

- Solo rete di griglia
- Reti di griglia e di amministrazione
- Reti di griglia e client
- Reti di griglia, amministrazione e client

La rete Grid è obbligatoria 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 ai cambiamenti dei requisiti. Sebbene la rete amministrativa e la rete client siano facoltative, quando si utilizzano queste reti per gestire il traffico amministrativo e client, la rete Grid può essere isolata e protetta.

Le porte interne sono accessibili solo tramite la rete Grid. Le porte esterne sono accessibili da tutti i tipi di rete. Questa flessibilità offre molteplici opzioni per progettare una distribuzione StorageGRID e impostare il filtraggio di IP e porte esterne in switch e firewall. Vedere ["comunicazioni interne del nodo della griglia"](#) E ["comunicazioni esterne"](#).

Interfacce di rete

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

Rete	Nome dell'interfaccia
Rete di griglia (obbligatorio)	eth0
Rete di amministrazione (facoltativa)	eth1
Rete clienti (facoltativa)	eth2

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

Nodi basati su software

- ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
- ["Installa StorageGRID su Ubuntu o Debian"](#)
- ["Installa StorageGRID su VMware"](#)

Nodi dell'appliance

- ["Dispositivo di archiviazione SG6160"](#)
- ["Dispositivo di archiviazione SGF6112"](#)
- ["Dispositivo di archiviazione SG6000"](#)
- ["Dispositivo di archiviazione SG5800"](#)
- ["Dispositivo di archiviazione SG5700"](#)
- ["Apparecchiature di servizio SG110 e SG1100"](#)
- ["Apparecchiature di servizio SG100 e SG1000"](#)

Informazioni di rete per ogni nodo

Per ogni rete abilitata su un nodo è necessario configurare quanto segue:

- indirizzo IP
- Maschera di sottorete
- Indirizzo IP del gateway

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

Gruppi ad alta disponibilità

I gruppi ad alta disponibilità (HA) offrono la possibilità di aggiungere indirizzi IP virtuali (VIP) all'interfaccia Grid o Client Network. Per ulteriori informazioni, consultare ["Gestire gruppi ad alta disponibilità"](#).

Rete a griglia

È richiesta la rete Grid. Viene utilizzato per tutto il traffico StorageGRID interno. La rete Grid fornisce connettività tra tutti i nodi della griglia, in tutti i siti e le sottoreti. Tutti i nodi della rete Grid devono essere in grado di comunicare con tutti gli altri nodi. La rete Grid può essere composta da più subnet. Anche le reti contenenti servizi di griglia critici, come NTP, possono essere aggiunte come subnet di griglia.



StorageGRID non supporta la traduzione degli indirizzi di rete (NAT) 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 amministrativa 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 la rete Grid, è necessario assicurarsi che la rete sia protetta da client non attendibili, come quelli presenti sulla rete Internet aperta.

Si prega di notare i seguenti requisiti e dettagli per il gateway Grid Network:

- Se sono presenti più subnet della griglia, è necessario configurare il gateway della rete di griglia.
- Il gateway Grid Network è il gateway predefinito del nodo finché la configurazione della griglia non è completata.
- Le rotte statiche vengono generate automaticamente per tutti i nodi verso tutte le subnet configurate nell'elenco globale delle subnet della rete Grid.
- Se viene aggiunta una rete client, il gateway predefinito passa dal gateway della rete di griglia al gateway della rete client al termine della configurazione della griglia.

Rete di amministrazione

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

È possibile scegliere su quali nodi della griglia abilitare la rete di amministrazione.

Quando si utilizza la rete di amministrazione, il traffico amministrativo e di manutenzione non deve attraversare la rete Grid. Gli utilizzi tipici della rete di amministrazione includono quanto segue:

- Accesso alle interfacce utente Grid Manager e Tenant Manager.
- Accesso a servizi critici quali server NTP, server DNS, server di gestione delle chiavi esterne (KMS) e server Lightweight Directory Access Protocol (LDAP).
- Accesso ai registri di controllo sui nodi amministrativi.
- Accesso tramite Secure Shell Protocol (SSH) per manutenzione e supporto.

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

Tenere presente i seguenti requisiti e dettagli per il gateway della rete di amministrazione:

- Il gateway della rete amministrativa è necessario se le connessioni verranno effettuate dall'esterno della subnet della rete amministrativa o se sono configurate più subnet della rete amministrativa.
- Vengono create rotte statiche per ogni subnet configurata nell'elenco delle subnet della rete di amministrazione del nodo.

Rete clienti

La rete client è facoltativa. Una volta configurato, viene utilizzato per fornire l'accesso ai servizi di griglia per applicazioni client come S3. Se si prevede di rendere i dati StorageGRID accessibili a una risorsa esterna (ad esempio, un Cloud Storage Pool o il servizio di replica StorageGRID CloudMirror), la risorsa esterna può utilizzare anche la rete client. I nodi della griglia possono comunicare con qualsiasi subnet raggiungibile tramite il gateway della rete client.

È possibile scegliere su quali nodi della griglia abilitare la rete client. Non è necessario che tutti i nodi si trovino sulla stessa rete client e i nodi non comunicheranno mai tra loro tramite la rete client. La rete client non diventa operativa finché non è completata l'installazione della rete.

Per una maggiore sicurezza, è possibile specificare che l'interfaccia di rete client di un nodo non sia attendibile, in modo che la rete client sia più restrittiva riguardo alle connessioni consentite. Se l'interfaccia di rete client 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 bilanciatore del carico. Vedere ["Gestire i controlli del firewall"](#) E ["Configurare gli endpoint del bilanciatore del carico"](#) .

Quando si utilizza una rete client, il traffico client non deve attraversare la rete Grid. Il traffico di rete può essere suddiviso in 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 StorageGRID Load Balancer e l'accesso client S3 alla griglia.
- Nodi di archiviazione, perché questi nodi forniscono l'accesso al protocollo S3, ai pool di archiviazione cloud e al servizio di replica CloudMirror.
- Nodi amministrativi, per garantire che gli utenti tenant possano connettersi al Tenant Manager senza dover utilizzare la rete amministrativa.

Per il gateway della rete client, tenere presente quanto segue:

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

Reti VLAN opzionali

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

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

Se eth0 è configurato come trunk, il traffico della rete Grid scorre sull'interfaccia nativa del trunk, come configurato sullo switch. Allo stesso modo, se eth2 è configurato come trunk e anche la rete client è configurata sullo stesso nodo, la rete client utilizza la VLAN nativa della porta trunk come configurata sullo switch.

Sulle reti VLAN è supportato solo il traffico amministrativo in entrata, come quello utilizzato per SSH, Grid Manager o Tenant Manager. Il traffico in uscita, come quello utilizzato per NTP, DNS, LDAP, KMS e Cloud Storage Pools, non è supportato sulle reti VLAN.



Le interfacce VLAN possono essere aggiunte solo ai nodi amministrativi e ai nodi gateway. Non è possibile utilizzare un'interfaccia VLAN per l'accesso client o amministratore ai nodi di archiviazione.

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 gruppi ad alta disponibilità"](#) per istruzioni e linee guida.

Esempi di topologia di rete

Topologia della rete a griglia

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

Quando si configura la rete Grid, si stabilisce l'indirizzo IP host, la subnet mask e l'indirizzo IP gateway per l'interfaccia eth0 per ciascun nodo Grid.

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

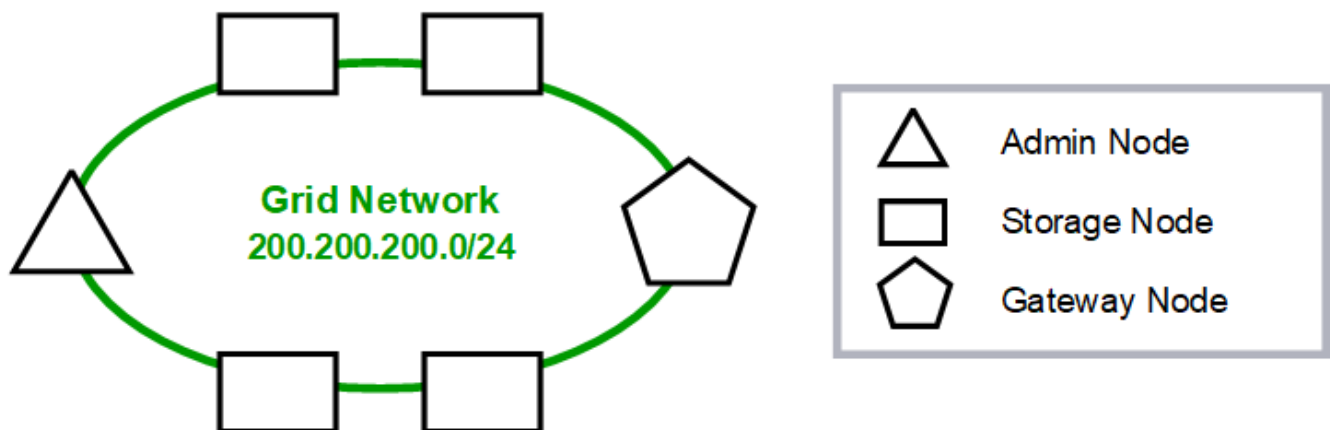
Durante l'installazione, l'interfaccia Grid Network applica percorsi statici per tutte le subnet nel GNSL e imposta il percorso predefinito del nodo sul gateway Grid Network, se configurato. Il GNSL non è richiesto se non è presente una rete client e il gateway della rete Grid è il percorso predefinito del nodo. Vengono generati anche 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 del client S3 e alle funzioni amministrative e di manutenzione.



Questa topologia è adatta per distribuzioni a sito singolo non disponibili esternamente, distribuzioni proof-of-concept o di prova oppure quando un bilanciatore del carico di terze parti funge da limite di accesso client. Quando possibile, la rete Grid dovrebbe essere utilizzata esclusivamente per il traffico interno. Sia la rete amministrativa che la rete client presentano ulteriori restrizioni firewall che bloccano il traffico esterno verso i servizi interni. È supportato l'utilizzo della Grid Network per il traffico client esterno, ma questo utilizzo offre meno livelli di protezione.

Topology example: Grid Network only



*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

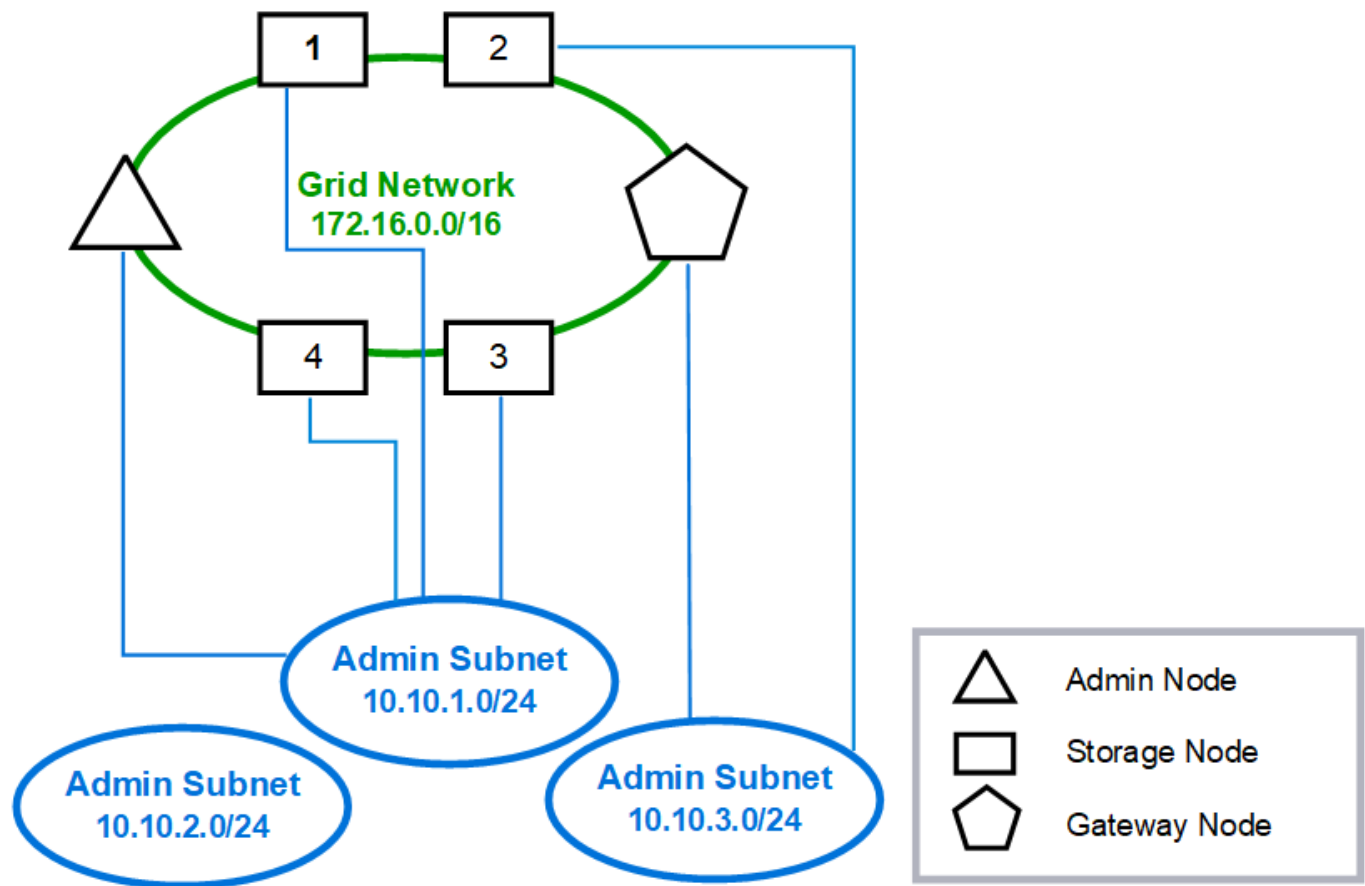
Avere una rete di amministrazione è facoltativo. Un modo per utilizzare una rete amministrativa e una rete a griglia è configurare una rete a griglia inostradabile e una rete amministrativa delimitata per ciascun nodo.

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

La rete di amministrazione può essere univoca per ciascun nodo e può essere composta da più subnet. Ogni nodo può essere configurato con un Admin External Subnet List (AESL). L'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 accederà tramite la rete di amministrazione, come NTP, DNS, KMS e LDAP. Per ogni subnet nell'AESL vengono applicati percorsi statici.

In questo esempio, la rete Grid viene utilizzata per il traffico correlato alle richieste del client S3 e alla gestione degli oggetti, mentre la rete Admin viene utilizzata per le funzioni amministrative.

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

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

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

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

Topologia della rete client

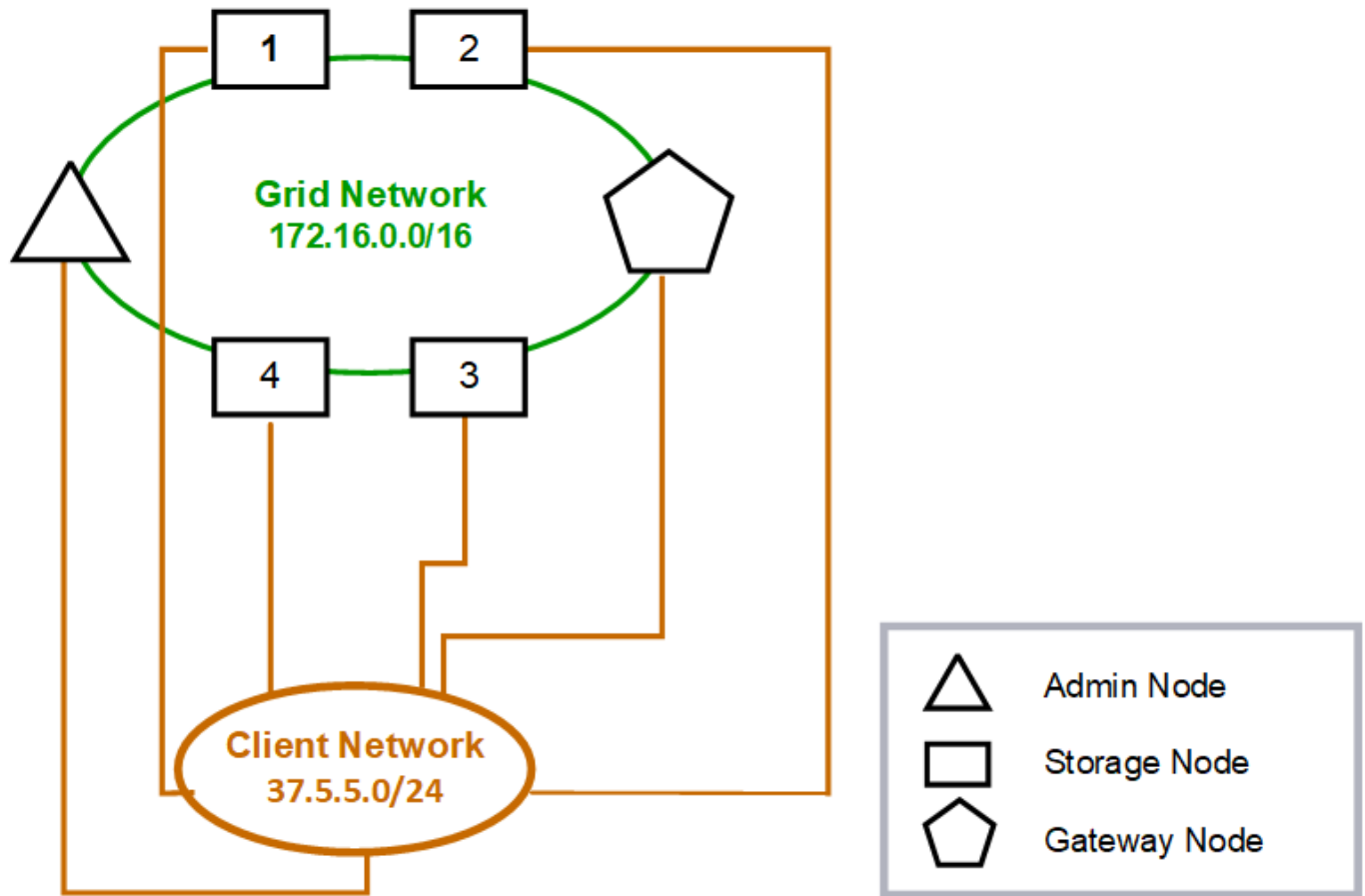
Avere una rete di clienti è facoltativo. L'utilizzo di una rete client consente di separare il traffico di rete client (ad esempio, S3) dal traffico interno alla griglia, rendendo così la rete della griglia più sicura. Quando la rete amministrativa non è configurata, il traffico amministrativo può essere gestito dalla rete client o dalla rete Grid.

Quando si configura la rete client, si stabilisce 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 della rete di griglia al gateway della rete client al termine dell'installazione. Se in seguito viene aggiunta una rete client, il gateway predefinito del nodo cambia nello stesso modo.

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

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

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

System Generated

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

Informazioni correlate

["Modifica la configurazione della rete del nodo"](#)

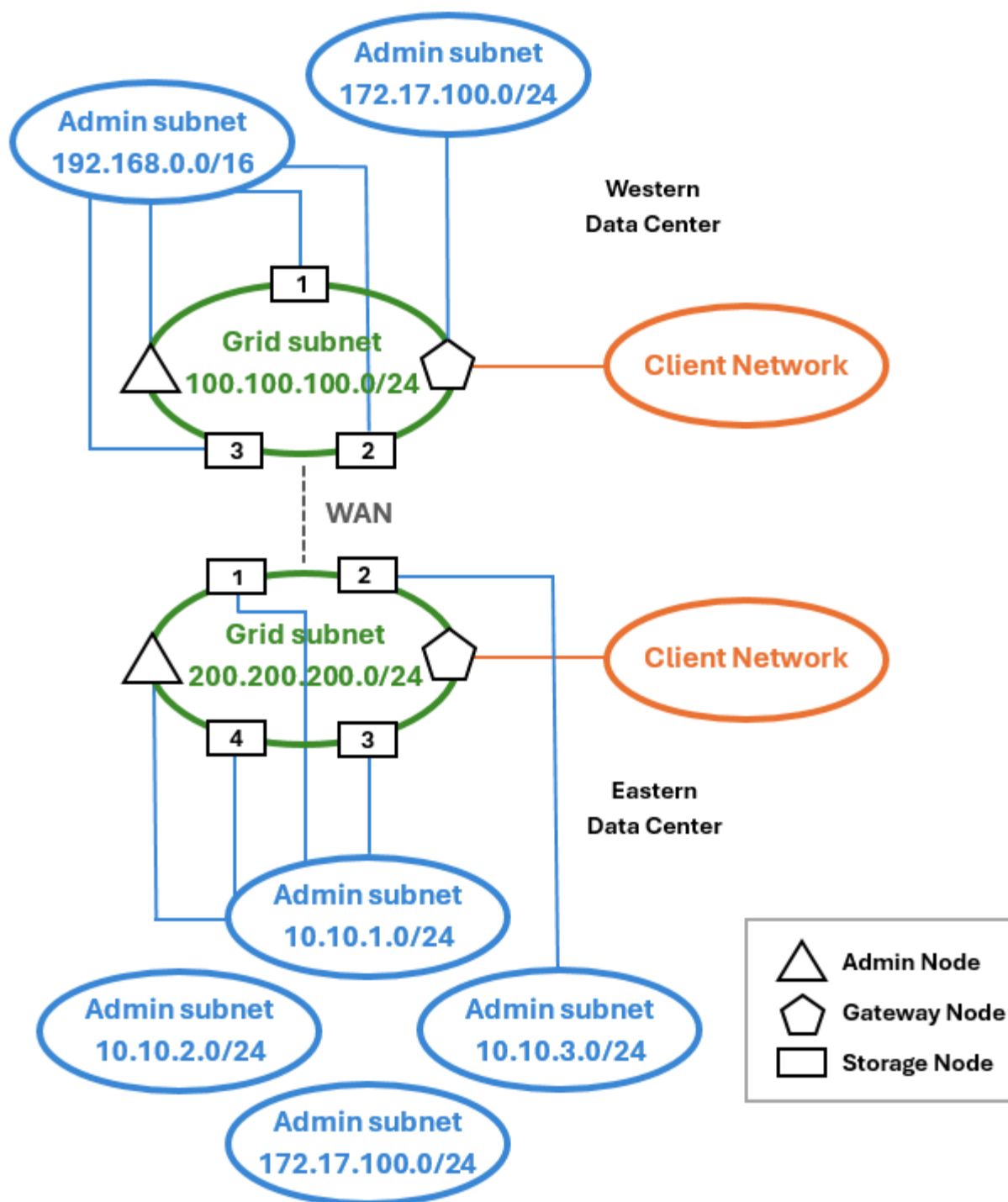
Topologia per tutte e tre le reti

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

In questo esempio:

- La rete Grid viene utilizzata per il traffico di rete correlato alle operazioni di gestione degli oggetti interni.
- La rete amministrativa viene utilizzata per il traffico correlato alle funzioni amministrative.
- La rete client viene utilizzata per il traffico correlato alle richieste client S3.

Esempio di topologia: reti Grid, Admin e Client



Requisiti di rete

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

Requisiti generali di rete

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

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

- **Connessioni di gestione:** connessioni in entrata da un amministratore al nodo, solitamente tramite SSH. Accesso tramite browser Web a Grid Manager, Tenant Manager e StorageGRID Appliance Installer.
- **Connessioni al server NTP:** connessione UDP in uscita che riceve una risposta UDP in ingresso.

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

- **Connessioni al server DNS:** connessione UDP in uscita che riceve una risposta UDP in ingresso.
- **Connessioni al server LDAP/Active Directory:** connessione TCP in uscita dal servizio Identity sui nodi di archiviazione.
- * AutoSupport*: Connessione TCP in uscita dai nodi di amministrazione a `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 abilitata.
- Connessioni TCP in entrata dai client S3.
- Richieste in uscita dai servizi della piattaforma StorageGRID, come la replica di CloudMirror o dai pool di archiviazione cloud.

Se StorageGRID non riesce a contattare nessuno dei server NTP o DNS forniti utilizzando le regole di routing predefinite, tenterà automaticamente il contatto su tutte le reti (Grid, Admin e Client) a condizione che siano specificati gli indirizzi IP dei server DNS e NTP. Se i server NTP o DNS sono raggiungibili su qualsiasi rete, StorageGRID creerà automaticamente regole di routing aggiuntive per garantire che tale rete venga utilizzata per tutti i futuri tentativi di connessione.



Sebbene sia possibile utilizzare questi percorsi host rilevati automaticamente, in genere è opportuno configurare manualmente i percorsi DNS e NTP per garantire la connettività nel caso in cui il rilevamento automatico fallisca.

Se non si è pronti a configurare le reti client e di amministrazione facoltative durante la distribuzione, è possibile configurare queste reti quando si approvano i nodi della griglia durante i passaggi di configurazione. Inoltre, è possibile configurare queste reti dopo l'installazione, utilizzando lo strumento Cambia IP (vedere "[Configurare gli indirizzi IP](#)").

Sono supportate solo le connessioni client S3 e le connessioni amministrative SSH, Grid Manager e Tenant Manager sulle interfacce VLAN. Le connessioni in uscita, ad esempio verso i server NTP, DNS, LDAP, AutoSupport e KMS, devono passare direttamente attraverso le interfacce Client, Admin o Grid Network. Se l'interfaccia è configurata come trunk per supportare le interfacce VLAN, questo traffico scorrerà sulla VLAN nativa dell'interfaccia, come configurato sullo switch.

Reti WAN (Wide Area Network) per più siti

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

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

Connessioni per nodi amministrativi e nodi gateway

I nodi amministrativi devono essere sempre protetti da client non attendibili, come quelli presenti su Internet aperto. È necessario assicurarsi che nessun client non attendibile possa accedere ad alcun nodo di amministrazione sulla rete Grid, sulla rete di amministrazione o sulla rete client.

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

Utilizzo della traduzione degli indirizzi di rete (NAT)

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

Requisiti specifici della rete

Seguire i requisiti per ogni 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 gateway diverso da 0.0.0.0.
- Se non si dispone di un gateway, la procedura consigliata è quella di impostare l'indirizzo del gateway come indirizzo IP dell'interfaccia di rete.

Sottoreti



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

Durante la distribuzione, Grid Manager applica le seguenti restrizioni. Vengono forniti qui per assistere nella pianificazione della rete prima dell'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 di interfaccia di rete e da una subnet mask (CIDR) non può sovrapporsi alla subnet di nessun'altra interfaccia configurata sullo stesso nodo.
- Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete amministrativa 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 sottorete della rete Grid per ciascun nodo deve essere inclusa nel GNSL.
- La subnet della rete amministrativa non può sovrapporsi alla subnet della rete Grid, alla subnet della rete client o a qualsiasi subnet nel GNSL.
- Le subnet nell'AESL non possono sovrapporsi ad alcuna subnet nel GNSL.
- La subnet della rete client non può sovrapporsi alla subnet della rete Grid, alla subnet della rete amministrativa, a nessuna subnet nel GNSL o a nessuna subnet nell'AESL.

Rete a griglia

- Al momento della distribuzione, ogni nodo della griglia deve essere collegato alla rete della griglia e deve essere in grado di comunicare con il nodo di amministrazione primario utilizzando la configurazione di rete specificata durante la distribuzione del nodo.
- Durante il normale funzionamento della rete, ogni nodo della rete deve essere in grado di comunicare con tutti gli altri nodi della rete tramite la rete stessa.



La rete Grid deve essere direttamente instradabile tra ciascun nodo. La traduzione degli indirizzi di rete (NAT) tra nodi non è supportata.

- Se la rete Grid è composta da più subnet, aggiungerle all'elenco delle subnet della rete Grid (GNSL). Le rotte statiche vengono create su tutti i nodi per ogni sottorete 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.

Rete di amministrazione

La rete di amministrazione è facoltativa. Se si prevede di configurare una rete di amministrazione, seguire questi requisiti e linee guida.

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



La rete di amministrazione e l'AESL possono essere univoche per ciascun nodo, purché i servizi di rete e i client desiderati siano raggiungibili.



È necessario definire almeno una subnet sulla rete di amministrazione per abilitare le connessioni in entrata da subnet esterne. Le rotte statiche vengono generate automaticamente su ciascun nodo per ciascuna sottorete nell'AESL.

Rete clienti

La rete client è facoltativa. Se si prevede di configurare una rete client, tenere presente le seguenti considerazioni.

- La rete client è progettata per supportare il traffico proveniente dai client S3. Se configurato, il gateway della 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 sugli endpoint del bilanciatore del carico configurati in modo esplicito. Vedere ["Configurare gli endpoint del bilanciatore 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 della rete client scorrerà sulla VLAN nativa del trunk, come configurato nello switch.

Informazioni correlate

["Modifica la configurazione della rete del nodo"](#)

Considerazioni sulla rete specifiche per l'implementazione

Distribuzioni Linux

Per garantire efficienza, affidabilità e sicurezza, il sistema StorageGRID funziona su Linux come una raccolta di motori di container. In un sistema StorageGRID non è richiesta la configurazione di rete relativa al motore del contenitore.

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



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

Vedere le istruzioni di installazione per ["Red Hat Enterprise Linux"](#) O ["Ubuntu o Debian"](#) distribuzioni.

Configurazione della rete host per le distribuzioni del motore del contenitore

Prima di avviare la distribuzione di StorageGRID su una piattaforma di motore di container, determina quali reti (Grid, Admin, Client) utilizzerà 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 larghezza di banda sufficiente.

Host fisici

Se si utilizzano host fisici per supportare i nodi della griglia:

- Assicurarsi che tutti gli host utilizzino la stessa interfaccia host per ogni interfaccia nodo. Questa strategia

semplifica la configurazione dell'host e consente la futura migrazione dei nodi.

- Ottenere un indirizzo IP per l'host fisico stesso.



Un'interfaccia fisica sull'host può essere utilizzata dall'host stesso e da uno o più nodi in esecuzione sull'host. Tutti 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 richieste all'host.
- Se si intende utilizzare le interfacce VLAN in StorageGRID, l'host deve disporre di una o più interfacce trunk che forniscano l'accesso alle VLAN desiderate. Queste interfacce possono essere passate al contenitore del nodo come eth0, eth2 o come interfacce aggiuntive. Per aggiungere interfacce trunk o 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: aggiungere interfacce trunk o di accesso a un nodo"](#)

Raccomandazioni sulla larghezza di banda minima

Nella tabella seguente sono riportate le raccomandazioni minime sulla larghezza di banda LAN per ciascun tipo di nodo StorageGRID e ciascun tipo di rete. È necessario fornire a ciascun host fisico o virtuale una larghezza di banda di rete sufficiente a soddisfare i requisiti minimi aggregati di larghezza di banda per il numero totale e il tipo di nodi StorageGRID che si prevede di eseguire su tale host.

Tipo di nodo	Tipo di rete		
	Griglia	Amministratore	Cliente
	Larghezza di banda LAN minima	Amministratore	10 Gbps
1 Gbps	1 Gbps	Portale	10 Gbps
1 Gbps	10 Gbps	Magazzinaggio	10 Gbps
1 Gbps	10 Gbps	Archivio	10 Gbps



Questa tabella non include la larghezza di banda 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 predisporre interfacce fisiche separate su ciascun host per garantire una larghezza di banda SAN sufficiente. Per evitare di introdurre un collo di bottiglia, la larghezza di banda SAN per un dato host dovrebbe corrispondere approssimativamente alla larghezza di banda di rete aggregata del nodo di archiviazione per tutti i nodi di archiviazione in esecuzione su quell'host.

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

Ad esempio, per eseguire un nodo di amministrazione, un nodo gateway e un nodo di archiviazione su un

singolo host:

- Collegare la rete e le reti amministrative sul nodo amministrativo (richiede $10 + 1 = 11$ Gbps)
- Collegare la rete e le reti client sul nodo gateway (richiede $10 + 10 = 20$ Gbps)
- Collegare la rete di rete al nodo di archiviazione (richiede 10 Gbps)

In questo scenario, dovresti fornire un minimo di $11 + 20 + 10 = 41$ Gbps di larghezza di banda di rete, che potrebbe essere soddisfatta da due interfacce da 40 Gbps o cinque interfacce da 10 Gbps, potenzialmente aggregate in trunk 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 nel cluster StorageGRID per preparare la distribuzione StorageGRID, vedere 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 pool di archiviazione cloud

Se si prevede di utilizzare i servizi della piattaforma StorageGRID o i pool di archiviazione cloud, è necessario configurare la rete grid e i firewall per garantire che gli endpoint di destinazione siano raggiungibili.

Networking per servizi di piattaforma

Come descritto in ["Gestire i servizi della piattaforma per gli inquilini"](#) E ["Gestire i servizi della piattaforma"](#), i servizi della piattaforma includono servizi esterni che forniscono integrazione di ricerca, notifica di eventi e replica CloudMirror.

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

- Sui nodi di archiviazione con servizi ADC, configurare reti amministrative univoche con voci AESL che instradano verso gli endpoint di destinazione.
- Affidati al percorso predefinito fornito da una rete client. Se si utilizza il percorso predefinito, è possibile utilizzare ["funzionalità di rete client non attendibile"](#) per limitare le connessioni in entrata.

Networking per pool di archiviazione cloud

I pool di archiviazione cloud richiedono inoltre l'accesso dai nodi di archiviazione agli endpoint forniti dal servizio esterno utilizzato, ad esempio Amazon S3 Glacier o Microsoft Azure Blob Storage. Per informazioni, vedere ["Che cos'è un Cloud Storage Pool"](#).

Porte per servizi di piattaforma e pool di archiviazione cloud

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

- **80:** Per gli URI degli endpoint che iniziano con `http`
- **443:** Per gli URI degli 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 archiviazione"](#) per consentire l'invio di messaggi a endpoint esterni, ad esempio un endpoint su Internet.

VLAN e servizi di piattaforma e pool di archiviazione cloud

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

Nodi dell'appliance

È possibile configurare le porte di rete sugli appliance StorageGRID per utilizzare le modalità di associazione delle porte che soddisfano i requisiti di throughput, ridondanza e failover.

Le porte 10/25-GbE sugli apparecchi StorageGRID possono essere configurate in modalità di collegamento fisso o aggregato per le connessioni alla rete di rete e alla rete client.

Le porte della rete amministrativa da 1 GbE possono essere configurate in modalità indipendente o attiva-backup per le connessioni alla rete amministrativa.

Consultare le informazioni sulle modalità di collegamento delle porte per il proprio apparecchio:

- ["Modalità di collegamento delle porte \(SG6160\)"](#)
- ["Modalità di legame delle porte \(SGF6112\)"](#)
- ["Modalità di collegamento delle porte \(controller SG6000-CN\)"](#)
- ["Modalità di collegamento delle porte \(controller SG5800\)"](#)
- ["Modalità di collegamento delle porte \(controller E5700SG\)"](#)
- ["Modalità di collegamento delle porte \(SG110 e SG1100\)"](#)
- ["Modalità di collegamento delle porte \(SG100 e SG1000\)"](#)

Installazione e provisioning della rete

È necessario comprendere come vengono utilizzate la rete Grid e le reti Admin e Client opzionali durante la distribuzione dei nodi e la configurazione della griglia.

Distribuzione iniziale di un nodo

Quando si distribuisce un nodo per la prima volta, è necessario collegarlo alla rete Grid e assicurarsi che abbia accesso al nodo di amministrazione primario. Se la rete Grid è isolata, è possibile configurare la rete di amministrazione sul nodo di amministrazione 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 la distribuzione. Il gateway predefinito consente ai nodi della griglia su subnet separate di comunicare con il nodo di amministrazione primario prima che la griglia sia stata configurata.

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

Registrazione automatica del nodo con il nodo amministratore primario

Dopo essere stati distribuiti, i nodi si registrano presso il nodo di amministrazione primario tramite la rete Grid. È quindi possibile utilizzare Grid Manager, il `configure-storagegrid.py` Script Python o API di installazione per configurare la griglia e approvare i nodi registrati. Durante la configurazione della griglia, è possibile configurare più subnet della griglia. Una volta completata la configurazione della griglia, su ciascun nodo verranno creati percorsi statici verso queste subnet tramite il gateway Grid Network.

Disabilitazione della rete amministrativa o della rete client

Se si desidera disabilitare la rete amministrativa o la rete client, è possibile rimuovere la configurazione da esse durante il processo di approvazione del nodo oppure è possibile utilizzare lo strumento Modifica IP al termine dell'installazione (vedere "[Configurare gli indirizzi IP](#)").

Linee guida post-installazione

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

- Se è stato utilizzato DHCP per assegnare gli indirizzi IP, configurare una prenotazione DHCP per ciascun indirizzo IP sulle reti utilizzate.

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



I nodi si riavviano quando la configurazione della rete Grid viene modificata da DHCP, il che può causare interruzioni se una modifica DHCP interessa più nodi contemporaneamente.

- È necessario utilizzare le procedure di modifica IP se si desidera modificare gli indirizzi IP, le maschere di sottorete e i gateway predefiniti per un nodo della griglia. Vedere "[Configurare gli indirizzi IP](#)".
- Se si apportano modifiche alla configurazione di rete, tra cui 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 apportate alla rete, potrebbe essere necessario ristabilire queste connessioni.

Riferimento porta di rete

Comunicazioni interne al nodo della griglia

Il firewall interno StorageGRID consente connessioni in entrata a porte specifiche sulla rete Grid. Le connessioni sono accettate anche sulle porte definite dagli endpoint del bilanciatore del carico.



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

Oltre a ICMP e alle porte elencate nella tabella, StorageGRID utilizza il protocollo VRRP (Virtual Router Redundancy Protocol). 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 aziendale limitano l'accesso a una qualsiasi di queste porte, è possibile rimappare le porte al momento della distribuzione utilizzando un parametro di configurazione della distribuzione. Per ulteriori informazioni sulla rimappatura delle porte e sui parametri di configurazione della distribuzione, vedere:

- ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
- ["Installa StorageGRID su Ubuntu o Debian"](#)

Linee guida per i nodi basati su VMware

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

Se i criteri di rete aziendale limitano l'accesso a una qualsiasi di queste porte, è possibile rimappare le porte quando si distribuiscono i nodi tramite VMware vSphere Web Client oppure utilizzando un'impostazione del file di configurazione durante l'automazione della distribuzione dei nodi della griglia. Per ulteriori informazioni sulla rimappatura delle porte e sui parametri di configurazione della distribuzione, vedere ["Installa StorageGRID su VMware"](#).

Linee guida per i nodi dell'appliance

Se i criteri di rete aziendale limitano l'accesso a una qualsiasi di queste porte, è possibile rimappare le porte utilizzando StorageGRID Appliance Installer. Vedere ["Facoltativo: rimappare le porte di rete per l'appliance"](#).

Porte interne StorageGRID

Porta	TCP o UDP	Da	A	Dettagli
22	TCP	Nodo di amministrazione 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 tramite SSH sulla porta 22. Consentire il traffico SSH da altri nodi è facoltativo.
80	TCP	Elettrodomestici	Nodo di amministrazione primario	Utilizzato dagli apparecchi StorageGRID per comunicare con il nodo di amministrazione primario per avviare l'installazione.
123	UDP	Tutti i nodi	Tutti i nodi	Servizio di protocollo di tempo di rete. Ogni nodo sincronizza il proprio orario con quello di tutti gli altri nodi tramite NTP.
443	TCP	Tutti i nodi	Nodo di amministrazione 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 di amministrazione primario	Traffico interno per installazione, ampliamento, ripristino e altre procedure di manutenzione.

Porta	TCP o UDP	Da	A	Dettagli
1139	TCP	Nodi di archiviazione	Nodi di archiviazione	Traffico interno tra nodi di archiviazione.
1501	TCP	Tutti i nodi	Nodi di archiviazione e con ADC	Segnalazione, controllo e configurazione del traffico interno.
1502	TCP	Tutti i nodi	Nodi di archiviazione	Traffico interno correlato a S3 e Swift.
1504	TCP	Tutti i nodi	Nodi amministrativi	Traffico interno di configurazione e segnalazione del servizio NMS.
1505	TCP	Tutti i nodi	Nodi amministrativi	Traffico interno del servizio AMS.
1506	TCP	Tutti i nodi	Tutti i nodi	Traffico interno sullo stato del server.
1507	TCP	Tutti i nodi	Nodi gateway	Traffico interno del bilanciatore del carico.
1508	TCP	Tutti i nodi	Nodo di amministrazione primario	Traffico interno di gestione della configurazione.
1511	TCP	Tutti i nodi	Nodi di archiviazione	Traffico interno dei metadati.
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 archiviazione	Nodi di archiviazione	Comunicazione tra cluster TLS Cassandra.

Porta	TCP o UDP	Da	A	Dettagli
7443	TCP	Tutti i nodi	Nodo di amministrazione primario	Traffico interno per installazione, espansione, ripristino, altre procedure di manutenzione e segnalazione di errori.
8011	TCP	Tutti i nodi	Nodo di amministrazione primario	Traffico interno per installazione, ampliamento, ripristino e altre procedure di manutenzione.
8443	TCP	Nodo di amministrazione primario	Nodi dell'applicazione	Traffico interno correlato alla procedura di modalità di manutenzione.
9042	TCP	Nodi di archiviazione	Nodi di archiviazione	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 archiviazione	Nodo di amministrazione primario	Utilizzato dagli apparecchi StorageGRID per inoltrare i pacchetti AutoSupport da E-Series SANtricity System Manager al nodo di amministrazione primario.
10342	TCP	Tutti i nodi	Nodo di amministrazione primario	Traffico interno per installazione, ampliamento, ripristino e altre procedure di manutenzione.
18000	TCP	Nodi di amministrazione/archiviazione	Nodi di archiviazione e con ADC	Traffico interno del servizio di account.
18001	TCP	Nodi di amministrazione/archiviazione	Nodi di archiviazione e con ADC	Traffico interno della federazione delle identità.
18002	TCP	Nodi di amministrazione/archiviazione	Nodi di archiviazione	Traffico API interno correlato ai protocolli degli oggetti.

Porta	TCP o UDP	Da	A	Dettagli
18003	TCP	Nodi di amministrazione/archiviazione	Nodi di archiviazione e con ADC	Traffico interno dei servizi della piattaforma.
18017	TCP	Nodi di amministrazione/archiviazione	Nodi di archiviazione	Traffico interno del servizio Data Mover per i pool di archiviazione cloud.
18019	TCP	Tutti i nodi	Tutti i nodi	Traffico interno del servizio Chunk per la codifica di cancellazione e la replicazione
18082	TCP	Nodi di amministrazione/archiviazione	Nodi di archiviazione	Traffico interno correlato a S3.
18083	TCP	Tutti i nodi	Nodi di archiviazione	Traffico interno correlato a Swift.
18086	TCP	Tutti i nodi	Nodi di archiviazione	Traffico interno correlato al servizio LDR.
18200	TCP	Nodi di amministrazione/archiviazione	Nodi di archiviazione	Statistiche aggiuntive sulle richieste dei clienti.
19000	TCP	Nodi di amministrazione/archiviazione	Nodi di archiviazione e con ADC	Traffico interno del servizio Keystone .

Informazioni correlate

["Comunicazioni esterne"](#)

Comunicazioni esterne

I client devono comunicare con i nodi della griglia per acquisire e recuperare i contenuti. Le porte utilizzate dipendono dai protocolli di archiviazione degli oggetti scelti. Queste porte devono essere accessibili al client.

Accesso limitato ai porti

Se i criteri di rete aziendale limitano l'accesso a una qualsiasi delle porte, è possibile procedere in uno dei seguenti modi:

- Utilizzo ["endpoint del bilanciatore del carico"](#) per consentire l'accesso alle porte definite dall'utente.
- Riassegnare le porte durante la distribuzione dei nodi. Tuttavia, non dovresti rimappare gli endpoint del bilanciatore del carico. Consulta le informazioni sulla rimappatura delle porte per il tuo nodo StorageGRID :
 - ["Chiavi di rimappatura delle porte per StorageGRID su Red Hat Enterprise Linux"](#)
 - ["Chiavi di rimappatura delle porte per StorageGRID su Ubuntu o Debian"](#)
 - ["Riassegna le porte per StorageGRID su VMware"](#)
 - ["Facoltativo: rimappare le porte di rete per l'appliance"](#)

Porte utilizzate per le comunicazioni esterne

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



Questo elenco non include le porte che potrebbero essere configurate come ["endpoint del bilanciatore del carico"](#).

Porta	TCP o UDP	Protocollo	Da	A	Dettagli
22	TCP	SSH	Computer portatile di servizio	Tutti i nodi	Per le procedure con passaggi della console è richiesto l'accesso SSH o alla console. Facoltativamente, è possibile utilizzare la porta 2022 anziché la 22.
25	TCP	SMTP	Nodi amministrativi	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 facoltativamente per supportare la configurazione di rete basata su DHCP. Il servizio dhclient non funziona per le griglie configurate staticamente.
68	UDP	DHCP	Servizio DHCP	Tutti i nodi	Utilizzato facoltativamente per supportare la configurazione di rete basata su DHCP. Il servizio dhclient non funziona per le griglie che utilizzano indirizzi IP statici.
80	TCP	HTTP	Navigatore	Nodi amministrativi	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	Navigatore	Elettrodomestici	La porta 80 reindirizza alla porta 8443 per StorageGRID Appliance Installer.
80	TCP	HTTP	Nodi di archiviazione con ADC	AWS	Utilizzato per i messaggi dei servizi di piattaforma inviati ad AWS o ad altri servizi esterni che utilizzano HTTP. I tenant possono ignorare l'impostazione predefinita della porta HTTP 80 durante la creazione di un endpoint.
80	TCP	HTTP	Nodi di archiviazione	AWS	Richieste di Cloud Storage Pool inviate a destinazioni AWS che utilizzano HTTP. Gli amministratori della griglia possono ignorare l'impostazione predefinita della porta HTTP 80 durante la configurazione di un Cloud Storage Pool.
111	TCP/UDP	RPCBind	Cliente NFS	Nodi amministrativi	Utilizzato dall'esportazione di audit basata su NFS (portmap). Nota: questa porta è richiesta solo se è abilitata l'esportazione di audit basata su NFS. Nota: il supporto per NFS è stato deprecato e verrà rimosso in una versione futura.
123	UDP	NTP	Nodi NTP primari	NTP esterno	Servizio di protocollo di tempo di rete. I nodi selezionati come sorgenti NTP primarie sincronizzano anche gli orari degli orologi con le sorgenti NTP esterne.
161	TCP/UDP	SNMP	Cliente SNMP	Tutti i nodi	Utilizzato per il polling SNMP. Tutti i nodi forniscono informazioni di base; i nodi amministrativi forniscono anche dati di avviso. Se configurato, il valore predefinito è la porta UDP 161. Nota: questa porta è obbligatoria e viene aperta sul firewall del nodo solo se è configurato SNMP. Se si prevede di utilizzare SNMP, è possibile configurare porte alternative. Nota: per informazioni sull'utilizzo di SNMP con StorageGRID, contattare il rappresentante dell'account NetApp .

Porta	TCP o UDP	Protocollo	Da	A	Dettagli
162	TCP/UDP	Notifiche SNMP	Tutti i nodi	Destinazioni di notifica	Le notifiche e le trap SNMP in uscita vengono impostate per impostazione predefinita sulla porta UDP 162. Nota: questa porta è necessaria solo se SNMP è abilitato e sono configurate le destinazioni di notifica. Se si prevede di utilizzare SNMP, è possibile configurare porte alternative. Nota: per informazioni sull'utilizzo di SNMP con StorageGRID, contattare il rappresentante dell'account NetApp .
389	TCP/UDP	LDAP	Nodi di archiviazione con ADC	Directory attiva/LDAP	Utilizzato per la connessione a un server Active Directory o LDAP per la federazione delle identità.
443	TCP	HTTPS	Navigatore	Nodi amministrativi	Utilizzato dai browser Web e dai client API di gestione per accedere a Grid Manager e Tenant Manager. Nota: se chiudi le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi su una porta bloccata, incluso te, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati. Fare riferimento a "Configurare i controlli del firewall" per configurare indirizzi IP privilegiati.
443	TCP	HTTPS	Nodi amministrativi	Directory attiva	Utilizzato dai nodi di amministrazione che si connettono ad Active Directory se è abilitato l'accesso singolo (SSO).
443	TCP	HTTPS	Nodi di archiviazione con ADC	AWS	Utilizzato per i messaggi dei servizi di piattaforma inviati ad AWS o ad altri servizi esterni che utilizzano HTTPS. I tenant possono sovrascrivere l'impostazione predefinita della porta HTTP 443 durante la creazione di un endpoint.
443	TCP	HTTPS	Nodi di archiviazione	AWS	Richieste di Cloud Storage Pool inviate a destinazioni AWS che utilizzano HTTPS. Gli amministratori della griglia possono ignorare l'impostazione predefinita della porta HTTPS 443 durante la configurazione di un Cloud Storage Pool.

Porta	TCP o UDP	Protocollo	Da	A	Dettagli
903	TCP	NFS	Cliente NFS	Nodi amministrativi	Utilizzato dall'esportazione di audit basata su NFS(<code>rpc.mountd</code>). Nota: questa porta è richiesta solo se è abilitata l'esportazione di audit basata su NFS. Nota: il supporto per NFS è stato deprecato e verrà rimosso in una versione futura.
2022	TCP	SSH	Computer portatile di servizio	Tutti i nodi	Per le procedure con passaggi della console è richiesto l'accesso SSH o alla console. Facoltativamente, è possibile utilizzare la porta 22 anziché la 2022.
2049	TCP	NFS	Cliente NFS	Nodi amministrativi	Utilizzato dall'esportazione di audit basata su NFS (<code>nfs</code>). Nota: questa porta è richiesta solo se è abilitata l'esportazione di audit basata su NFS. Nota: il supporto per NFS è stato deprecato 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	Apparecchio	Chilometri	Traffico esterno del protocollo KMIP (Key Management Interoperability Protocol) dagli apparecchi configurati per la crittografia dei nodi al Key Management Server (KMS), a meno che non venga specificata una porta diversa nella pagina di configurazione KMS del programma di installazione dell'apparecchio StorageGRID .
8022	TCP	SSH	Computer portatile di servizio	Tutti i nodi	SSH sulla porta 8022 garantisce l'accesso al sistema operativo di base sulle piattaforme appliance e nodi virtuali per supporto e risoluzione dei problemi. Questa porta non viene utilizzata per i nodi basati su Linux (bare metal) e non è necessario che sia accessibile tra i nodi della griglia o durante le normali operazioni.

Porta	TCP o UDP	Protocollo	Da	A	Dettagli
8443	TCP	HTTPS	Navigatore	Nodi amministrativi	Opzionale. Utilizzato dai browser Web e dai client API di gestione per accedere a Grid Manager. Può essere utilizzato per separare le comunicazioni tra Grid Manager e Tenant Manager. Nota: se chiudi le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi su una porta bloccata, incluso te, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati. Fare riferimento a "Configurare i controlli del firewall" per configurare indirizzi IP privilegiati.
8443	TCP	HTTPS	Navigatore	Elettrodomestici	Utilizzato dai browser Web e dai client API di gestione per accedere al programma di installazione dell'appliance StorageGRID . Nota: la porta 443 reindirizza alla porta 8443 per StorageGRID Appliance Installer.
9022	TCP	SSH	Computer portatile di servizio	Elettrodomestici	Concede l'accesso agli apparecchi StorageGRID in modalità di preconfigurazione per supporto e 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 amministrativi	Utilizzato dai servizi Grafana esterni per l'accesso sicuro al servizio StorageGRID Prometheus. Nota: questa porta è richiesta solo se è abilitato l'accesso Prometheus basato su certificato.
9092	TCP	Kafka	Nodi di archiviazione con ADC	Cluster di Kafka	Utilizzato per i messaggi dei servizi di piattaforma inviati a un cluster Kafka. I tenant possono sovrascrivere l'impostazione predefinita della porta Kafka pari a 9092 durante la creazione di un endpoint.
9443	TCP	HTTPS	Navigatore	Nodi amministrativi	Opzionale. Utilizzato dai browser Web e dai client API di gestione per accedere a Tenant Manager. Può essere utilizzato per separare le comunicazioni tra Grid Manager e Tenant Manager.

Porta	TCP o UDP	Protocollo	Da	A	Dettagli
18082	TCP	HTTPS	Clienti S3	Nodi di archiviazione	Traffico client S3 direttamente ai nodi di archiviazione (HTTPS).
18083	TCP	HTTPS	Clienti rapidi	Nodi di archiviazione	Traffico client rapido direttamente ai nodi di archiviazione (HTTPS).
18084	TCP	HTTP	Clienti S3	Nodi di archiviazione	Traffico client S3 direttamente ai nodi di archiviazione (HTTP).
18085	TCP	HTTP	Clienti rapidi	Nodi di archiviazione	Traffico client rapido direttamente ai nodi di archiviazione (HTTP).
23000-23999	TCP	HTTPS	Tutti i nodi sulla griglia di origine per la replica tra griglie	Nodi amministrativi e nodi gateway sulla griglia di destinazione per la replica tra griglie	Questo intervallo di porte è riservato alle connessioni della federazione di rete. Entrambe le griglie in una determinata connessione utilizzano la stessa porta.

Avvio rapido per StorageGRID

Per configurare e utilizzare qualsiasi sistema StorageGRID , seguire questi passaggi generali.

1

Impara, pianifica e raccogli dati

Rivolgiti al tuo rappresentante NetApp per comprendere le opzioni e pianificare il tuo nuovo sistema StorageGRID . Prendi in considerazione questi tipi di domande:

- Quanti dati oggetto prevedi di archiviare inizialmente e nel tempo?
- Di quanti siti hai bisogno?
- Quanti e quali tipi di nodi sono necessari in ogni sito?
- Quali reti StorageGRID utilizzerai?
- Chi utilizzerà la tua griglia per immagazzinare oggetti? Quali applicazioni utilizzeranno?
- Hai esigenze particolari in termini di sicurezza o di stoccaggio?
- Devi rispettare dei requisiti legali o normativi?

Facoltativamente, puoi rivolgerti al tuo consulente NetApp Professional Services per accedere allo strumento NetApp ConfigBuilder e compilare una cartella di lavoro di configurazione da utilizzare durante l'installazione e la distribuzione del nuovo sistema. È possibile utilizzare questo strumento anche per automatizzare la configurazione di qualsiasi appliance StorageGRID. Vedere ["Automatizza l'installazione e la configurazione degli elettrodomestici"](#).

Revisione ["Scopri di più su StorageGRID"](#) e il ["Linee guida per il networking"](#).

2

Installa nodi

Un sistema StorageGRID è costituito da singoli nodi basati su hardware e software. Per prima cosa, è necessario installare l'hardware per ciascun nodo dell'appliance e configurare ciascun host Linux o VMware.

Per completare l'installazione, è necessario installare il software StorageGRID su ciascun dispositivo o host software e collegare i nodi in una griglia. Durante questa fase, fornisci i nomi dei siti e dei nodi, i dettagli della subnet e gli indirizzi IP per i tuoi server NTP e DNS.

Scopri come:

- ["Installare l'hardware dell'apparecchio"](#)
- ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
- ["Installa StorageGRID su Ubuntu o Debian"](#)
- ["Installa StorageGRID su VMware"](#)

3

Sign in e controlla lo stato del sistema

Non appena installi il nodo di amministrazione primario, puoi accedere a Grid Manager. Da lì, puoi esaminare lo stato generale del tuo nuovo sistema, abilitare AutoSupport e le e-mail di avviso e configurare i nomi di dominio degli endpoint S3.

Scopri come:

- ["Sign in a Grid Manager"](#)
- ["Monitorare lo stato di salute del sistema"](#)
- ["Configura AutoSupport"](#)
- ["Imposta notifiche e-mail per gli avvisi"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)

4

Configurare e gestire

Le attività di configurazione da eseguire per un nuovo sistema StorageGRID dipendono da come si intende utilizzare la griglia. Come minimo, è necessario configurare l'accesso al sistema, utilizzare le procedure guidate FabricPool e S3 e gestire varie impostazioni di archiviazione e sicurezza.

Scopri come:

- ["Controllo dell'accesso a StorageGRID"](#)
- ["Utilizzare la procedura guidata di configurazione S3"](#)

- ["Utilizzare la procedura guidata di configurazione FabricPool"](#)
- ["Gestire la sicurezza"](#)
- ["Rafforzamento del sistema"](#)

5

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) composta da una o più regole ILM. Le regole ILM indicano a StorageGRID come creare e distribuire copie dei dati degli oggetti e come gestire tali copie nel tempo.

Scopri come: ["Gestire gli oggetti con ILM"](#)

6

Utilizzare StorageGRID

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

Scopri come:

- ["Utilizzare un account tenant"](#)
- ["Utilizzare l'API REST S3"](#)

7

Monitorare e risolvere i problemi

Quando il sistema è attivo e funzionante, è necessario monitorarne regolarmente le attività e risolvere eventuali problemi e avvisi. Potrebbe anche essere necessario configurare un server syslog esterno, utilizzare il monitoraggio SNMP o raccogliere dati aggiuntivi.

Scopri come:

- ["Monitorare StorageGRID"](#)
- ["Risoluzione dei problemi StorageGRID"](#)

8

Espandere, mantenere e recuperare

È possibile aggiungere nodi o siti per espandere la capacità o la funzionalità del sistema. È inoltre possibile eseguire diverse procedure di manutenzione per ripristinare il sistema in seguito a guasti o per mantenerlo aggiornato ed efficiente.

Scopri come:

- ["Espandi una griglia"](#)
- ["Mantieni la tua rete"](#)
- ["Recuperare i nodi"](#)

Installa, aggiorna e correggi StorageGRID

Dispositivi StorageGRID

Vai a "[Documentazione dell'appliance StorageGRID](#)" per imparare come installare, configurare e gestire gli appliance di archiviazione e servizi StorageGRID .

Installa StorageGRID su Red Hat Enterprise Linux

Guida rapida all'installazione di StorageGRID su Red Hat Enterprise Linux

Per installare un nodo Linux StorageGRID di Red Hat Enterprise Linux (RHEL), seguire questi passaggi generali.

1

Preparazione

- Scopri di più "[Architettura StorageGRID e topologia di rete](#)" .
- Scopri le specifiche di "[Rete StorageGRID](#)" .
- Raccogliere e preparare il "[Informazioni e materiali richiesti](#)" .
- Preparare il necessario "[CPU e RAM](#)" .
- Provvedere a "[requisiti di archiviazione e prestazioni](#)" .
- "[Preparare i server Linux](#)" che ospiterà i tuoi nodi StorageGRID .

2

Distribuzione

Distribuisci i nodi della griglia. Quando si distribuiscono i nodi della griglia, questi vengono creati come parte del sistema StorageGRID e connessi a una o più reti.

- Per distribuire nodi di griglia basati su software sugli host preparati nel passaggio 1, utilizzare la riga di comando di Linux e "[file di configurazione del nodo](#)" .
- Per distribuire i nodi dell'appliance StorageGRID , seguire le istruzioni "[Avvio rapido per l'installazione dell'hardware](#)" .

3

Configurazione

Quando tutti i nodi sono stati distribuiti, utilizzare 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 della griglia.

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

- Installazione di RHEL
- Configurazione di rete e storage
- Installazione del motore del contenitore e del servizio host StorageGRID
- Distribuzione di nodi di griglia virtuali

Vedere ["Automatizza l'installazione e la configurazione del servizio host StorageGRID"](#) .

- Dopo aver distribuito i nodi della griglia, ["automatizzare la configurazione del sistema StorageGRID"](#) utilizzando lo script di configurazione Python fornito nell'archivio di installazione.
- ["Automatizzare l'installazione e la configurazione dei nodi della griglia degli elettrodomestici"](#)
- Se sei uno sviluppatore avanzato di distribuzioni StorageGRID , automatizza l'installazione dei nodi della griglia utilizzando ["installazione REST API"](#) .

Pianificare e preparare l'installazione su Red Hat

Informazioni e materiali richiesti

Prima di installare StorageGRID, raccogliere e preparare le informazioni e i materiali richiesti.

Informazioni richieste

Piano di rete

Quali reti intendi collegare a ciascun nodo StorageGRID . StorageGRID supporta più reti per la separazione del traffico, la sicurezza e la praticità amministrativa.

Vedi StorageGRID ["Linee guida per il networking"](#) .

Informazioni di rete

Indirizzi IP da assegnare a ciascun nodo della griglia e gli indirizzi IP dei server DNS e NTP.

Server per nodi di griglia

Identifica un set di server (fisici, virtuali o entrambi) che, nel complesso, forniscano risorse sufficienti a supportare il numero e il tipo di nodi StorageGRID che intendi distribuire.



Se l'installazione StorageGRID non utilizzerà i nodi StorageGRID (hardware) dell'appliance StorageGRID, è necessario utilizzare un archivio RAID hardware con cache di scrittura con batteria di backup (BBWC). StorageGRID non supporta l'uso di reti di archiviazione virtuali (vSAN), RAID software o nessuna protezione RAID.

Migrazione dei nodi (se necessario)

Capire il ["requisiti per la migrazione dei nodi"](#) , se si desidera eseguire una manutenzione programmata sugli host fisici senza alcuna interruzione del servizio.

Informazioni correlate

["Strumento matrice di interoperabilità NetApp"](#)

Materiali richiesti

Licenza NetApp StorageGRID

È necessario disporre di una licenza NetApp valida e firmata digitalmente.



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

Archivio di installazione di StorageGRID

["Scarica l'archivio di installazione StorageGRID ed estrai i file"](#) .

Computer portatile di servizio

Il sistema StorageGRID viene installato tramite un laptop di servizio.

Il portatile di servizio deve avere:

- Porta di rete
- Client SSH (ad esempio, PuTTY)
- ["Browser web supportato"](#)

Documentazione StorageGRID

- ["Note di rilascio"](#)
- ["Istruzioni per la gestione di StorageGRID"](#)

Scarica ed estrai i file di installazione StorageGRID

È necessario scaricare l'archivio di installazione StorageGRID ed estrarre i file richiesti. Facoltativamente, è possibile verificare manualmente i file nel pacchetto di installazione.

Passi

1. Vai al ["Pagina di download di NetApp per StorageGRID"](#) .
2. Seleziona il pulsante per scaricare l'ultima versione oppure seleziona un'altra versione dal menu a discesa e seleziona **Vai**.
3. Sign in con il nome utente e la password del tuo account NetApp .
4. Se viene visualizzata una dichiarazione di Attenzione/Lettura obbligatoria, leggerla e selezionare la casella di controllo.



Dopo aver installato la versione StorageGRID , è necessario applicare tutti gli hotfix richiesti. Per ulteriori informazioni, consultare il sito ["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 **Accetta e continua**.
6. Nella colonna **Installa StorageGRID**, seleziona l'archivio di installazione .tgz o .zip per Red Hat Enterprise Linux.



Seleziona il .zip file se si utilizza Windows sul portatile di servizio.

7. Salvare l'archivio di installazione.

8. Se è necessario verificare l'archivio di installazione:
 - a. Scarica il pacchetto di verifica della firma del codice StorageGRID . Il nome del file per questo pacchetto utilizza il formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , Dove `<version-number>` è la versione del software StorageGRID .
 - b. Segui i passaggi per "[verificare manualmente i file di installazione](#)" .
9. Estrarre i file dall'archivio di installazione.
10. Scegli i file di cui hai bisogno.

I file necessari dipendono dalla topologia della griglia pianificata e dal modo in cui verrà distribuito 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 StorageGRID .
	Una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Pacchetto RPM per l'installazione delle immagini dei nodi StorageGRID sugli host RHEL.
	Pacchetto RPM per l'installazione del servizio host StorageGRID sugli host RHEL.
Strumento di scripting di distribuzione	Descrizione
	Uno script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID .
	Uno script Python utilizzato per automatizzare la configurazione degli appliance StorageGRID .
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Uno script Python di esempio che puoi utilizzare per accedere all'API di gestione della griglia quando è abilitato l'accesso singolo. È possibile utilizzare questo script anche per l'integrazione di Ping Federate.

Percorso e nome del file	Descrizione
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Esempio di ruolo e playbook Ansible per la configurazione di host RHEL per la distribuzione di container StorageGRID . È possibile personalizzare il ruolo o il playbook in base alle proprie esigenze.
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO) tramite Active Directory o Ping Federate.
	Uno script di supporto chiamato dal compagno <code>storagegrid-ssoauth-azure.py</code> Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: prima di eseguire un aggiornamento, puoi utilizzare questi schemi per confermare che il codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova versione StorageGRID se non disponi di un ambiente StorageGRID non di produzione per i test di compatibilità dell'aggiornamento.

Verifica manuale dei file di installazione (facoltativo)

Se necessario, è possibile verificare manualmente i file nell'archivio di installazione StorageGRID .

Prima di iniziare

Hai [scaricato il pacchetto di verifica](#) dal ["Pagina di download di NetApp per StorageGRID"](#) .

Passi

1. Estrarre gli artefatti dal pacchetto di verifica:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Assicurarsi che questi artefatti siano stati estratti:

- Certificato fogliare: `Leaf-Cert.pem`
- Catena di certificati: `CA-Int-Cert.pem`
- Catena di risposta del timestamp: `TS-Cert.pem`
- File di checksum: `sha256sum`
- Firma di checksum: `sha256sum.sig`

◦ File di risposta con timestamp: sha256sum.sig.tsr

3. Utilizzare la catena per verificare che il certificato fogliare sia valido.

Esempio: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Risultati previsti: Leaf-Cert.pem: OK

4. Se il passaggio 2 non è riuscito a causa di un certificato foglia scaduto, utilizzare tsr file da verificare.

Esempio: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

I risultati previsti includono: Verification: OK

5. Creare un file di chiave pubblica dal certificato foglia.

Esempio: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Risultato previsto: *nessuno*

6. Utilizzare la chiave pubblica per verificare il sha256sum presentare ricorso contro sha256sum.sig.

Esempio: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Risultati previsti: Verified OK

7. Verificare il sha256sum il contenuto del file rispetto ai checksum appena creati.

Esempio: `sha256sum -c sha256sum`

Risultati previsti: <filename>: OK

<filename> è il nome del file di archivio che hai scaricato.

8. ["Completa i passaggi rimanenti"](#) per estrarre e scegliere i file appropriati dall'archivio di installazione.

Requisiti software per Red Hat Enterprise Linux

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

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 del pacchetto software su cui vengono testate le installazioni StorageGRID includono quelle elencate in questa pagina.

Se selezioni un'opzione di installazione della distribuzione Linux e del runtime del contenitore che richiede uno qualsiasi di questi pacchetti e questi non vengono installati automaticamente dalla distribuzione Linux, installa una delle versioni elencate qui, se disponibile dal tuo provider o dal fornitore di supporto per la tua distribuzione Linux. In caso contrario, utilizzare le versioni predefinite del pacchetto messe a disposizione dal fornitore.

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



Il supporto per Docker come motore di container per distribuzioni esclusivamente software è deprecato. Docker verrà sostituito con un altro motore di container in una versione futura.

Versioni di 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 Docker testate



Il supporto Docker è obsoleto e verrà rimosso in una versione 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 CPU e RAM

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

Ogni nodo StorageGRID richiede le seguenti risorse minime:

- Core CPU: 8 per nodo
- RAM: Dipende dalla RAM totale disponibile e dalla quantità di software non StorageGRID in esecuzione sul sistema
 - In genere, almeno 24 GB per nodo e da 2 a 16 GB in meno rispetto alla RAM totale del sistema
 - Un minimo di 64 GB per ogni tenant che avrà circa 5.000 bucket

Le risorse dei nodi basati solo su metadati software devono corrispondere alle risorse dei nodi di archiviazione esistenti. Per esempio:

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

Quando si aggiunge un nuovo sito StorageGRID , la capacità totale dei metadati del nuovo sito deve corrispondere almeno ai siti StorageGRID esistenti e le risorse del nuovo sito devono corrispondere ai nodi di archiviazione nei siti StorageGRID esistenti.

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



Monitora regolarmente l'utilizzo della CPU e della memoria per assicurarti che queste risorse continuino a soddisfare il tuo carico di lavoro. Ad esempio, raddoppiando l'allocazione di RAM e CPU per i nodi di archiviazione virtuali si otterrebbero risorse simili a quelle fornite per i nodi dell'appliance StorageGRID . Inoltre, se la quantità di metadati per nodo supera i 500 GB, valutare di aumentare la RAM per nodo a 48 GB o più. Per informazioni sulla gestione dell'archiviazione dei metadati degli oggetti, sull'aumento dell'impostazione Spazio riservato ai metadati e sul monitoraggio dell'utilizzo della CPU e della memoria, vedere le istruzioni per ["amministrare"](#) , ["monitoraggio"](#) , E ["aggiornamento"](#) StorageGRID.

Se l'hyperthreading è abilitato sugli host fisici sottostanti, è possibile fornire 8 core virtuali (4 core fisici) per nodo. Se l'hyperthreading non è abilitato 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 VM, è consigliabile utilizzare una singola VM per ogni nodo StorageGRID e dimensionare la VM di conseguenza.

Per le distribuzioni di produzione, non dovresti eseguire più nodi di archiviazione sullo stesso hardware di archiviazione fisico o host virtuale. Ogni nodo di archiviazione in una singola distribuzione StorageGRID dovrebbe trovarsi nel proprio dominio di errore isolato. È possibile massimizzare la durabilità e la disponibilità

dei dati degli oggetti se ci si assicura che un singolo guasto hardware possa avere un impatto solo su un singolo nodo di archiviazione.

Vedere anche ["Requisiti di archiviazione e prestazioni"](#) .

Requisiti di archiviazione e prestazioni

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

I nodi StorageGRID richiedono tre categorie logiche di archiviazione:

- **Pool di contenitori:** archiviazione a livello di prestazioni (SAS o SSD da 10K) per i contenitori dei nodi, che verrà assegnata al driver di archiviazione del motore dei contenitori quando si installa e si configura il motore dei contenitori sugli host che supporteranno i nodi StorageGRID .
- **Dati di sistema** — Archiviazione a livello di prestazioni (SAS o SSD da 10K) per l'archiviazione persistente per nodo dei dati di sistema e dei registri delle transazioni, che i servizi host StorageGRID utilizzeranno e mapperanno nei singoli nodi.
- **Dati oggetto** - Archiviazione di livello prestazionale (SAS o SSD da 10K) e archiviazione di massa di livello di capacità (NL-SAS/SATA) per l'archiviazione persistente di dati oggetto e metadati oggetto.

È necessario utilizzare dispositivi a blocchi con supporto RAID per tutte le categorie di archiviazione. Non sono supportati dischi non ridondanti, SSD o JBOD. È possibile utilizzare l'archiviazione RAID condivisa o locale per qualsiasi categoria di archiviazione; tuttavia, se si desidera utilizzare la funzionalità di migrazione dei nodi in StorageGRID, è necessario archiviare sia i dati di sistema sia i dati degli oggetti nell'archiviazione condivisa. Per ulteriori informazioni, consultare ["Requisiti per la migrazione dei contenitori dei nodi"](#) .

Requisiti di prestazione

Le prestazioni dei volumi utilizzati per il pool di contenitori, i dati di sistema e i metadati degli oggetti influiscono in modo significativo sulle prestazioni complessive del sistema. Per questi volumi è consigliabile utilizzare un archivio di livello prestazionale (SAS o SSD da 10K) per garantire prestazioni del disco adeguate in termini di latenza, operazioni di input/output al secondo (IOPS) e throughput. È possibile utilizzare l'archiviazione a livelli di capacità (NL-SAS/SATA) per l'archiviazione persistente dei dati degli oggetti.

I volumi utilizzati per il pool di contenitori, i dati di sistema e i dati degli oggetti devono avere la memorizzazione nella cache write-back abilitata. La cache deve trovarsi su un supporto protetto o persistente.

Requisiti per gli host che utilizzano l'archiviazione NetApp ONTAP

Se il nodo StorageGRID utilizza storage assegnato da un sistema NetApp ONTAP , verificare che il volume non abbia un criterio di suddivisione in livelli FabricPool abilitato. La disattivazione della suddivisione in livelli FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di archiviazione.



Non utilizzare mai FabricPool per riportare i dati relativi a StorageGRID a StorageGRID stesso. Il riordino dei dati StorageGRID su StorageGRID aumenta la complessità operativa e la risoluzione dei problemi.

Numero di host richiesti

Ogni sito StorageGRID richiede un minimo di tre nodi di archiviazione.



In una distribuzione di produzione, non eseguire più di un nodo di archiviazione su un singolo host fisico o virtuale. Utilizzando un host dedicato per ogni nodo di archiviazione si ottiene un dominio di errore isolato.

Altri tipi di nodi, come i nodi amministrativi o i nodi gateway, possono essere distribuiti sugli stessi host oppure possono essere distribuiti sui propri host dedicati, a seconda delle necessità.

Numero di volumi di archiviazione per ciascun host

Nella tabella seguente viene mostrato il numero di volumi di archiviazione (LUN) richiesti per ciascun host e la dimensione minima richiesta per ogni LUN, in base ai nodi che verranno distribuiti su tale host.

La dimensione massima della LUN testata è 39 TB.



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

Scopo LUN	Categoria di archiviazione	Numero di LUN	Dimensione minima/LUN
Piscina di stoccaggio per motori container	Piscina di contenitori	1	Numero totale di nodi × 100 GB
`/var/local`volume	Dati di sistema	1 per ogni nodo su questo host	90 GB
Nodo di archiviazione	Dati oggetto	3 per ogni nodo di archiviazione su questo host Nota: un nodo di archiviazione basato su software può avere da 1 a 48 volumi di archiviazione; si consigliano almeno 3 volumi di archiviazione.	12 TB (4 TB/LUN) Vedi Requisiti di archiviazione per i nodi di archiviazione per maggiori informazioni.
Nodo di archiviazione (solo metadati)	Metadati dell'oggetto	1	4 TB Vedi Requisiti di archiviazione per i nodi di archiviazione per maggiori informazioni. Nota: per i nodi di archiviazione solo metadati è richiesto un solo rangedb.
Registri di controllo del nodo di amministrazione	Dati di sistema	1 per ogni nodo amministrativo su questo host	200 GB

Scopo LUN	Categoria di archiviazione	Numero di LUN	Dimensione minima/LUN
Tabelle dei nodi di amministrazione	Dati di sistema	1 per ogni nodo amministrativo su questo host	200 GB



A seconda del livello di controllo configurato, delle dimensioni degli input utente, come il nome della chiave dell'oggetto S3, e della quantità di dati del registro di controllo da conservare, potrebbe essere necessario aumentare le dimensioni della LUN del registro di controllo su ciascun nodo di amministrazione. In genere, una griglia genera circa 1 KB di dati di controllo per operazione S3, il che significa che una LUN da 200 GB supporterebbe 70 milioni di operazioni al giorno o 800 operazioni al secondo per due o tre giorni.

Spazio di archiviazione minimo per un host

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



Gli snapshot del disco non possono essere utilizzati per ripristinare i nodi della griglia. Fare invece riferimento al ["ripristino del nodo della griglia"](#) procedure per ogni tipo di nodo.

Tipo di nodo	Piscina di contenitori	Dati di sistema	Dati oggetto
Nodo di archiviazione	100 GB	90 GB	4.000 GB
Nodo di amministrazione	100 GB	490 GB (3 LUN)	<i>non applicabile</i>
Nodo Gateway	100 GB	90 GB	<i>non applicabile</i>

Esempio: calcolo dei requisiti di archiviazione per un host

Supponiamo di voler distribuire tre nodi sullo stesso host: un nodo di archiviazione, un nodo di amministrazione e un nodo gateway. È necessario fornire all'host almeno nove volumi di archiviazione. Saranno necessari almeno 300 GB di storage di livello prestazioni per i contenitori dei nodi, 670 GB di storage di livello prestazioni per i dati di sistema e i registri delle transazioni e 12 TB di storage di livello capacità per i dati degli oggetti.

Tipo di nodo	Scopo LUN	Numero di LUN	dimensione LUN
Nodo di archiviazione	Piscina di stoccaggio per motori container	1	300 GB (100 GB/nodo)
Nodo di archiviazione	`/var/local` volume	1	90 GB
Nodo di archiviazione	Dati oggetto	3	12 TB (4 TB/LUN)
Nodo di amministrazione	`/var/local` volume	1	90 GB

Tipo di nodo	Scopo LUN	Numero di LUN	dimensione LUN
Nodo di amministrazione	Registri di controllo del nodo di amministrazione	1	200 GB
Nodo di amministrazione	Tabelle dei nodi di amministrazione	1	200 GB
Nodo Gateway	`/var/local` volume	1	90 GB
Totale		9	Pool di contenitori: 300 GB Dati di sistema: 670 GB Dati oggetto: 12.000 GB

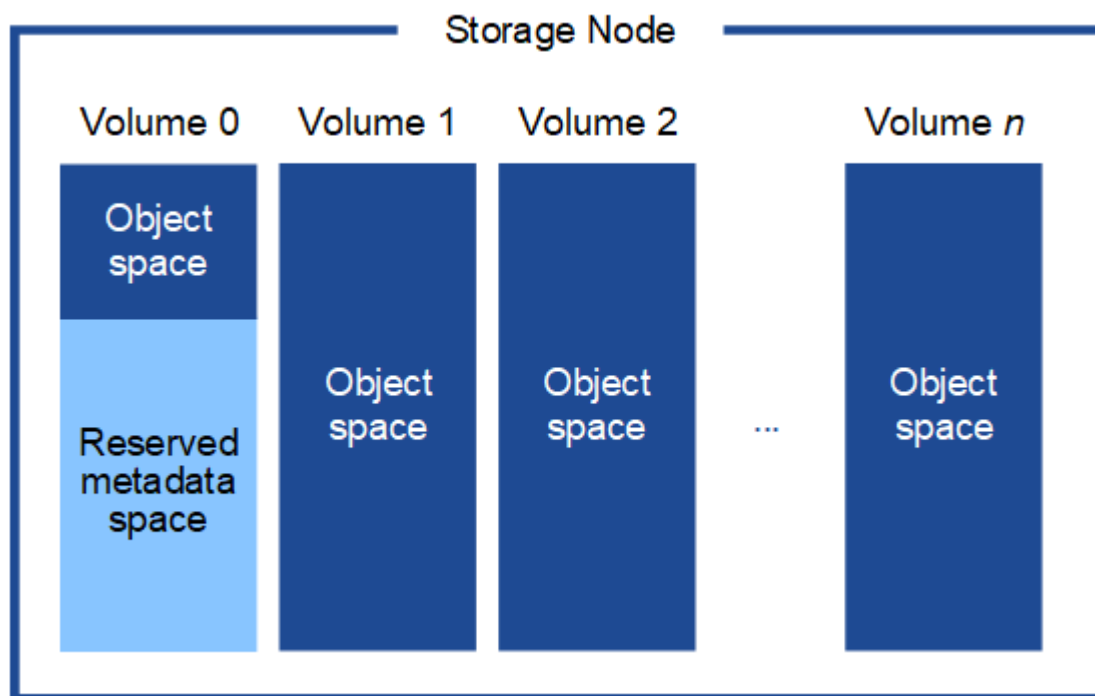
Requisiti di archiviazione per i nodi di archiviazione

Un nodo di archiviazione basato su software può avere da 1 a 48 volumi di archiviazione; si consigliano 3 o più volumi di archiviazione. Ogni volume di archiviazione deve essere pari o superiore a 4 TB.



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

Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di archiviazione 0 di ciascun nodo di archiviazione. Tutto lo spazio rimanente sul volume di archiviazione 0 e su tutti gli altri volumi di archiviazione nel nodo di archiviazione viene utilizzato esclusivamente per i dati degli oggetti.



Per garantire ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti nel sistema in ogni sito. Le tre copie dei metadati degli oggetti vengono

distribuite uniformemente tra tutti i nodi di archiviazione di ciascun sito.

Quando si installa una griglia con nodi di archiviazione solo metadati, la griglia deve contenere anche un numero minimo di nodi per l'archiviazione degli oggetti. Vedere "[Tipi di nodi di archiviazione](#)" per ulteriori informazioni sui nodi di archiviazione solo metadati.

- Per una griglia a sito singolo, sono configurati almeno due nodi di archiviazione per oggetti e metadati.
- Per una griglia multi-sito, almeno un nodo di archiviazione per sito è configurato per oggetti e metadati.

Quando si assegna spazio al volume 0 di un nuovo nodo di archiviazione, è necessario assicurarsi che vi sia spazio adeguato per la porzione di tutti i metadati degli oggetti di quel nodo.

- Come minimo, è necessario assegnare almeno 4 TB al volume 0.



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



Se si assegnano meno di 500 GB al volume 0 (solo per uso non produttivo), il 10% della capacità del volume di archiviazione è riservato ai metadati.

- Le risorse dei nodi basati solo su metadati software devono corrispondere alle risorse dei nodi di archiviazione esistenti. Per esempio:
 - Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo su software devono soddisfare i seguenti requisiti minimi:
 - 128 GB di RAM
 - CPU a 8 core
 - SSD da 8 TB o spazio di archiviazione equivalente per il database Cassandra (rangedb/0)
 - Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuali con 24 GB di RAM, CPU a 8 core e 3 TB o 4 TB di spazio di archiviazione dei metadati, i nodi basati solo su software devono utilizzare risorse simili (24 GB di RAM, CPU a 8 core e 4 TB di spazio di archiviazione dei metadati (rangedb/0).

Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve corrispondere almeno ai siti StorageGRID esistenti e le risorse del nuovo sito devono corrispondere ai nodi di archiviazione nei siti StorageGRID esistenti.

- Se si installa un nuovo sistema (StorageGRID 11.6 o versione successiva) e ogni nodo di archiviazione dispone di 128 GB o più di RAM, assegnare 8 TB o più al volume 0. Utilizzando un valore maggiore per il volume 0 è possibile aumentare lo spazio consentito per i metadati su ciascun nodo di archiviazione.
- Quando si configurano diversi nodi di archiviazione per un sito, utilizzare la stessa impostazione per il volume 0, se possibile. Se un sito contiene nodi di archiviazione di dimensioni diverse, il nodo di archiviazione con il volume più piccolo, 0, determinerà la capacità dei metadati di quel sito.

Per i dettagli, vai a "[Gestire l'archiviazione dei metadati degli oggetti](#)".

Requisiti per la migrazione dei contenitori dei nodi

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

La migrazione dei nodi consente di eseguire la manutenzione fisica dell'host senza interrompere le operazioni della griglia. È necessario spostare tutti i nodi StorageGRID , uno alla volta, su un altro host prima di mettere offline l'host fisico. La migrazione dei nodi richiede solo un breve periodo di inattività per ciascun nodo e non dovrebbe influire sul funzionamento o sulla disponibilità dei servizi di rete.

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

- Nomi di interfaccia di rete coerenti tra gli host in un singolo data center fisico
- Archiviazione condivisa per volumi di repository di oggetti e metadati StorageGRID , accessibile a tutti gli host in un singolo data center fisico. Ad esempio, potresti utilizzare array di storage NetApp E-Series.

Se si utilizzano host virtuali e il livello hypervisor sottostante supporta la migrazione delle VM, potrebbe essere opportuno utilizzare questa funzionalità anziché la funzionalità di migrazione dei nodi in StorageGRID. In questo caso, puoi ignorare questi requisiti aggiuntivi.

Prima di eseguire la migrazione o la manutenzione dell'hypervisor, arrestare i nodi in modo corretto. Vedi le istruzioni per ["chiusura di un nodo della griglia"](#) .

VMware Live Migration non supportato

Quando si esegue un'installazione bare-metal su VM VMware, OpenStack Live Migration e VMware Live vMotion causano un salto temporale nella macchina virtuale e non sono supportati per nodi di griglia di alcun tipo. Anche se raramente, orari errati possono causare la perdita di dati o di aggiornamenti della configurazione.

È supportata la migrazione a freddo. Nella migrazione a freddo, i nodi StorageGRID vengono arrestati prima di migrarli tra gli host. Vedi le istruzioni per ["chiusura di un nodo della griglia"](#) .

Nomi di interfaccia di rete coerenti

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

Supponiamo, ad esempio, che StorageGRID NodeA in esecuzione su Host1 sia stato configurato con le seguenti mappature di interfaccia:

eth0 → bond0.1001

eth1 → bond0.1002

eth2 → bond0.1003

Il lato sinistro delle frecce corrisponde alle interfacce tradizionali visualizzate dall'interno di un contenitore StorageGRID (ovvero, rispettivamente, le interfacce Grid, Admin e Client Network). Il lato destro delle frecce corrisponde alle interfacce host effettive che forniscono queste reti, ovvero tre interfacce VLAN subordinate allo stesso legame di interfaccia fisica.

Supponiamo ora di voler migrare NodeA su Host2. Se Host2 ha anche interfacce denominate bond0.1001, bond0.1002 e bond0.1003, il sistema consentirà lo spostamento, presupponendo che le interfacce con nomi simili forniscano la stessa connettività su Host2 come su Host1. Se Host2 non ha interfacce con gli stessi

nomi, lo spostamento non sarà consentito.

Esistono molti modi per ottenere una denominazione coerente dell'interfaccia di rete su più host; vedere "[Configurazione della rete host](#)" per alcuni esempi.

Archiviazione condivisa

Per ottenere migrazioni dei nodi rapide e con un overhead ridotto, la funzionalità di migrazione dei nodi StorageGRID non sposta fisicamente i dati dei nodi. Invece, la migrazione dei nodi viene eseguita come una coppia di operazioni di esportazione e importazione, come segue:

1. Durante l'operazione di "esportazione del nodo", una piccola quantità di dati di stato persistenti viene estratta dal contenitore del nodo in esecuzione su HostA e memorizzata nella cache del volume di dati di sistema di quel nodo. Quindi, il contenitore del nodo su HostA viene deistanziato.
2. Durante l'operazione di "importazione del nodo", viene creato un'istanza del contenitore del nodo su HostB che utilizza la stessa interfaccia di rete e le stesse mappature di archiviazione a blocchi in vigore su HostA. Quindi, i dati sullo stato persistente memorizzati nella cache vengono inseriti nella nuova istanza.

Data questa modalità di funzionamento, tutti i dati di sistema e i volumi di archiviazione degli oggetti del nodo devono essere accessibili sia da HostA che da HostB affinché la migrazione sia consentita e funzioni. Inoltre, devono essere stati mappati nel nodo utilizzando nomi che garantiscano di fare riferimento alle stesse LUN su HostA e HostB.

L'esempio seguente mostra una soluzione per la mappatura dei dispositivi a blocchi per un nodo di archiviazione StorageGRID, in cui il multipathing DM è in uso sugli host e il campo alias è stato utilizzato in `/etc/multipath.conf` per fornire nomi di dispositivi a blocchi coerenti e intuitivi disponibili su tutti gli host.

```
/var/local    → /dev/mapper/sgws-sn1-var-local
rangedb0     → /dev/mapper/sgws-sn1-rangedb0
rangedb1     → /dev/mapper/sgws-sn1-rangedb1
rangedb2     → /dev/mapper/sgws-sn1-rangedb2
rangedb3     → /dev/mapper/sgws-sn1-rangedb3
```

Preparare gli host (Red Hat)

Come cambiano le impostazioni dell'host durante l'installazione

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

Sono state 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 RAM
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

```

Installa Linux

È necessario installare StorageGRID su tutti gli host grid di Red Hat Enterprise Linux. Per un elenco delle versioni supportate, utilizzare lo strumento NetApp Interoperability Matrix.

Prima di iniziare

Assicurati che il tuo sistema operativo soddisfi i requisiti minimi di versione del kernel di StorageGRID, come elencato di seguito. Utilizzare il comando `uname -r` per ottenere la versione del kernel del tuo sistema operativo oppure consulta il fornitore del sistema operativo.

Versione di Red Hat Enterprise Linux	Versione minima del kernel	Nome del pacchetto del kernel
8.8 (obsoleto)	4.18.0-477.10.1.el8_8.x86_64	kernel-4.18.0-477.10.1.el8_8.x86_64
8,10	4.18.0-553.el8_10.x86_64	kernel-4.18.0-553.el8_10.x86_64
9.0 (obsoleto)	5.14.0-70.22.1.el9_0.x86_64	kernel-5.14.0-70.22.1.el9_0.x86_64

Versione di Red Hat Enterprise Linux	Versione minima del kernel	Nome del pacchetto del kernel
9.2 (obsoleto)	5.14.0-284.11.1.el9_2.x86_64	kernel-5.14.0-284.11.1.el9_2.x86_64
9,4	5.14.0-427.18.1.el9_4.x86_64	kernel-5.14.0-427.18.1.el9_4.x86_64
9,6	5.14.0-570.18.1.el9_6.x86_64	kernel-5.14.0-570.18.1.el9_6.x86_64

Passi

1. Installare Linux su tutti gli host fisici o virtuali della griglia secondo le istruzioni del distributore o la procedura standard.



Se si utilizza il programma di installazione standard di Linux, selezionare la configurazione software "compute node", se disponibile, oppure l'ambiente di base "minimal install". Non installare alcun ambiente desktop grafico.

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

Potrebbero essere necessari questi pacchetti aggiuntivi più avanti nella procedura di installazione.

3. Se lo swap è abilitato:

- a. Eseguire il seguente comando: `$ sudo swapoff --all`
- b. Rimuovi tutte le voci di swap da `/etc/fstab` per mantenere le impostazioni.



Se non si disattiva completamente lo swap, le prestazioni possono ridursi notevolmente.

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 alla mappatura nei nodi StorageGRID che verranno distribuiti in seguito.

Prima di iniziare

- Hai esaminato il "[Linee guida per la rete StorageGRID](#)".
- Hai esaminato le informazioni su "[requisiti di migrazione del contenitore del nodo](#)".
- Se si utilizzano host virtuali, è necessario leggere [considerazioni e raccomandazioni per la clonazione degli indirizzi MAC](#) prima di configurare la rete host.



Se si utilizzano VM come host, è necessario selezionare VMXNET 3 come scheda di rete virtuale. La scheda di rete VMware E1000 ha causato problemi di connettività con i container StorageGRID distribuiti su alcune distribuzioni di Linux.

Informazioni su questo compito

I nodi della griglia devono essere in grado di accedere alla rete della griglia e, facoltativamente, alle reti di

amministrazione 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 la distribuzione su tutti gli host e 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 per l'accesso alla rete di amministrazione del nodo, per facilitare la manutenzione dell'host e del nodo. Sebbene la stessa interfaccia possa essere condivisa tra l'host e i singoli nodi, tutti devono avere indirizzi IP diversi. Gli indirizzi IP non possono essere condivisi tra i nodi o tra l'host e un nodo.

È possibile utilizzare la stessa interfaccia di rete host per fornire l'interfaccia di rete Grid per tutti i nodi StorageGRID sull'host; è possibile utilizzare un'interfaccia di rete host diversa per ciascun nodo; oppure è possibile fare una via di mezzo. Tuttavia, in genere non si fornisce la stessa interfaccia di rete host come interfaccia di rete Grid e Admin per un singolo nodo, oppure come interfaccia di rete Grid per un nodo e interfaccia di rete client per un altro.

Puoi completare questo compito in molti modi. Ad esempio, se gli host sono macchine virtuali e si distribuiscono uno o due nodi StorageGRID per ciascun host, è possibile creare il numero corretto di interfacce di rete nell'hypervisor e utilizzare una mappatura 1 a 1. Se si distribuiscono più nodi su host bare metal per uso produttivo, è possibile sfruttare il supporto dello stack di rete Linux per VLAN e LACP per la tolleranza agli errori e la condivisione della larghezza di banda. Le sezioni seguenti forniscono approcci dettagliati per entrambi gli esempi. Non è necessario utilizzare nessuno di questi esempi; puoi utilizzare qualsiasi approccio che soddisfi le tue esigenze.



Non utilizzare dispositivi bond o bridge direttamente come interfaccia di rete del contenitore. In questo modo si potrebbe impedire l'avvio del nodo causato da un problema del kernel con l'uso di MACVLAN con dispositivi bond e bridge nello spazio dei nomi del contenitore. Utilizzare invece un dispositivo non vincolato, come una VLAN o una coppia Ethernet virtuale (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 raccomandazioni per la clonazione degli indirizzi MAC

La clonazione dell'indirizzo MAC fa sì che il contenitore utilizzi l'indirizzo MAC dell'host e che l'host utilizzi l'indirizzo MAC di un indirizzo specificato dall'utente o di uno generato casualmente. È consigliabile utilizzare la clonazione degli indirizzi MAC per evitare l'uso di configurazioni di rete in modalità promiscua.

Abilitazione della clonazione MAC

In determinati ambienti, la sicurezza può essere migliorata tramite la clonazione dell'indirizzo MAC, poiché consente di utilizzare una NIC virtuale dedicata per la rete amministrativa, la rete Grid e la rete client. Facendo in modo che il contenitore utilizzi l'indirizzo MAC della NIC dedicata sull'host, è possibile evitare di utilizzare configurazioni di rete in modalità promiscua.



La clonazione degli indirizzi MAC è pensata per essere utilizzata con installazioni di server virtuali e potrebbe non funzionare correttamente con tutte le configurazioni di dispositivi fisici.



Se un nodo non riesce ad avviarsi perché un'interfaccia di destinazione della clonazione MAC è 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 ad avviarsi perché un'interfaccia è occupata, impostare il collegamento su "inattivo" prima di avviare il nodo potrebbe risolvere il problema.

La clonazione dell'indirizzo MAC è disabilitata per impostazione predefinita e deve essere impostata tramite le chiavi di configurazione del nodo. Dovresti abilitarlo quando installi StorageGRID.

Esiste una chiave per ogni rete:

- 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 contenitore utilizzerà l'indirizzo MAC della scheda di rete dell'host. Inoltre, l'host utilizzerà l'indirizzo MAC della rete container specificata. Per impostazione predefinita, l'indirizzo del contenitore è un indirizzo generato casualmente, ma se ne hai impostato uno utilizzando `_NETWORK_MAC` chiave di configurazione del nodo, al suo posto viene utilizzato quell'indirizzo. L'host e il contenitore avranno sempre indirizzi MAC diversi.



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

Casi d'uso della clonazione MAC

Ci sono due casi d'uso da considerare con la clonazione MAC:

- Clonazione MAC non abilitata: quando il `_CLONE_MAC` chiave nel file di configurazione del nodo non è impostata o è impostata su "false", l'host utilizzerà il MAC della NIC dell'host e il contenitore avrà un MAC generato da StorageGRID a meno che non venga specificato un MAC nel `_NETWORK_MAC` chiave. Se un indirizzo è impostato nel `_NETWORK_MAC` chiave, il contenitore avrà l'indirizzo specificato nella `_NETWORK_MAC` chiave. Questa configurazione delle chiavi richiede l'uso della modalità promiscua.
- Clonazione MAC abilitata: quando il `_CLONE_MAC` la chiave nel file di configurazione del nodo è impostata su "true", il contenitore utilizza il MAC della NIC host e l'host utilizza un MAC generato da StorageGRID a meno che non venga specificato un MAC in `_NETWORK_MAC` chiave. Se un indirizzo è impostato nel `_NETWORK_MAC` chiave, l'host utilizza l'indirizzo specificato anziché uno generato. In questa configurazione di chiavi, non si dovrebbe utilizzare la modalità promiscua.



Se non si desidera utilizzare la clonazione degli indirizzi MAC e si preferisce 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 **Accetta** per Modalità promiscua, Modifiche indirizzo MAC e Trasmissioni contraffatte. 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 entrambi i punti.

Per abilitare la clonazione MAC, vedere ["Istruzioni per la creazione di file di configurazione del nodo"](#).

Esempio di clonazione MAC

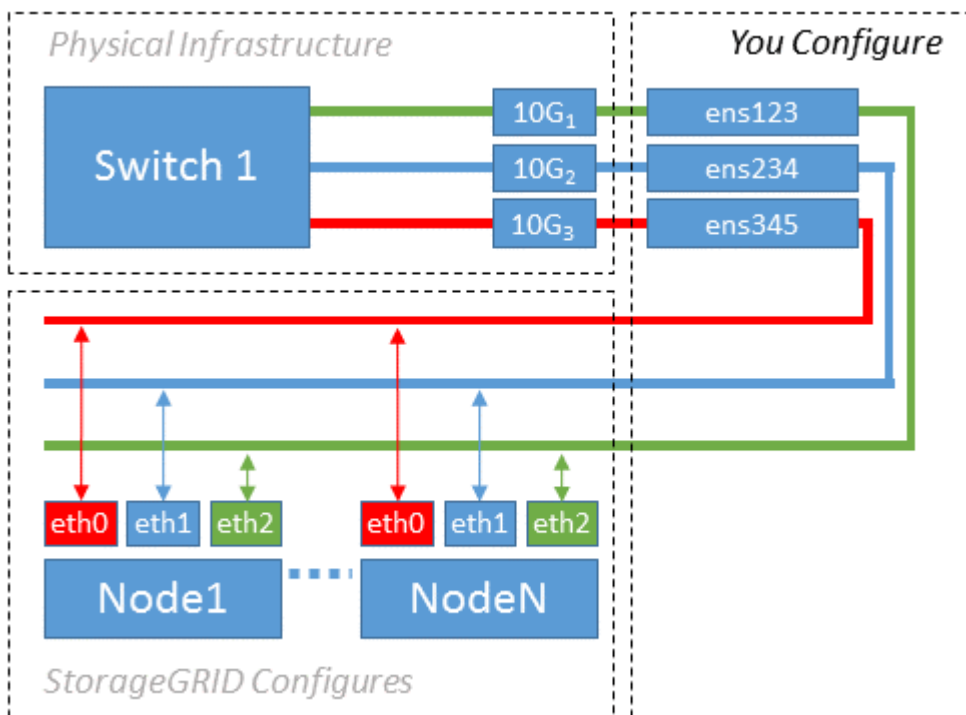
Esempio di clonazione MAC abilitata con un host con indirizzo MAC 11:22:33:44:55:66 per l'interfaccia ens256 e le seguenti chiavi nel file di configurazione del nodo:

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

Risultato: l'host MAC per ens256 è b2:9c:02:c2:27:10 e il MAC della rete di amministrazione 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 lato host minima o nulla.



Il sistema operativo Linux crea il `ensXYZ` interfacce automaticamente durante l'installazione o l'avvio, oppure quando le interfacce vengono aggiunte a caldo. Non è richiesta alcuna configurazione, se non quella di assicurarsi che le interfacce siano impostate per attivarsi automaticamente dopo l'avvio. Devi determinare quale `ensXYZ` corrisponde alla rete StorageGRID (Grid, Admin o Client), in modo da poter fornire le mappature corrette in seguito nel processo di configurazione.

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

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

Esempio 2: VLAN che trasportano legami LACP

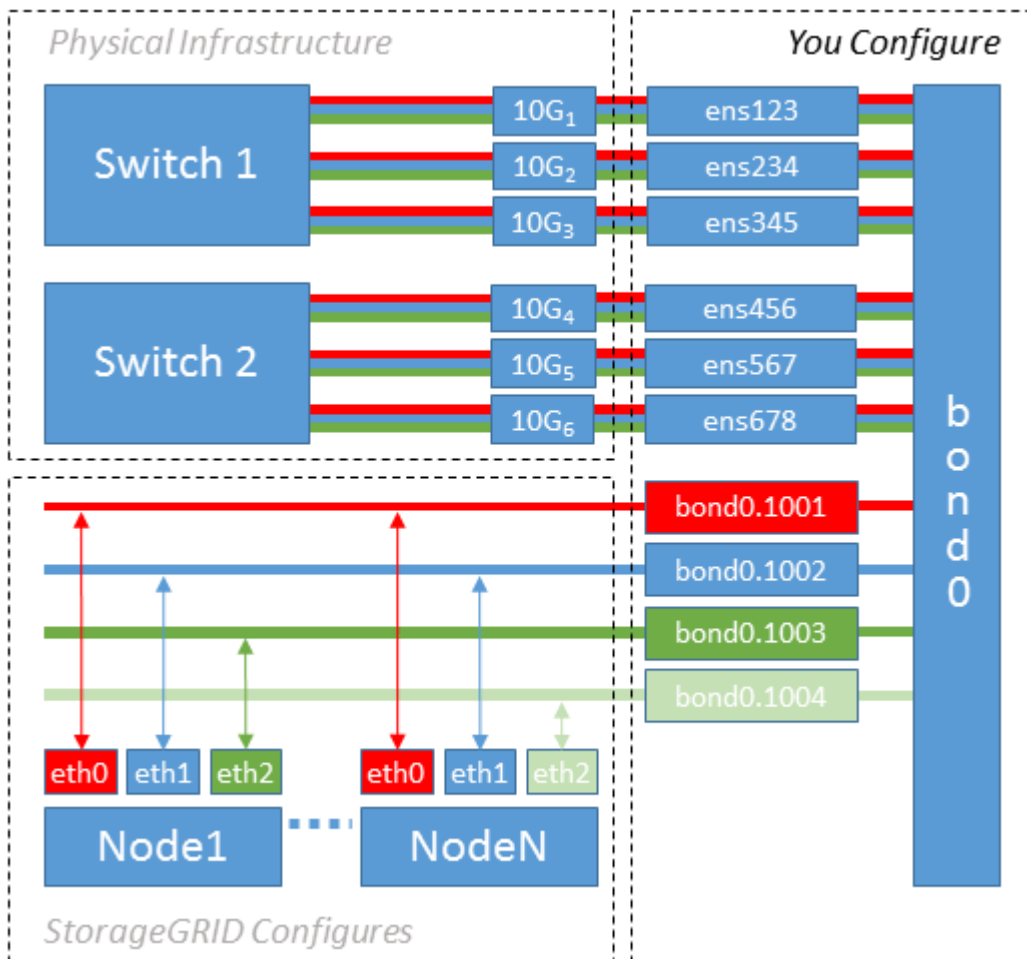
Informazioni su questo compito

L'esempio 2 presuppone che tu abbia familiarità con il bonding delle interfacce di rete e con la creazione di interfacce VLAN sulla distribuzione Linux che stai utilizzando.

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

Per comprendere questo esempio, supponiamo di avere tre subnet separate per la rete Grid, la rete Admin e la rete Client in ogni data center. Le subnet si trovano su VLAN separate (1001, 1002 e 1003) e vengono presentate all'host su una porta trunk legata a LACP (bond0). Dovresti configurare tre interfacce VLAN sul bond: bond0.1001, bond0.1002 e bond0.1003.

Se sono necessarie VLAN e subnet separate per le reti di nodi sullo stesso host, è possibile aggiungere interfacce VLAN sul bond e mapparle nell'host (mostrato come bond0.1004 nell'illustrazione).



Passi

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

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

2. Creare interfacce VLAN che utilizzano questo legame come "dispositivo fisico" associato, utilizzando la

convenzione di denominazione standard delle interfacce VLAN `physdev-name.VLAN ID`.

Si noti che i passaggi 1 e 2 richiedono una configurazione appropriata sugli switch edge che terminano le altre estremità dei collegamenti di rete. Anche le porte dello switch edge devono essere aggregate in un canale porta LACP, configurate come trunk e autorizzate a passare tutte le VLAN richieste.

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

Informazioni correlate

["Esempio /etc/sysconfig/network-scripts"](#)

Configurare l'archiviazione host

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

Prima di iniziare

Hai esaminato i seguenti argomenti, che forniscono le informazioni necessarie per portare a termine questa attività:

- ["Requisiti di archiviazione e prestazioni"](#)
- ["Requisiti per la migrazione dei contenitori dei nodi"](#)

Informazioni su questo compito

Quando si assegnano volumi di archiviazione 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 distribuiti su tale host)
- Categoria di archiviazione per ciascun volume (ovvero, dati di sistema o dati oggetto)
- Dimensione di ogni volume

Queste informazioni, insieme al nome persistente assegnato da Linux a ciascun volume fisico, verranno utilizzate quando si distribuiscono i nodi StorageGRID sull'host.



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



Per i nodi di archiviazione solo metadati è richiesta una sola LUN di dati oggetto.

Evitare di utilizzare file di dispositivi speciali "raw" (`/dev/sdb`, ad esempio) mentre componi l'elenco dei nomi dei volumi. Questi file possono cambiare durante i riavvii dell'host, il che può influire sul corretto funzionamento del sistema. Se si utilizzano iSCSI LUN e Device Mapper Multipathing, valutare l'utilizzo di alias multipath in `/dev/mapper` directory, soprattutto se la topologia SAN include percorsi di rete ridondanti verso l'archiviazione condivisa. In alternativa, è possibile utilizzare i collegamenti softlink creati dal sistema in `/dev/disk/by-path/` per i nomi dei tuoi dispositivi persistenti.

Per 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 archiviazione a blocchi per semplificare l'installazione iniziale StorageGRID e le future procedure di manutenzione. Se si utilizza il driver multipath del mapper del dispositivo per l'accesso ridondante ai volumi di archiviazione condivisi, è possibile utilizzare `alias` campo nel tuo `/etc/multipath.conf` file.

Per esempio:

```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-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
    }
    ...
}

```

Utilizzando il campo alias in questo modo, gli alias vengono visualizzati come dispositivi a blocchi in /dev/mapper directory sull'host, consentendo di specificare un nome descrittivo e facilmente convalidabile ogni volta che un'operazione di configurazione o manutenzione richiede di specificare un volume di archiviazione a blocchi.



Se si sta configurando un archivio condiviso per supportare la migrazione dei nodi StorageGRID e si utilizza Device Mapper Multipathing, è possibile creare e installare un archivio comune /etc/multipath.conf su tutti gli host co-localizzati. Assicurati solo di utilizzare un volume di archiviazione del motore del contenitore diverso su ciascun host. L'utilizzo di alias e l'inclusione del nome host di destinazione nell'alias per ogni LUN del volume di archiviazione del motore del contenitore renderanno tutto più facile da ricordare e sono consigliati.



Il supporto per Docker come motore di container per distribuzioni esclusivamente software è deprecato. Docker verrà sostituito con un altro motore di container in una versione futura.

Informazioni correlate

["Configurare il volume di archiviazione del motore del contenitore"](#)

Configurare il volume di archiviazione del motore del contenitore

Prima di installare il motore del contenitore (Docker o Podman), potrebbe essere necessario formattare il volume di archiviazione e montarlo.



Il supporto per Docker come motore di container per distribuzioni esclusivamente software è deprecato. Docker verrà sostituito con un altro motore di container in una versione futura.

Informazioni su questo compito

È possibile saltare questi passaggi se si prevede di utilizzare l'archiviazione locale per il volume di archiviazione Docker o Podman e si dispone di spazio sufficiente disponibile 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).

Passi

1. Creare un file system sul volume di archiviazione del motore del contenitore:

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

2. Montare il volume di stoccaggio del motore del contenitore:

- 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 archiviazione venga rimontato automaticamente dopo il riavvio dell'host.

Installa Docker

Il sistema StorageGRID funziona su Red Hat Enterprise Linux come una raccolta di container. Se hai scelto di utilizzare il motore del contenitore Docker, segui questi passaggi per installare Docker. Altrimenti, [installare Podman](#).

Passi

1. Installa Docker seguendo le istruzioni per la tua distribuzione Linux.



Se Docker non è incluso nella tua distribuzione Linux, puoi scaricarlo dal sito web di Docker.

2. Assicurati che Docker sia stato abilitato e avviato eseguendo i due comandi seguenti:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Conferma di aver installato la versione prevista di Docker immettendo quanto segue:

```
sudo docker version
```

Le versioni Client e Server devono essere 1.11.0 o successive.

Installa Podman

Il sistema StorageGRID funziona su Red Hat Enterprise Linux come una raccolta di container. Se hai scelto di utilizzare il motore contenitore Podman, segui questi passaggi per installare Podman. Altrimenti, [installare Docker](#).



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

Passi

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



Quando si installa Podman, è necessario installare anche il pacchetto Podman-Docker.

2. Conferma di aver installato la versione prevista di Podman e Podman-Docker immettendo 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
```


Installa i servizi host StorageGRID

Per installare i servizi host StorageGRID , utilizzare il pacchetto StorageGRID RPM.

Informazioni su questo compito

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

Passi

1. Copia i pacchetti RPM di StorageGRID su ciascuno dei tuoi host oppure rendili disponibili su un archivio condiviso.

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

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

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

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



È necessario installare prima il pacchetto Images e poi il pacchetto Service.



Se hai inserito i pacchetti in una directory diversa da `/tmp` , modifica il comando in modo che rifletta il percorso utilizzato.

Automatizza l'installazione StorageGRID su Red Hat Enterprise Linux

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

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

- Utilizzi già un framework di orchestrazione standard, come Ansible, Puppet o Chef, per distribuire e configurare host fisici o virtuali.
- Si intende distribuire più istanze StorageGRID .
- Stai distribuendo un'istanza StorageGRID complessa e di grandi dimensioni.

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

- ["Creare i file di configurazione"](#) interattivamente durante un'installazione manuale.

- Preparare in anticipo i file di configurazione (o a livello di programmazione) per abilitare l'installazione automatizzata utilizzando framework di orchestrazione standard, come descritto in questo articolo.

StorageGRID fornisce script Python opzionali per automatizzare la configurazione degli appliance StorageGRID e dell'intero sistema StorageGRID (la "griglia"). È possibile utilizzare questi script direttamente oppure è possibile esaminarli per imparare come utilizzarli. ["API REST di installazione di StorageGRID"](#) negli strumenti di distribuzione e configurazione della griglia che sviluppi autonomamente.

Automatizza l'installazione e la configurazione del servizio host StorageGRID

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

Il servizio host 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 abilitare l'installazione automatica. Se utilizzi già 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 ruolo e playbook di Ansible in `/extras` cartella fornita con l'archivio di installazione. Il playbook di Ansible mostra come `storagegrid` il ruolo prepara l'host e installa StorageGRID sui server di destinazione. È possibile personalizzare il ruolo o il playbook in base alle proprie esigenze.



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

È possibile automatizzare tutti i passaggi per la preparazione degli host e la distribuzione dei nodi della griglia virtuale.

Esempio di ruolo e playbook di Ansible

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

Le attività di installazione fornite `storagegrid` esempio di ruolo usa il `ansible.builtin.dnf` modulo per eseguire l'installazione dai file RPM locali o da un repository Yum remoto. Se il modulo non è disponibile o non è supportato, potrebbe essere necessario modificare le attività Ansible appropriate nei seguenti file per utilizzare il `yum` O `ansible.builtin.yum` modulo:

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`
- `roles/storagegrid/tasks/rhel_install_from_local.yml`

Automatizza la configurazione di StorageGRID

Dopo aver distribuito i nodi della griglia, è possibile automatizzare la configurazione del sistema StorageGRID.

Prima di iniziare

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

Nome del 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

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

Informazioni su questo compito

Puoi usare il `configure-storagegrid.py` Script Python e il `configure-storagegrid.json` file di configurazione per automatizzare la configurazione del sistema StorageGRID .



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

Passi

1. Accedi al computer Linux che stai utilizzando per eseguire lo script Python.
2. Passare alla directory in cui è stato estratto l'archivio di installazione.

Per esempio:

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

Dove `platform` È `debs` , `rpms` , O `vsphere` .

3. Esegui lo script Python e utilizza il file di configurazione che hai creato.

Per esempio:

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

Risultato

Un pacchetto di recupero `.zip` Il file viene generato durante il processo di configurazione e scaricato nella directory in cui si sta eseguendo 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, copialo in una posizione di rete protetta e sottoposta a backup e in un archivio cloud protetto.



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 hai specificato che vengano generate password casuali, apri il `Passwords.txt` file e cerca le password necessarie per accedere al tuo 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 è installato e configurato quando viene visualizzato un messaggio di conferma.

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

Informazioni correlate

["Installazione REST API"](#)

Distribuisci nodi di griglia virtuali (Red Hat)

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

I file di configurazione dei nodi sono piccoli file di testo che forniscono le informazioni di cui il servizio host StorageGRID ha bisogno per avviare un nodo e connetterlo alle risorse di rete e di archiviazione a blocchi appropriate. I file di configurazione dei nodi vengono utilizzati per i nodi virtuali e non per i nodi appliance.

Posizione per i file di configurazione del nodo

Posizionare il file di configurazione per ciascun nodo StorageGRID nel `/etc/storagegrid/nodes` directory sull'host in cui verrà eseguito il nodo. Ad esempio, se si prevede di eseguire un nodo di amministrazione, un nodo gateway e un nodo di archiviazione su HostA, è necessario posizionare tre file di configurazione del nodo in `/etc/storagegrid/nodes` su HostA.

È possibile creare i file di configurazione direttamente su ciascun host utilizzando un editor di testo, come vim o nano, oppure è possibile 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 che assegni al nodo. Questo nome appare nel programma di installazione StorageGRID e viene utilizzato per le operazioni di manutenzione dei nodi, come la migrazione dei nodi.

I nomi dei nodi devono seguire queste regole:

- Deve essere unico
- Deve iniziare con una lettera
- Può contenere i caratteri dalla A alla Z e dalla a alla z

- Può contenere i numeri da 0 a 9
- Può contenere uno o più trattini (-)
- Non deve contenere più di 32 caratteri, escluso il `.conf` estensione

Tutti i file in `/etc/storagegrid/nodes` che non seguono queste convenzioni di denominazione non verranno analizzati dal servizio host.

Se hai pianificato una topologia multi-sito per la tua griglia, uno schema di denominazione tipico dei nodi potrebbe essere:

```
site-nodetype-nodenum.conf
```

Ad esempio, potresti usare `dc1-adm1.conf` per il primo nodo amministrativo nel Data Center 1 e `dc2-sn3.conf` per il terzo nodo di archiviazione nel Data Center 2. Tuttavia, puoi usare qualsiasi schema tu preferisca, 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, seguire queste regole:

- La chiave e il valore devono essere separati da un segno di uguale(=) e spazi vuoti facoltativi.
- Le chiavi non possono contenere spazi.
- I valori possono contenere spazi incorporati.
- Eventuali spazi iniziali o finali vengono ignorati.

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

- **Obbligatorio:** obbligatorio per ogni nodo o per i tipi di nodo specificati
- **Migliore pratica:** Facoltativo, sebbene consigliato
- **Facoltativo:** facoltativo per tutti i nodi

Chiavi di rete amministrative

ADMIN_IP

Valore	Designazione
Indirizzo IPv4 della rete Grid del nodo di amministrazione primario per la griglia a cui appartiene questo nodo. Utilizzare lo stesso valore specificato per <code>GRID_NETWORK_IP</code> per il nodo della griglia con <code>NODE_TYPE = VM_Admin_Node</code> e <code>ADMIN_ROLE = Primary</code>. Se si omette questo parametro, il nodo tenta di individuare un nodo amministrativo primario tramite mDNS. "Come i nodi della griglia scoprono il nodo di amministrazione primario" Nota: questo valore viene ignorato e potrebbe essere vietato sul nodo di amministrazione primario.	Le migliori pratiche

ADMIN_NETWORK_CONFIG

Valore	Designazione
DHCP, STATICO o DISABILITATO	Opzionale

ADMIN_NETWORK_ESL

Valore	Designazione
Elenco separato da virgole delle subnet in notazione CIDR con cui questo nodo deve comunicare tramite il gateway di rete di amministrazione. Esempio: 172.16.0.0/21, 172.17.0.0/21	Opzionale

GATEWAY DI RETE AMMINISTRATIVA

Valore	Designazione
Indirizzo IPv4 del gateway di rete di amministrazione 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 tramite DHCP. Esempi: 1.1.1.1 10.224.4.81	Obbligatorio se ADMIN_NETWORK_ESL è specificato. Altrimenti facoltativo.

IP_RETE_AMMINISTRATIVO

Valore	Designazione
Indirizzo IPv4 di questo nodo sulla rete di amministrazione. Questa chiave è richiesta solo quando ADMIN_NETWORK_CONFIG = STATIC; non specificarla per altri valori. Esempi: 1.1.1.1 10.224.4.81	Obbligatorio quando ADMIN_NETWORK_CONFIG = STATIC. Altrimenti facoltativo.

AMMINISTRAZIONE_RETE_MAC

Valore	Designazione
L'indirizzo MAC per l'interfaccia di rete di amministrazione nel contenitore. Questo campo è facoltativo. Se omissso, verrà generato automaticamente un indirizzo MAC. Deve essere composto da 6 coppie di cifre esadecimali separate da due punti. Esempio: b2:9c:02:c2:27:10	Opzionale

MASCHERA_DI_RETE_ADMIN

Valore	Designazione
Maschera di rete 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	Obbligatorio se è specificato ADMIN_NETWORK_IP e ADMIN_NETWORK_CONFIG = STATIC. Altrimenti facoltativo.

ADMIN_NETWORK_MTU

Valore	Designazione
L'unità di trasmissione massima (MTU) per questo nodo sulla rete di amministrazione. Non specificare se ADMIN_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omissso, viene utilizzato 1500. Se si desidera utilizzare i jumbo frame, impostare l'MTU su un valore adatto ai jumbo frame, ad esempio 9000. Altrimenti, mantieni 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 prestazioni di rete o perdita di pacchetti. Esempi: 1500 8192	Opzionale

AMMINISTRAZIONE_RETE_TARGET

Valore	Designazione
Nome del dispositivo host che verrà utilizzato per l'accesso alla rete di amministrazione da parte del 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) sul dispositivo di bonding oppure utilizzare un bridge e una coppia Ethernet virtuale (veth). Migliore pratica: specificare un valore anche se inizialmente questo nodo non avrà un indirizzo IP di rete amministrativa. Successivamente potrai aggiungere un indirizzo IP di rete amministrativa, senza dover riconfigurare il nodo sull'host. Esempi: bond0.1002 ens256	Le migliori pratiche

TIPO_TARGET_RETE_AMMINISTRAZIONE

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 far sì che il contenitore StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete di amministrazione. Migliore pratica: nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per maggiori dettagli sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione dell'indirizzo MAC (Ubuntu o Debian)"	Le migliori pratiche

RUOLO_AMMINISTRATORE

Valore	Designazione
Primario o non primario Questa chiave è richiesta solo quando NODE_TYPE = VM_Admin_Node; non specificarla per altri tipi di nodo.	Obbligatorio quando NODE_TYPE = VM_Admin_Node Altrimenti facoltativo.

Blocca le chiavi del dispositivo

BLOCK_DEVICE_AUDIT_LOGS

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi che questo nodo utilizzerà per l'archiviazione persistente dei registri di controllo. Esempi: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adm1-audit-logs</pre>	Obbligatorio per i nodi con NODE_TYPE = VM_Admin_Node. Non specificarlo per altri tipi di nodo.

BLOCK_DEVICE_RANGEDB_nnn

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi che questo nodo utilizzerà per l'archiviazione persistente degli oggetti. Questa chiave è richiesta solo per i nodi con NODE_TYPE = VM_Storage_Node; non specificarla per altri tipi di nodo. È obbligatorio 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 spazi vuoti. Se si specifica BLOCK_DEVICE_RANGEDB_005, è necessario specificare anche BLOCK_DEVICE_RANGEDB_004. Nota: per garantire la compatibilità con le distribuzioni esistenti, per i nodi aggiornati sono supportate chiavi a due cifre. Esempi: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-rangedb-000</pre>	Necessario: 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

TABELLE_DISPOSITIVI_BLOCCHI

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi che questo nodo utilizzerà per l'archiviazione persistente delle tabelle del database. Questa chiave è richiesta solo per i nodi con NODE_TYPE = VM_Admin_Node; non specificarla per altri tipi di nodo. Esempi: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-tables</pre>	Necessario

BLOCK_DEVICE_VAR_LOCAL

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi che questo nodo utilizzerà per il suo /var/local archiviazione persistente. Esempi: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-var-local</pre>	Necessario

Chiavi di rete del cliente

CLIENT_NETWORK_CONFIG

Valore	Designazione
DHCP, STATICO o DISABILITATO	Opzionale

GATEWAY_RETE_CLIENT

Valore	Designazione

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

IP_RETE_CLIENTE

Valore	Designazione
Indirizzo IPv4 di questo nodo sulla rete client. Questa chiave è richiesta solo quando CLIENT_NETWORK_CONFIG = STATIC; non specificarla per altri valori. Esempi: 1.1.1.1 10.224.4.81	Obbligatorio quando CLIENT_NETWORK_CONFIG = STATIC Altrimenti facoltativo.

CLIENT_NETWORK_MAC

Valore	Designazione
L'indirizzo MAC per l'interfaccia di rete client nel contenitore. Questo campo è facoltativo. Se omissso, verrà generato automaticamente un indirizzo MAC. Deve essere composto da 6 coppie di cifre esadecimali separate da due punti. Esempio: b2:9c:02:c2:27:20	Opzionale

CLIENT_NETWORK_MASK

Valore	Designazione
Maschera di rete 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	Obbligatorio se è specificato CLIENT_NETWORK_IP e CLIENT_NETWORK_CONFIG = STATIC Altrimenti facoltativo.

CLIENT_NETWORK_MTU

Valore	Designazione
L'unità di trasmissione massima (MTU) 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 jumbo frame, impostare l'MTU su un valore adatto ai jumbo frame, ad esempio 9000. Altrimenti, mantieni 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 prestazioni di rete o perdita di pacchetti. Esempi: 1500 8192	Opzionale

CLIENT_NETWORK_TARGET

Valore	Designazione
Nome del dispositivo host che verrà utilizzato per l'accesso alla rete client da parte del 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) sul dispositivo di bonding oppure utilizzare un bridge e una coppia Ethernet virtuale (veth). Procedura consigliata: specificare un valore anche se inizialmente questo nodo non avrà un indirizzo IP di rete client. Successivamente è possibile aggiungere un indirizzo IP di rete client, senza dover riconfigurare il nodo sull'host. Esempi: bond0.1003 ens423	Le migliori pratiche

TIPO_DESTINAZIONE_RETE_CLIENT

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

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o falso Impostare la chiave su "true" per far sì che il contenitore StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete client. Migliore pratica: nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per maggiori dettagli sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione dell'indirizzo MAC (Ubuntu o Debian)"	Le migliori pratiche

Chiavi di rete della griglia

GRID_NETWORK_CONFIG

Valore	Designazione
STATICO o DHCP Se non specificato, il valore predefinito è STATIC.	Le migliori pratiche

GRID_NETWORK_GATEWAY

Valore	Designazione
Indirizzo IPv4 del gateway di rete Grid locale per questo nodo, che deve trovarsi nella subnet definita da GRID_NETWORK_IP e GRID_NETWORK_MASK. Questo valore viene ignorato per le reti configurate tramite DHCP. Se la rete Grid è una singola subnet senza gateway, utilizzare l'indirizzo gateway standard per la subnet (XYZ1) o il valore GRID_NETWORK_IP di questo nodo; entrambi i valori semplificheranno le potenziali espansioni future della rete Grid.	Necessario

IP_RETE_GRIGLIA

Valore	Designazione
Indirizzo IPv4 di questo nodo sulla rete Grid. Questa chiave è richiesta solo quando GRID_NETWORK_CONFIG = STATIC; non specificarla per altri valori. Esempi: 1.1.1.1 10.224.4.81	Obbligatorio quando GRID_NETWORK_CONFIG = STATIC Altrimenti facoltativo.

GRID_NETWORK_MAC

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

GRID_NETWORK_MASK

Valore	Designazione
Maschera di rete IPv4 per questo nodo sulla rete Grid. Specificare questa chiave quando GRID_NETWORK_CONFIG = STATIC; non specificarla per altri valori. Esempi: 255.255.255.0 255.255.248.0	Obbligatorio quando è specificato GRID_NETWORK_IP e GRID_NETWORK_CONFIG = STATIC. Altrimenti facoltativo.

GRID_NETWORK_MTU

Valore	Designazione
L'unità di trasmissione massima (MTU) per questo nodo sulla rete Grid. Non specificare se GRID_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omissso, viene utilizzato 1500. Se si desidera utilizzare i jumbo frame, impostare l'MTU su un valore adatto ai jumbo frame, ad esempio 9000. Altrimenti, mantieni 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 prestazioni di rete o perdita di pacchetti. IMPORTANTE: Per ottenere le migliori prestazioni di rete, tutti i nodi devono essere configurati con valori MTU simili sulle loro interfacce di rete Grid. L'avviso Mancata corrispondenza MTU della rete Grid viene attivato se si verifica una differenza significativa nelle impostazioni MTU per la rete Grid sui singoli nodi. I valori MTU non devono essere gli stessi 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 Grid da parte del 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) sul dispositivo di bonding oppure utilizzare un bridge e una coppia Ethernet virtuale (veth). Esempi: <pre>bond0.1001</pre> <pre>ens192</pre>	Necessario

TIPO_TARGET_RETE_GRIGLIA

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 far sì che il contenitore StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete Grid. Migliore pratica: nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per maggiori dettagli sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione dell'indirizzo MAC (Ubuntu o Debian)"	Le migliori pratiche

Chiave password di installazione (temporanea)

HASH_PASSWORD_TEMPORANEO_PERSONALIZZATO

Valore	Designazione
Per il nodo di amministrazione primario, impostare una password temporanea predefinita per l'API di installazione StorageGRID durante l'installazione. Nota: impostare una password di installazione solo sul nodo di amministrazione primario. Se si tenta di impostare una password su un altro tipo di nodo, la convalida del file di configurazione del nodo fallirà. L'impostazione di questo valore non ha alcun effetto al termine dell'installazione. Se questa chiave viene omessa, per impostazione predefinita non viene impostata alcuna password temporanea. In alternativa, è possibile impostare una password temporanea utilizzando l'API di installazione StorageGRID . Deve essere un <code>crypt()</code> Hash della password SHA-512 con formato <code>\$6\$<salt>\$<password hash></code> per una password di almeno 8 e non più di 32 caratteri. Questo hash può essere generato utilizzando strumenti CLI, come <code>openssl passwd</code> comando in modalità SHA-512.	Le migliori pratiche

Chiave delle interfacce

INTERFACCIA_DESTINAZIONE_nnnn

Valore	Designazione
Nome e descrizione facoltativa per un'interfaccia aggiuntiva che si desidera aggiungere a questo nodo. È possibile aggiungere più interfacce extra a ciascun nodo. Per <i>nnnn</i>, specificare un numero univoco per ogni voce <code>INTERFACE_TARGET</code> 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 Interfacce VLAN e nella pagina Gruppi HA. Esempio: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Se si aggiunge un'interfaccia trunk, 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

RAM MASSIMA

Valore	Designazione
La quantità massima di RAM che questo nodo può consumare. Se questa chiave viene omessa, il nodo non ha restrizioni di memoria. Quando si imposta questo campo per un nodo di livello di produzione, specificare un valore pari ad almeno 24 GB e da 16 a 32 GB in meno rispetto alla RAM totale del sistema. Nota: il valore della RAM influisce sullo spazio effettivo riservato ai metadati di un nodo. Vedi il "descrizione di cosa è lo spazio riservato ai metadati". Il formato per questo campo è <i>numberunit</i>, Dove <i>unit</i> 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 cgroup di memoria.	Opzionale

Chiavi di tipo nodo

TIPO_NODO

Valore	Designazione
Tipo di nodo: • Nodo amministratore VM • Nodo di archiviazione VM • VM_Archive_Node • Gateway VM_API	Necessario

TIPO_DI_ARCHIVIAZIONE

Valore	Designazione
Definisce il tipo di oggetti contenuti in un nodo di archiviazione. Per ulteriori informazioni, consultare "Tipi di nodi di archiviazione". Questa chiave è richiesta solo per i nodi con NODE_TYPE = VM_Storage_Node; non specificarla per altri tipi di nodo. Tipi di archiviazione: • combinato • dati • metadati Nota: se STORAGE_TYPE non è specificato, per impostazione predefinita il tipo di nodo di archiviazione è impostato su combinato (dati e metadati).	Opzionale

Tasti di rimappatura delle porte

PORT_REMAP

Valore	Designazione
Riassegna qualsiasi porta utilizzata da un nodo per le comunicazioni interne del nodo della griglia o per le comunicazioni esterne. La rimappatura delle porte è necessaria se i criteri di rete aziendale limitano una o più porte utilizzate da StorageGRID, come descritto in "Comunicazioni interne al nodo della griglia" O "Comunicazioni esterne". IMPORTANTE: non rimappare le porte che intendi utilizzare per configurare gli endpoint del bilanciatore del carico. Nota: se è impostato solo PORT_REMAP, la mappatura specificata viene utilizzata sia per le comunicazioni in entrata che per quelle in uscita. Se viene specificato anche PORT_REMAP_INBOUND, PORT_REMAP si applica solo alle comunicazioni in uscita. Il formato utilizzato è: <i>network type/protocol/default port used by grid node/new port</i>, Dove <i>network type</i> è griglia, amministratore o client e <i>protocol</i> è tcp o udp. Esempio: PORT_REMAP = client/tcp/18082/443 È anche possibile rimappare più porte utilizzando un elenco separato da virgole. Esempio: PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80	Opzionale

PORT_REMAP_INBOUND

Valore	Designazione
Riassegna 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 intendi utilizzare per configurare gli endpoint del bilanciatore del carico. Il formato utilizzato è: <i>network type/protocol/remapped port /default port used by grid node</i>, Dove <i>network type</i> è griglia, amministratore o client e <i>protocol</i> è tcp o udp. Esempio: PORT_REMAP_INBOUND = grid/tcp/3022/22 È anche possibile rimappare più porte in ingresso utilizzando un elenco separato da virgole. Esempio: PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22	Opzionale

Come i nodi della griglia scoprono il nodo di amministrazione primario

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

Per garantire che un nodo della griglia possa accedere al nodo di amministrazione primario, è possibile effettuare una delle seguenti operazioni durante la distribuzione del nodo:

- È possibile utilizzare il parametro ADMIN_IP per immettere manualmente l'indirizzo IP del nodo di amministrazione primario.
- È possibile omettere il parametro ADMIN_IP per fare in modo che il nodo della griglia rilevi automaticamente il valore. La rilevazione automatica è particolarmente utile quando la rete Grid utilizza DHCP per assegnare l'indirizzo IP al nodo di amministrazione primario.

Il rilevamento automatico del nodo di amministrazione primario viene eseguito tramite un sistema di nomi di dominio multicast (mDNS). Quando il nodo di amministrazione primario viene avviato per la prima volta, pubblica il suo indirizzo IP tramite mDNS. Altri nodi sulla stessa subnet possono quindi richiedere l'indirizzo IP e acquisirlo automaticamente. Tuttavia, poiché il traffico IP multicast non è normalmente instradabile tra subnet, i nodi su altre subnet non possono acquisire direttamente l'indirizzo IP del nodo amministrativo primario.

Se si utilizza la rilevazione automatica:



- È necessario includere l'impostazione `ADMIN_IP` per almeno un nodo della griglia su tutte le subnet a cui il nodo di amministrazione primario non è direttamente collegato. Questo nodo della griglia pubblicherà quindi l'indirizzo IP del nodo di amministrazione primario affinché altri nodi sulla subnet possano individuarlo con mDNS.
- Assicurati che la tua infrastruttura di rete supporti il passaggio del traffico IP multicast all'interno di una subnet.

File di configurazione dei nodi di esempio

È possibile utilizzare i file di configurazione dei nodi di esempio per impostare 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 della griglia.

Per la maggior parte dei nodi, è possibile aggiungere informazioni sull'indirizzamento di rete dell'amministratore e del client (IP, maschera, gateway e così via) quando si configura la griglia tramite Grid Manager o l'API di installazione. L'eccezione è il nodo di amministrazione primario. Se si desidera accedere all'IP della rete amministrativa del nodo amministrativo primario per completare la configurazione della griglia (ad esempio perché la rete della griglia non è instradata), è necessario configurare la connessione alla rete amministrativa per il nodo amministrativo primario nel relativo file di configurazione del nodo. Ciò è mostrato nell'esempio.



Negli esempi, la destinazione Client Network è stata configurata come best practice, anche se Client Network è disabilitata per impostazione predefinita.

Esempio per il nodo di amministrazione primario

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

Esempio di contenuto del file:

```

NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adml-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adml-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adml-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 archiviazione

Nome file di esempio: /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 il nodo gateway

Nome file di esempio: /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/dcl-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 per un nodo di amministrazione non primario

Nome file di esempio: /etc/storagegrid/nodes/dcl-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/dcl-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dcl-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dcl-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
```

Convalida 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 ogni file di configurazione, come mostrato nell'esempio.



Quando si utilizza una sola LUN su 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 dcl-adm1... PASSED
Checking configuration file for node dcl-gw1... PASSED
Checking configuration file for node dcl-sn1... PASSED
Checking configuration file for node dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes... PASSED
```



Per un'installazione automatizzata, è possibile sopprimere questo output utilizzando `-q` o `--quiet` opzioni nel `storagegrid` comando (ad esempio, `storagegrid --quiet...`). Se si sopprime 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** ed **ERROR**, come mostrato nell'esempio. Se vengono rilevati errori di configurazione, è necessario correggerli prima di continuare con l'installazione.

```

Checking for misnamed node configuration files...
WARNING: ignoring /etc/storagegrid/nodes/dcl-adml
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
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 dcl-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 dcl-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 dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
ERROR: GRID_NETWORK_IP = 10.1.0.4
      dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Avviare il servizio host StorageGRID

Per avviare i nodi StorageGRID e assicurarsi che si riavviino dopo un riavvio dell'host, è necessario abilitare e avviare il servizio host StorageGRID .

Passi

1. Eseguire i seguenti comandi su ciascun host:

```

sudo systemctl enable storagegrid
sudo systemctl start storagegrid

```

2. Eseguire il seguente comando per assicurarsi che la distribuzione proceda:

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

3. Se un nodo restituisce lo stato "Non in esecuzione" o "Arrestato", eseguire il seguente comando:

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

4. Se in precedenza hai abilitato e avviato il servizio host StorageGRID (o se non sei sicuro che il servizio sia stato abilitato e avviato), esegui anche il seguente comando:

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

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

Vai al Grid Manager

Utilizzare Grid Manager per definire tutte le informazioni necessarie per configurare il sistema StorageGRID .

Prima di iniziare

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

Passi

1. Apri il tuo browser web e vai su:

```
https://primary_admin_node_ip
```

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

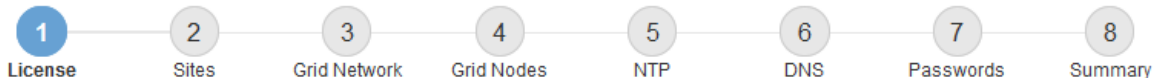
```
https://primary_admin_node_ip:8443
```

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

2. Gestisci una password di installazione temporanea secondo necessità:
 - Se è già stata impostata una password utilizzando uno di questi metodi, immetterla per procedere.
 - Un utente ha impostato la password durante l'accesso al programma di installazione in precedenza
 - La password è stata importata automaticamente dal file di configurazione del nodo in `/etc/storagegrid/nodes/<node_name>.conf`
 - Se non è stata impostata una password, impostarne una facoltativamente per proteggere il programma di installazione StorageGRID .
3. Selezionare ***Installa un sistema StorageGRID ***.

Viene visualizzata la pagina utilizzata per configurare un sistema StorageGRID .

Install



License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Browse

Specificare le informazioni sulla licenza StorageGRID

È necessario specificare il nome del sistema StorageGRID e caricare il file di licenza fornito da NetApp.

Passi

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 Nodi.

2. Selezionare **Sfogli**, individuare il file di licenza NetApp(*NLF-unique-id.txt*) e seleziona **Apri**.

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



L'archivio di installazione StorageGRID include una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto. Dopo l'installazione è possibile effettuare l'aggiornamento a una licenza che offra supporto.

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File NLF-959007-Internal.txt

License Serial Number

3. Selezionare **Avanti**.

Aggiungi siti

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

Passi

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

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

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top is a blue header with 'NetApp® StorageGRID®' and a 'Help' dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites (highlighted in blue), 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Below the progress bar, the 'Sites' section is active. It contains two paragraphs of text explaining single-site and multi-site deployments. Below the text are two input fields for site names. The first field is labeled 'Site Name 1' and contains the text 'Raleigh', with a red 'x' icon to its right. The second field is labeled 'Site Name 2' and contains the text 'Atlanta', with a red '+ x' icon to its right.

3. Fare clic su **Avanti**.

Specificare le subnet della rete Grid

È necessario specificare le subnet utilizzate nella rete Grid.

Informazioni su questo compito

Le voci di subnet includono le subnet per la rete Grid per ciascun sito nel sistema StorageGRID, insieme a tutte le subnet che devono essere raggiungibili tramite la rete Grid.

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

Passi

1. Specificare l'indirizzo di rete CIDR per almeno una rete Grid nella casella di testo **Subnet 1**.
2. Fare clic sul segno più accanto all'ultima voce per aggiungere un'ulteriore voce di rete. È necessario specificare tutte le subnet per tutti i siti nella rete Grid.
 - Se hai già distribuito almeno un nodo, fai clic su **Scopri subnet di Grid Networks** per popolare automaticamente l'elenco delle subnet di Grid Network con le subnet segnalate dai nodi di Grid che si

sono registrati con Grid Manager.

- È necessario aggiungere manualmente eventuali subnet per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway Grid Network.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.
Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1

172.16.0.0/21

+

Discover Grid Network subnets

3. Fare clic su **Avanti**.

Approva i nodi della griglia in sospeso

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

Prima di iniziare

Sono stati distribuiti tutti i nodi griglia virtuali e degli appliance StorageGRID .



È più efficiente eseguire un'unica installazione di tutti i nodi, piuttosto che installare alcuni nodi ora e altri in seguito.

Passi

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



Se un nodo della griglia risulta mancante, verificare che sia stato distribuito correttamente e che abbia impostato l'IP di rete della griglia corretto del nodo di amministrazione primario per ADMIN_IP.

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



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

<

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

✎ Edit ↺ Reset ✕ Remove		Search Q				
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
◀ ▶						

3. Fare clic su **Approva**.

4. Nelle Impostazioni generali, modificare le impostazioni per le seguenti proprietà, se necessario:

- **Sito**: il nome di sistema del sito per questo nodo della griglia.
- **Nome**: il nome di sistema per il nodo. Il nome predefinito è quello specificato durante la configurazione del nodo.

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

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



Assicurarsi che almeno due nodi in ogni sito possano accedere ad almeno quattro fonti NTP esterne. Se solo un nodo in un sito riesce a raggiungere le sorgenti NTP, si verificheranno problemi di temporizzazione se quel nodo non funziona. Inoltre, la designazione di due nodi per sito come fonti NTP primarie garantisce una temporizzazione accurata se un sito è isolato dal resto della griglia.

- **Tipo di archiviazione** (solo nodi di archiviazione): specifica che un nuovo nodo di archiviazione deve essere utilizzato esclusivamente per i dati, solo per i metadati o per entrambi. Le opzioni sono **Dati e metadati** ("combinati"), **Solo dati** e **Solo metadati**.



Vedere "[Tipi di nodi di archiviazione](#)" per informazioni sui requisiti per questi tipi di nodo.

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

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

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

Il gateway è necessario se sono presenti più subnet della griglia.



Se hai selezionato DHCP per la configurazione della rete Grid e modifichi il valore qui, il nuovo valore verrà configurato come indirizzo statico sul nodo. È necessario assicurarsi che l'indirizzo IP configurato non sia compreso in un pool di indirizzi DHCP.

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

Immettere le subnet di destinazione delle rotte in uscita da questa interfaccia nella casella di testo **Subnet (CIDR)**. Se sono presenti più subnet di amministrazione, è necessario il gateway di amministrazione.



Se hai selezionato DHCP per la configurazione della rete di amministrazione e modifichi il valore qui, il nuovo valore verrà configurato come indirizzo statico sul nodo. È necessario assicurarsi che l'indirizzo IP configurato non sia compreso in un pool di indirizzi DHCP.

Appliance: per un'appliance StorageGRID, se la rete di amministrazione non è stata configurata durante l'installazione iniziale tramite StorageGRID Appliance Installer, non può essere configurata in questa finestra di dialogo Grid Manager. Invece, devi seguire questi passaggi:

- a. Riavviare l'appliance: nell'Appliance Installer, selezionare **Avanzate > Riavvia**.

Il riavvio può richiedere diversi minuti.

- b. Selezionare **Configura rete > Configurazione collegamento** e abilitare le reti appropriate.
- c. Selezionare **Configura rete > Configurazione IP** e configurare le reti abilitate.
- d. Torna alla Home page e clicca su **Avvia installazione**.

- e. In Grid Manager: se il nodo è elencato nella tabella Nodi approvati, rimuoverlo.
- f. Rimuovere il nodo dalla tabella Nodi in sospeso.
- g. Attendi che il nodo riappaia nell'elenco dei nodi in sospeso.
- h. Verificare di poter configurare le reti appropriate. Dovrebbero già essere compilati con le informazioni fornite nella pagina Configurazione IP dell'Appliance Installer.

Per ulteriori informazioni, consultare le istruzioni di installazione del modello di elettrodomestico in uso.

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



Se hai selezionato DHCP per la configurazione della rete client e modifichi il valore qui, il nuovo valore verrà configurato come indirizzo statico sul nodo. È necessario assicurarsi che l'indirizzo IP configurato non sia compreso in un pool di indirizzi DHCP.

Appliance: per un'appliance StorageGRID , se la rete client non è stata configurata durante l'installazione iniziale tramite StorageGRID Appliance Installer, non può essere configurata in questa finestra di dialogo Grid Manager. Invece, devi seguire questi passaggi:

- a. Riavviare l'appliance: nell'Appliance Installer, selezionare **Avanzate > Riavvia**.

Il riavvio può richiedere diversi minuti.

- b. Selezionare **Configura rete > Configurazione collegamento** e abilitare le reti appropriate.
- c. Selezionare **Configura rete > Configurazione IP** e configurare le reti abilitate.
- d. Torna alla Home page e clicca su **Avvia installazione**.
- e. In Grid Manager: se il nodo è elencato nella tabella Nodi approvati, rimuoverlo.
- f. Rimuovere il nodo dalla tabella Nodi in sospeso.
- g. Attendi che il nodo riappaia nell'elenco dei nodi in sospeso.
- h. Verificare di poter configurare le reti appropriate. Dovrebbero già essere compilati con le informazioni fornite nella pagina Configurazione IP dell'Appliance Installer.

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

8. Fare clic su **Salva**.

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



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

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

Devi approvare tutti i nodi che desideri nella griglia. Tuttavia, puoi 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 della griglia, fare clic su **Avanti**.

Specificare le informazioni del server Network Time Protocol

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

Informazioni su questo compito

È necessario specificare gli indirizzi IPv4 per i server NTP.

È necessario specificare server NTP esterni. I server NTP specificati devono utilizzare il protocollo NTP.

Per evitare problemi di deriva temporale, è necessario specificare quattro riferimenti al server NTP di Stratum 3 o superiore.



Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Ora di Windows (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio orario delle versioni precedenti di Windows non è sufficientemente preciso e non è supportato da Microsoft per l'uso in ambienti ad alta precisione, come StorageGRID.

["Limite di supporto per configurare il servizio Ora di Windows per ambienti ad alta precisione"](#)

I server NTP esterni vengono utilizzati dai nodi a cui sono stati precedentemente assegnati ruoli NTP primari.



Assicurarsi che almeno due nodi in ogni sito possano accedere ad almeno quattro fonti NTP esterne. Se solo un nodo in un sito riesce a raggiungere le sorgenti NTP, si verificheranno problemi di temporizzazione se quel nodo non funziona. Inoltre, la designazione di due nodi per sito come fonti NTP primarie garantisce una temporizzazione accurata se un sito è isolato dal resto della griglia.

Passi

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 ulteriori voci del server.

The screenshot shows the 'NetApp® StorageGRID®' installation wizard. The progress bar at the top indicates the current step is '5 NTP', with previous steps '1 License', '2 Sites', '3 Grid Network', and '4 Grid Nodes' completed, and subsequent steps '6 DNS', '7 Passwords', and '8 Summary' pending. Below the progress bar, the 'Network Time Protocol' section is active. It contains the instruction: 'Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.' There are four input fields labeled 'Server 1' through 'Server 4'. The values entered are: Server 1: 10.60.248.183, Server 2: 10.227.204.142, Server 3: 10.235.48.111, and Server 4: 0.0.0.0. A plus sign (+) is visible to the right of the Server 4 field, indicating an option to add more servers.

Server	IP Address
Server 1	10.60.248.183
Server 2	10.227.204.142
Server 3	10.235.48.111
Server 4	0.0.0.0

3. Selezionare **Avanti**.

Specificare le informazioni del server DNS

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

Informazioni su questo compito

Specificando ["Informazioni sul server DNS"](#) consente di utilizzare nomi host FQDN (Fully Qualified Domain Name) anziché indirizzi IP per le notifiche e-mail e AutoSupport.

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

Se possibile, utilizzare server DNS a cui ogni sito possa accedere localmente per garantire che un sito isolato possa risolvere gli FQDN per le destinazioni esterne.

Passi

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 ulteriori voci del server.

The screenshot shows the NetApp StorageGRID installation wizard. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is visible. It contains a text box for "Server 1" with the IP address "10.224.223.130" and a red "X" icon. Below that, there's a "Server 2" entry with the IP address "10.224.223.136" and a red "X" icon. To the left of the "Server 2" entry, there's a plus sign icon.

La procedura migliore è specificare almeno due server DNS. È possibile specificare fino a sei server DNS.

3. Selezionare **Avanti**.

Specificare le password del sistema StorageGRID

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

Informazioni su questo compito

Utilizzare la pagina Installa password per specificare la passphrase di provisioning e la password dell'utente root per la 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 conservare la passphrase di provisioning in un luogo sicuro.
- È possibile modificare la passphrase di provisioning da Grid Manager se si dispone di quella attuale.
- La password dell'utente root per la gestione della griglia può essere modificata tramite Grid Manager.

- Le password della console della riga di comando e SSH generate casualmente vengono memorizzate nel `Passwords.txt` file nel pacchetto di ripristino.

Passi

1. In **Provisioning Passphrase**, immettere la passphrase di provisioning che sarà necessaria per apportare modifiche alla topologia della griglia del sistema StorageGRID .

Conservare la passphrase di provisioning in un luogo sicuro.



Se dopo il completamento dell'installazione si desidera modificare la passphrase di provisioning in un secondo momento, è possibile utilizzare Grid Manager. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.

2. In **Conferma passphrase di provisioning**, reinserisci la passphrase di provisioning per confermarla.
3. In **Password utente root di Grid Management**, immettere la password da utilizzare per accedere a Grid Manager come utente "root".

Conservare la password in un luogo sicuro.

4. In **Conferma password utente root**, reinserisci la password di Grid Manager per confermarla.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 **Passwords** 8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning Passphrase

Confirm Provisioning Passphrase

Grid Management Root User Password

Confirm Root User Password

☒ Create random command line passwords.

5. Se si installa una griglia a scopo dimostrativo o di prova del concetto, è possibile deselegionare la casella di controllo **Crea password casuali per la riga di comando**.

Per le distribuzioni di produzione, per motivi di sicurezza è sempre opportuno utilizzare password casuali. Deseleziona **Crea password casuali per la riga di comando** solo per le griglie demo se vuoi utilizzare password predefinite per accedere ai nodi della griglia dalla riga di comando utilizzando l'account "root" o "admin".



Ti verrà chiesto di scaricare il file del pacchetto di ripristino(`sgws-recovery-package-id-revision.zip`) dopo aver cliccato su **Installa** nella pagina Riepilogo. Devi "[scarica questo file](#)" per completare l'installazione. Le password necessarie per accedere al sistema sono memorizzate nel `Passwords.txt` file, contenuto nel file Recovery Package.

6. Fare clic su **Avanti**.

Rivedi la tua configurazione e completa l'installazione

È necessario rivedere attentamente le informazioni di configurazione immesse per garantire che l'installazione venga completata correttamente.

Passi

1. Visualizza la pagina **Riepilogo**.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 **Summary**

Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1 dc1-g1 dc1-s1 dc1-s2 dc1-s3 NetApp-SGA		

2. Verificare che tutte le informazioni sulla configurazione della griglia siano corrette. Utilizzare i link Modifica nella pagina 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 Grid alla rete client quando si fa clic su **Installa**. Se si perde la connettività, è necessario assicurarsi di accedere al nodo di amministrazione primario tramite una subnet accessibile. Vedere "[Linee guida per il networking](#)" per i dettagli.

4. Fare clic su **Scarica pacchetto di ripristino**.

Quando l'installazione procede fino al punto in cui viene definita la topologia della griglia, viene richiesto di scaricare il file del pacchetto di ripristino(. zip) e conferma di poter accedere correttamente al contenuto di questo file. È necessario scaricare il file Recovery Package per poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi della griglia. L'installazione continua in background, ma non sarà possibile completarla e accedere al sistema StorageGRID finché non si scarica e si verifica questo file.

5. Verificare che sia possibile estrarre il contenuto del . zip file e salvarlo in due posizioni sicure, protette 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. Seleziona la casella di controllo **Ho scaricato e verificato correttamente il file del pacchetto di ripristino** e fai 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.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

							Search
Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage
dc1-adm1		Site1		172.16.4.215/21			Starting services
dc1-g1		Site1		172.16.4.216/21			Complete
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed

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

7. Sign in a Grid Manager utilizzando l'utente "root" e la password specificati durante l'installazione.

Linee guida post-installazione

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

- Se è stato utilizzato DHCP per assegnare gli indirizzi IP, configurare una prenotazione DHCP per ciascun indirizzo IP sulle reti utilizzate.

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



I nodi si riavviano quando la configurazione della rete Grid viene modificata da DHCP, il che può causare interruzioni se una modifica DHCP interessa più nodi contemporaneamente.

- È necessario utilizzare le procedure di modifica IP se si desidera modificare gli indirizzi IP, le maschere di sottorete e i gateway predefiniti per un nodo della griglia. Vedere ["Configurare gli indirizzi IP"](#) .
- Se si apportano modifiche alla configurazione di rete, tra cui 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 apportate alla rete, potrebbe essere necessario ristabilire queste connessioni.

Installazione REST API

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

L'API utilizza la piattaforma API open source Swagger per fornire la documentazione API. Swagger consente sia agli sviluppatori sia ai non sviluppatori di interagire con l'API tramite un'interfaccia utente che illustra come l'API risponde a parametri e opzioni. Questa documentazione presuppone che tu abbia familiarità con le tecnologie web standard e con il formato dati JSON.



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

Ogni comando API REST include l'URL dell'API, un'azione HTTP, eventuali parametri URL obbligatori o facoltativi e una risposta API prevista.

API di installazione StorageGRID

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

Per accedere alla documentazione API, vai alla pagina web di installazione sul nodo di amministrazione principale e seleziona **Aiuto > Documentazione API** dalla barra dei menu.

L'API di installazione StorageGRID include le seguenti sezioni:

- **config** — Operazioni relative alla versione del prodotto e alle versioni dell'API. È possibile elencare la versione del prodotto e le principali versioni dell'API supportate da tale versione.
- **grid** — Operazioni di configurazione a livello di griglia. È possibile ottenere e aggiornare le impostazioni della griglia, inclusi i dettagli della griglia, le subnet della rete Grid, 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 della griglia, eliminare un nodo della griglia, configurare un nodo della griglia, visualizzare un nodo della griglia e reimpostare la configurazione di un nodo della griglia.
- **provision** — Operazioni di provisioning. È possibile avviare l'operazione di provisioning e visualizzarne lo stato.
- **recupero** — Operazioni di recupero del nodo amministrativo primario. È possibile reimpostare 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.
- **siti** — Operazioni di configurazione a livello di sito. È possibile creare, visualizzare, eliminare e modificare un sito.
- **temporary-password** — Operazioni sulla password temporanea per proteggere mgmt-api durante l'installazione.

Dove andare dopo

Dopo aver completato l'installazione, eseguire le attività di integrazione e configurazione richieste. È possibile eseguire le attività facoltative in base alle proprie esigenze.

Compiti richiesti

- ["Crea un account inquilino"](#) per il protocollo client S3 che verrà utilizzato per archiviare gli oggetti sul sistema StorageGRID .
- ["Controllo dell'accesso al sistema"](#) configurando gruppi e account utente. Facoltativamente, puoi ["configurare una fonte di identità federata"](#) (ad esempio Active Directory o OpenLDAP), in modo da poter importare gruppi di amministrazione e utenti. Oppure puoi ["creare gruppi e utenti locali"](#) .
- Integrare e testare il ["S3 API"](#) applicazioni client che utilizzerai per caricare oggetti sul tuo sistema StorageGRID .
- ["Configurare le regole di gestione del ciclo di vita delle informazioni \(ILM\) e la politica ILM"](#) che si desidera utilizzare per proteggere i dati degli oggetti.
- Se l'installazione include nodi di archiviazione dell'appliance, utilizzare SANtricity OS per completare le seguenti attività:
 - Connettersi a ciascun dispositivo StorageGRID .
 - Verificare la ricezione dei dati AutoSupport .Vedere ["Configurare l'hardware"](#) .
- Rivedi e segui il ["Linee guida per il rafforzamento del sistema StorageGRID"](#) per eliminare i rischi per la sicurezza.
- ["Configurare le notifiche e-mail per gli avvisi di sistema"](#) .

Attività facoltative

- ["Aggiorna gli indirizzi IP dei nodi della griglia"](#) se sono cambiati da quando hai pianificato la distribuzione e generato il pacchetto di ripristino.
- ["Configurare la crittografia dell'archiviazione"](#), se necessario.
- ["Configurare la compressione dell'archiviazione"](#) per ridurre le dimensioni degli oggetti memorizzati, se necessario.
- ["Configurare le interfacce VLAN"](#) per isolare e partizionare il traffico di rete, se necessario.
- ["Configurare gruppi ad alta disponibilità"](#) per migliorare la disponibilità della connessione per i client Grid Manager, Tenant Manager e S3, se necessario.
- ["Configurare gli endpoint del bilanciamento del carico"](#) per la connettività client S3, se necessario.

Risolvere i problemi di installazione

Se si verificano problemi durante l'installazione del sistema StorageGRID , è possibile accedere ai file di registro dell'installazione. Potrebbe anche essere necessario che il supporto tecnico utilizzi i file di registro dell'installazione per risolvere i problemi.

I seguenti file di registro di installazione sono disponibili dal contenitore che esegue ciascun nodo:

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

I seguenti file di registro dell'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 ["Raccogli file di registro e dati di sistema"](#) .

Informazioni correlate

["Risoluzione dei problemi di un sistema StorageGRID"](#)

Esempio /etc/sysconfig/network-scripts

È possibile utilizzare i file di esempio per aggregare quattro interfacce fisiche Linux in un singolo legame LACP e quindi stabilire tre interfacce VLAN che sottendono il legame da utilizzare come interfacce StorageGRID Grid, Admin e Client Network.

Interfacce fisiche

Si noti che gli switch alle altre estremità dei collegamenti devono anche trattare le quattro porte come un singolo trunk LACP o canale porta e devono passare almeno le tre VLAN referenziate 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 di legame

/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
```

Installa StorageGRID su Ubuntu o Debian

Guida rapida all'installazione di StorageGRID su Ubuntu o Debian

Per installare un nodo StorageGRID Ubuntu o Debian, seguire questi passaggi generali.

1

Preparazione

- Scopri di più "[Architettura StorageGRID e topologia di rete](#)".
- Scopri le specifiche di "[Rete StorageGRID](#)".
- Raccogliere e preparare il "[Informazioni e materiali richiesti](#)".
- Preparare il necessario "[CPU e RAM](#)".
- Provvedere a "[requisiti di archiviazione e prestazioni](#)".
- "[Preparare i server Linux](#)" che ospiterà i tuoi nodi StorageGRID.

2

Distribuzione

Distribuisci i nodi della griglia. Quando si distribuiscono i nodi della griglia, questi vengono creati come parte

del sistema StorageGRID e connessi a una o più reti.

- Per distribuire nodi di griglia basati su software sugli host preparati nel passaggio 1, utilizzare la riga di comando di Linux e ["file di configurazione del nodo"](#) .
- Per distribuire i nodi dell'appliance StorageGRID , seguire le istruzioni ["Avvio rapido per l'installazione dell'hardware"](#) .

3

Configurazione

Quando tutti i nodi sono stati distribuiti, utilizzare 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 della griglia.

- Utilizzare 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 contenitore e del servizio host StorageGRID
 - Distribuzione di nodi di griglia virtuali

Vedere ["Automatizza l'installazione e la configurazione del servizio host StorageGRID"](#) .

- Dopo aver distribuito i nodi della griglia, ["automatizzare la configurazione del sistema StorageGRID"](#) utilizzando lo script di configurazione Python fornito nell'archivio di installazione.
- ["Automatizzare l'installazione e la configurazione dei nodi della griglia degli elettrodomestici"](#)
- Se sei uno sviluppatore avanzato di distribuzioni StorageGRID , automatizza l'installazione dei nodi della griglia utilizzando ["installazione REST API"](#) .

Pianificare e preparare l'installazione su Ubuntu o Debian

Informazioni e materiali richiesti

Prima di installare StorageGRID, raccogliere e preparare le informazioni e i materiali richiesti.

Informazioni richieste

Piano di rete

Quali reti intendi collegare a ciascun nodo StorageGRID . StorageGRID supporta più reti per la separazione del traffico, la sicurezza e la praticità amministrativa.

Vedi StorageGRID ["Linee guida per il networking"](#) .

Informazioni di rete

Indirizzi IP da assegnare a ciascun nodo della griglia e gli indirizzi IP dei server DNS e NTP.

Server per nodi di griglia

Identifica un set di server (fisici, virtuali o entrambi) che, nel complesso, forniscano risorse sufficienti a supportare il numero e il tipo di nodi StorageGRID che intendi distribuire.



Se l'installazione StorageGRID non utilizzerà i nodi StorageGRID (hardware) dell'appliance StorageGRID, è necessario utilizzare un archivio RAID hardware con cache di scrittura con batteria di backup (BBWC). StorageGRID non supporta l'uso di reti di archiviazione virtuali (vSAN), RAID software o nessuna protezione RAID.

Migrazione dei nodi (se necessario)

Capire il ["requisiti per la migrazione dei nodi"](#), se si desidera eseguire una manutenzione programmata sugli host fisici senza alcuna interruzione del servizio.

Informazioni correlate

["Strumento matrice di interoperabilità NetApp"](#)

Materiali richiesti

Licenza NetApp StorageGRID

È necessario disporre di una licenza NetApp valida e firmata digitalmente.



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

Archivio di installazione di StorageGRID

["Scarica l'archivio di installazione StorageGRID ed estrai i file"](#).

Computer portatile di servizio

Il sistema StorageGRID viene installato tramite un laptop di servizio.

Il portatile di servizio deve avere:

- Porta di rete
- Client SSH (ad esempio, PuTTY)
- ["Browser web supportato"](#)

Documentazione StorageGRID

- ["Note di rilascio"](#)
- ["Istruzioni per la gestione di StorageGRID"](#)

Scarica ed estrai i file di installazione StorageGRID

È necessario scaricare l'archivio di installazione StorageGRID ed estrarre i file richiesti. Facoltativamente, è possibile verificare manualmente i file nel pacchetto di installazione.

Passi

1. Vai al ["Pagina di download di NetApp per StorageGRID"](#).
2. Seleziona il pulsante per scaricare l'ultima versione oppure seleziona un'altra versione dal menu a discesa e seleziona **Vai**.

3. Sign in con il nome utente e la password del tuo account NetApp .
4. Se viene visualizzata una dichiarazione di Attenzione/Lettura obbligatoria, leggerla e selezionare la casella di controllo.



Dopo aver installato la versione StorageGRID , è necessario applicare tutti gli hotfix richiesti. Per maggiori informazioni, vedere il ["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 **Accetta e continua**.
6. Nella colonna **Installa StorageGRID**, seleziona l'archivio di installazione .tgz o .zip per Ubuntu o Debian.



Seleziona il .zip file se si utilizza Windows sul portatile di servizio.

7. Salvare l'archivio di installazione.
8. Se devi verificare l'archivio di installazione:
 - a. Scarica il pacchetto di verifica della firma del codice StorageGRID . Il nome del file per questo pacchetto utilizza il formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , Dove `<version-number>` è la versione del software StorageGRID .
 - b. Segui i passaggi per ["verificare manualmente i file di installazione"](#) .
9. Estrarre i file dall'archivio di installazione.
10. Scegli i file di cui hai bisogno.

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



I percorsi elencati nella tabella sono relativi alla directory di livello superiore 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 StorageGRID .
	Un file di licenza NetApp non di produzione che puoi utilizzare per test e distribuzioni di prova di concetto.
	Pacchetto DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.
	Checksum MD5 per il file <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Pacchetto DEB per l'installazione del servizio host StorageGRID su host Ubuntu o Debian.

Percorso e nome del file	Descrizione
Strumento di scripting di distribuzione	Descrizione
	Uno script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID .
	Uno script Python utilizzato per automatizzare la configurazione degli appliance StorageGRID .
	Uno script Python di esempio che puoi utilizzare per accedere all'API di gestione della griglia quando è abilitato l'accesso singolo. È possibile utilizzare questo script anche per l'integrazione di Ping Federate.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Esempio di ruolo e playbook Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID . È possibile personalizzare il ruolo o il playbook in base alle proprie esigenze.
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO) tramite Active Directory o Ping Federate.
	Uno script di supporto chiamato dal compagno <code>storagegrid-ssoauth-azure.py</code> Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: prima di eseguire un aggiornamento, puoi utilizzare questi schemi per confermare che il codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova versione StorageGRID se non disponi di un ambiente StorageGRID non di produzione per i test di compatibilità dell'aggiornamento.

Verifica manuale dei file di installazione (facoltativo)

Se necessario, è possibile verificare manualmente i file nell'archivio di installazione StorageGRID .

Prima di iniziare

Hai [scaricato il pacchetto di verifica](#) dal ["Pagina di download di NetApp per StorageGRID"](#) .

Passi

1. Estrarre gli artefatti dal pacchetto di verifica:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Assicurarsi che questi artefatti siano stati estratti:

- Certificato fogliare: Leaf-Cert.pem
- Catena di certificati: CA-Int-Cert.pem
- Catena di risposta del timestamp: TS-Cert.pem
- File di checksum: sha256sum
- Firma di checksum: sha256sum.sig
- File di risposta con timestamp: sha256sum.sig.tsr

3. Utilizzare la catena per verificare che il certificato fogliare sia valido.

Esempio: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Risultati previsti: Leaf-Cert.pem: OK

4. Se il passaggio 2 non è riuscito a causa di un certificato foglia scaduto, utilizzare tsr file da verificare.

Esempio: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

I risultati previsti includono: Verification: OK

5. Creare un file di chiave pubblica dal certificato foglia.

Esempio: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Risultato previsto: *nessuno*

6. Utilizzare la chiave pubblica per verificare il sha256sum presentare ricorso contro sha256sum.sig .

Esempio: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Risultati previsti: Verified OK

7. Verificare il sha256sum il contenuto del file rispetto ai checksum appena creati.

Esempio: `sha256sum -c sha256sum`

Risultati previsti: `<filename>`: OK

`<filename>` è il nome del file di archivio che hai scaricato.

8. **"Completa i passaggi rimanenti"** per estrarre e scegliere i file di installazione appropriati.

Requisiti software per Ubuntu e Debian

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

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 del pacchetto software su cui vengono testate le installazioni StorageGRID includono quelle elencate in questa pagina.

Se selezioni un'opzione di installazione della distribuzione Linux e del runtime del contenitore che richiede uno qualsiasi di questi pacchetti e questi non vengono installati automaticamente dalla distribuzione Linux, installa una delle versioni elencate qui, se disponibile dal tuo provider o dal fornitore di supporto per la tua distribuzione Linux. In caso contrario, utilizzare le versioni predefinite del pacchetto messe a disposizione dal fornitore.

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



Il supporto per Docker come motore di container per distribuzioni esclusivamente software è deprecato. Docker verrà sostituito con un altro motore di container in una versione futura.

Versioni di 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 Docker testate



Il supporto Docker è obsoleto e verrà rimosso in una versione 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 CPU e RAM

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

Ogni nodo StorageGRID richiede le seguenti risorse minime:

- Core CPU: 8 per nodo
- RAM: Dipende dalla RAM totale disponibile e dalla quantità di software non StorageGRID in esecuzione sul sistema
 - In genere, almeno 24 GB per nodo e da 2 a 16 GB in meno rispetto alla RAM totale del sistema
 - Un minimo di 64 GB per ogni tenant che avrà circa 5.000 bucket

Le risorse dei nodi basati solo su metadati software devono corrispondere alle risorse dei nodi di archiviazione esistenti. Per esempio:

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

Quando si aggiunge un nuovo sito StorageGRID , la capacità totale dei metadati del nuovo sito deve corrispondere almeno ai siti StorageGRID esistenti e le risorse del nuovo sito devono corrispondere ai nodi di archiviazione nei siti StorageGRID esistenti.

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



Monitora regolarmente l'utilizzo della CPU e della memoria per assicurarti che queste risorse continuino a soddisfare il tuo carico di lavoro. Ad esempio, raddoppiando l'allocazione di RAM e CPU per i nodi di archiviazione virtuali si otterrebbero risorse simili a quelle fornite per i nodi dell'appliance StorageGRID. Inoltre, se la quantità di metadati per nodo supera i 500 GB, valutare di aumentare la RAM per nodo a 48 GB o più. Per informazioni sulla gestione dell'archiviazione dei metadati degli oggetti, sull'aumento dell'impostazione Spazio riservato ai metadati e sul monitoraggio dell'utilizzo della CPU e della memoria, vedere le istruzioni per ["amministrare"](#), ["monitoraggio"](#), e ["aggiornamento"](#) StorageGRID.

Se l'hyperthreading è abilitato sugli host fisici sottostanti, è possibile fornire 8 core virtuali (4 core fisici) per nodo. Se l'hyperthreading non è abilitato 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 VM, è consigliabile utilizzare una singola VM per ogni nodo StorageGRID e dimensionare la VM di conseguenza.

Per le distribuzioni di produzione, non dovresti eseguire più nodi di archiviazione sullo stesso hardware di archiviazione fisico o host virtuale. Ogni nodo di archiviazione in una singola distribuzione StorageGRID dovrebbe trovarsi nel proprio dominio di errore isolato. È possibile massimizzare la durabilità e la disponibilità dei dati degli oggetti se ci si assicura che un singolo guasto hardware possa avere un impatto solo su un singolo nodo di archiviazione.

Vedere anche ["Requisiti di archiviazione e prestazioni"](#).

Requisiti di archiviazione e prestazioni

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

I nodi StorageGRID richiedono tre categorie logiche di archiviazione:

- **Pool di contenitori:** archiviazione a livello di prestazioni (SAS o SSD da 10K) per i contenitori dei nodi, che verrà assegnata al driver di archiviazione Docker quando installi e configuri Docker sugli host che supporteranno i tuoi nodi StorageGRID.
- **Dati di sistema** — Archiviazione a livello di prestazioni (SAS o SSD da 10K) per l'archiviazione persistente per nodo dei dati di sistema e dei registri delle transazioni, che i servizi host StorageGRID utilizzeranno e mapperanno nei singoli nodi.
- **Dati oggetto** - Archiviazione di livello prestazionale (SAS o SSD da 10K) e archiviazione di massa di livello di capacità (NL-SAS/SATA) per l'archiviazione persistente di dati oggetto e metadati oggetto.

È necessario utilizzare dispositivi a blocchi con supporto RAID per tutte le categorie di archiviazione. Non sono supportati dischi non ridondanti, SSD o JBOD. È possibile utilizzare l'archiviazione RAID condivisa o locale per qualsiasi categoria di archiviazione; tuttavia, se si desidera utilizzare la funzionalità di migrazione dei nodi in StorageGRID, è necessario archiviare sia i dati di sistema sia i dati degli oggetti nell'archiviazione condivisa. Per ulteriori informazioni, consultare ["Requisiti per la migrazione dei contenitori dei nodi"](#).

Requisiti di prestazione

Le prestazioni dei volumi utilizzati per il pool di contenitori, i dati di sistema e i metadati degli oggetti influiscono in modo significativo sulle prestazioni complessive del sistema. Per questi volumi è consigliabile utilizzare un archivio di livello prestazionale (SAS o SSD da 10K) per garantire prestazioni del disco adeguate in termini di latenza, operazioni di input/output al secondo (IOPS) e throughput. È possibile utilizzare l'archiviazione a livelli di capacità (NL-SAS/SATA) per l'archiviazione persistente dei dati degli oggetti.

I volumi utilizzati per il pool di contenitori, i dati di sistema e i dati degli oggetti devono avere la memorizzazione nella cache write-back abilitata. La cache deve trovarsi su un supporto protetto o persistente.

Requisiti per gli host che utilizzano l'archiviazione NetApp ONTAP

Se il nodo StorageGRID utilizza storage assegnato da un sistema NetApp ONTAP, verificare che il volume non abbia un criterio di suddivisione in livelli FabricPool abilitato. La disattivazione della suddivisione in livelli FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di archiviazione.



Non utilizzare mai FabricPool per riportare i dati relativi a StorageGRID a StorageGRID stesso. Il riordino dei dati StorageGRID su StorageGRID aumenta la complessità operativa e la risoluzione dei problemi.

Numero di host richiesti

Ogni sito StorageGRID richiede un minimo di tre nodi di archiviazione.



In una distribuzione di produzione, non eseguire più di un nodo di archiviazione su un singolo host fisico o virtuale. Utilizzando un host dedicato per ogni nodo di archiviazione si ottiene un dominio di errore isolato.

Altri tipi di nodi, come i nodi amministrativi o i nodi gateway, possono essere distribuiti sugli stessi host oppure possono essere distribuiti sui propri host dedicati, a seconda delle necessità.

Numero di volumi di archiviazione per ciascun host

Nella tabella seguente viene mostrato il numero di volumi di archiviazione (LUN) richiesti per ciascun host e la dimensione minima richiesta per ogni LUN, in base ai nodi che verranno distribuiti su tale host.

La dimensione massima della LUN testata è 39 TB.



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

Scopo LUN	Categoria di archiviazione	Numero di LUN	Dimensione minima/LUN
Piscina di stoccaggio per motori container	Piscina di contenitori	1	Numero totale di nodi × 100 GB
`/var/local` volumi	Dati di sistema	1 per ogni nodo su questo host	90 GB

Scopo LUN	Categoria di archiviazione	Numero di LUN	Dimensione minima/LUN
Nodo di archiviazione	Dati oggetto	3 per ogni nodo di archiviazione su questo host Nota: un nodo di archiviazione basato su software può avere da 1 a 48 volumi di archiviazione; si consigliano almeno 3 volumi di archiviazione.	12 TB (4 TB/LUN) Vedi Requisiti di archiviazione per i nodi di archiviazione per maggiori informazioni.
Nodo di archiviazione (solo metadati)	Metadati dell'oggetto	1	4 TB Vedi Requisiti di archiviazione per i nodi di archiviazione per maggiori informazioni. Nota: per i nodi di archiviazione solo metadati è richiesto un solo rangedb.
Registri di controllo del nodo di amministrazione	Dati di sistema	1 per ogni nodo amministrativo su questo host	200 GB
Tabelle dei nodi di amministrazione	Dati di sistema	1 per ogni nodo amministrativo su questo host	200 GB



A seconda del livello di controllo configurato, delle dimensioni degli input utente, come il nome della chiave dell'oggetto S3, e della quantità di dati del registro di controllo da conservare, potrebbe essere necessario aumentare le dimensioni della LUN del registro di controllo su ciascun nodo di amministrazione. In genere, una griglia genera circa 1 KB di dati di controllo per operazione S3, il che significa che una LUN da 200 GB supporterebbe 70 milioni di operazioni al giorno o 800 operazioni al secondo per due o tre giorni.

Spazio di archiviazione minimo per un host

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



Gli snapshot del disco non possono essere utilizzati per ripristinare i nodi della griglia. Fare invece riferimento al "[ripristino del nodo della griglia](#)" procedure per ogni tipo di nodo.

Tipo di nodo	Piscina di contenitori	Dati di sistema	Dati oggetto
Nodo di archiviazione	100 GB	90 GB	4.000 GB
Nodo di amministrazione	100 GB	490 GB (3 LUN)	<i>non applicabile</i>

Tipo di nodo	Piscina di contenitori	Dati di sistema	Dati oggetto
Nodo Gateway	100 GB	90 GB	<i>non applicabile</i>

Esempio: calcolo dei requisiti di archiviazione per un host

Supponiamo di voler distribuire tre nodi sullo stesso host: un nodo di archiviazione, un nodo di amministrazione e un nodo gateway. È necessario fornire all'host almeno nove volumi di archiviazione. Saranno necessari almeno 300 GB di storage di livello prestazioni per i contenitori dei nodi, 670 GB di storage di livello prestazioni per i dati di sistema e i registri delle transazioni e 12 TB di storage di livello capacità per i dati degli oggetti.

Tipo di nodo	Scopo LUN	Numero di LUN	dimensione LUN
Nodo di archiviazione	Pool di archiviazione Docker	1	300 GB (100 GB/nodo)
Nodo di archiviazione	`/var/local` volume	1	90 GB
Nodo di archiviazione	Dati oggetto	3	12 TB (4 TB/LUN)
Nodo di amministrazione	`/var/local` volume	1	90 GB
Nodo di amministrazione	Registri di controllo del nodo di amministrazione	1	200 GB
Nodo di amministrazione	Tabelle dei nodi di amministrazione	1	200 GB
Nodo Gateway	`/var/local` volume	1	90 GB
Totale		9	Pool di contenitori: 300 GB Dati di sistema: 670 GB Dati oggetto: 12.000 GB

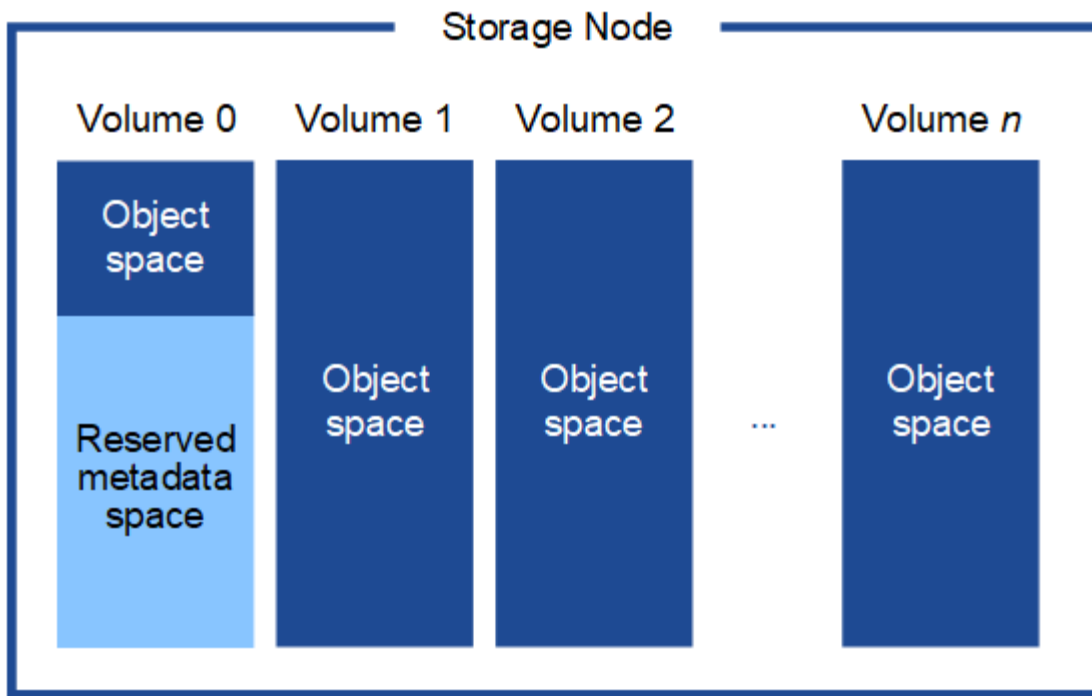
Requisiti di archiviazione per i nodi di archiviazione

Un nodo di archiviazione basato su software può avere da 1 a 48 volumi di archiviazione; si consigliano 3 o più volumi di archiviazione. Ogni volume di archiviazione deve essere pari o superiore a 4 TB.



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

Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di archiviazione 0 di ciascun nodo di archiviazione. Tutto lo spazio rimanente sul volume di archiviazione 0 e su tutti gli altri volumi di archiviazione nel nodo di archiviazione viene utilizzato esclusivamente per i dati degli oggetti.



Per garantire ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti nel sistema in ogni sito. Le tre copie dei metadati degli oggetti vengono distribuite uniformemente tra tutti i nodi di archiviazione di ciascun sito.

Quando si installa una griglia con nodi di archiviazione solo metadati, la griglia deve contenere anche un numero minimo di nodi per l'archiviazione degli oggetti. Vedere "[Tipi di nodi di archiviazione](#)" per ulteriori informazioni sui nodi di archiviazione solo metadati.

- Per una griglia a sito singolo, sono configurati almeno due nodi di archiviazione per oggetti e metadati.
- Per una griglia multi-sito, almeno un nodo di archiviazione per sito è configurato per oggetti e metadati.

Quando si assegna spazio al volume 0 di un nuovo nodo di archiviazione, è necessario assicurarsi che vi sia spazio adeguato per la porzione di tutti i metadati degli oggetti di quel nodo.

- Come minimo, è necessario assegnare almeno 4 TB al volume 0.



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



Se si assegnano meno di 500 GB al volume 0 (solo per uso non produttivo), il 10% della capacità del volume di archiviazione è riservato ai metadati.

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

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

Quando si aggiunge un nuovo sito StorageGRID , la capacità totale dei metadati del nuovo sito deve corrispondere almeno ai siti StorageGRID esistenti e le risorse del nuovo sito devono corrispondere ai nodi di archiviazione nei siti StorageGRID esistenti.

- Se si installa un nuovo sistema (StorageGRID 11.6 o versione successiva) e ogni nodo di archiviazione dispone di 128 GB o più di RAM, assegnare 8 TB o più al volume 0. Utilizzando un valore maggiore per il volume 0 è possibile aumentare lo spazio consentito per i metadati su ciascun nodo di archiviazione.
- Quando si configurano diversi nodi di archiviazione per un sito, utilizzare la stessa impostazione per il volume 0, se possibile. Se un sito contiene nodi di archiviazione di dimensioni diverse, il nodo di archiviazione con il volume più piccolo, 0, determinerà la capacità dei metadati di quel sito.

Per i dettagli, vai a ["Gestire l'archiviazione dei metadati degli oggetti"](#) .

Requisiti per la migrazione dei contenitori dei nodi

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

La migrazione dei nodi consente di eseguire la manutenzione fisica dell'host senza interrompere le operazioni della griglia. È necessario spostare tutti i nodi StorageGRID , uno alla volta, su un altro host prima di mettere offline l'host fisico. La migrazione dei nodi richiede solo un breve periodo di inattività per ciascun nodo e non dovrebbe influire sul funzionamento o sulla disponibilità dei servizi di rete.

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

- Nomi di interfaccia di rete coerenti tra gli host in un singolo data center fisico
- Archiviazione condivisa per volumi di repository di oggetti e metadati StorageGRID , accessibile a tutti gli host in un singolo data center fisico. Ad esempio, potresti utilizzare array di storage NetApp E-Series.

Se si utilizzano host virtuali e il livello hypervisor sottostante supporta la migrazione delle VM, potrebbe essere opportuno utilizzare questa funzionalità anziché la funzionalità di migrazione dei nodi in StorageGRID. In questo caso, puoi ignorare questi requisiti aggiuntivi.

Prima di eseguire la migrazione o la manutenzione dell'hypervisor, arrestare i nodi in modo corretto. Vedi le istruzioni per ["chiusura di un nodo della griglia"](#) .

VMware Live Migration non supportato

Quando si esegue un'installazione bare-metal su VM VMware, OpenStack Live Migration e VMware Live vMotion causano un salto temporale nella macchina virtuale e non sono supportati per nodi di griglia di alcun tipo. Anche se raramente, orari errati possono causare la perdita di dati o di aggiornamenti della configurazione.

È supportata la migrazione a freddo. Nella migrazione a freddo, i nodi StorageGRID vengono arrestati prima di migrarli tra gli host. Vedi le istruzioni per ["chiusura di un nodo della griglia"](#) .

Nomi di interfaccia di rete coerenti

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

Supponiamo, ad esempio, che StorageGRID NodeA in esecuzione su Host1 sia stato configurato con le seguenti mappature di interfaccia:

eth0 → bond0.1001

eth1 → bond0.1002

eth2 → bond0.1003

Il lato sinistro delle frecce corrisponde alle interfacce tradizionali visualizzate dall'interno di un contenitore StorageGRID (ovvero, rispettivamente, le interfacce Grid, Admin e Client Network). Il lato destro delle frecce corrisponde alle interfacce host effettive che forniscono queste reti, ovvero tre interfacce VLAN subordinate allo stesso legame di interfaccia fisica.

Supponiamo ora di voler migrare NodeA su Host2. Se Host2 ha anche interfacce denominate bond0.1001, bond0.1002 e bond0.1003, il sistema consentirà lo spostamento, presupponendo che le interfacce con nomi simili forniscano la stessa connettività su Host2 come su Host1. Se Host2 non ha interfacce con gli stessi nomi, lo spostamento non sarà consentito.

Esistono molti modi per ottenere una denominazione coerente dell'interfaccia di rete su più host; vedere ["Configurare la rete host"](#) per alcuni esempi.

Archiviazione condivisa

Per ottenere migrazioni dei nodi rapide e con un overhead ridotto, la funzionalità di migrazione dei nodi StorageGRID non sposta fisicamente i dati dei nodi. Invece, la migrazione dei nodi viene eseguita come una coppia di operazioni di esportazione e importazione, come segue:

Passi

1. Durante l'operazione di "esportazione del nodo", una piccola quantità di dati di stato persistenti viene estratta dal contenitore del nodo in esecuzione su HostA e memorizzata nella cache del volume di dati di sistema di quel nodo. Quindi, il contenitore del nodo su HostA viene deistanziato.
2. Durante l'operazione di "importazione del nodo", viene creato un'istanza del contenitore del nodo su HostB che utilizza la stessa interfaccia di rete e le stesse mappature di archiviazione a blocchi in vigore su HostA. Quindi, i dati sullo stato persistente memorizzati nella cache vengono inseriti nella nuova istanza.

Data questa modalità di funzionamento, tutti i dati di sistema e i volumi di archiviazione degli oggetti del nodo devono essere accessibili sia da HostA che da HostB affinché la migrazione sia consentita e funzioni. Inoltre, devono essere stati mappati nel nodo utilizzando nomi che garantiscano di fare riferimento alle stesse LUN su HostA e HostB.

L'esempio seguente mostra una soluzione per la mappatura dei dispositivi a blocchi per un nodo di archiviazione StorageGRID, in cui il multipathing DM è in uso sugli host e il campo alias è stato utilizzato in `/etc/multipath.conf` per fornire nomi di dispositivi a blocchi coerenti e intuitivi disponibili su tutti gli host.

`/var/local` → `/dev/mapper/sgws-sn1-var-local`

`rangedb0` → `/dev/mapper/sgws-sn1-rangedb0`

`rangedb1` → `/dev/mapper/sgws-sn1-rangedb1`

`rangedb2` → `/dev/mapper/sgws-sn1-rangedb2`

`rangedb3` → `/dev/mapper/sgws-sn1-rangedb3`

Preparare gli host (Ubuntu o Debian)

Come cambiano le impostazioni dell'host durante l'installazione

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

Sono state 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
```

Installa Linux

È necessario installare StorageGRID su tutti gli host grid Ubuntu o Debian. Per un elenco delle versioni supportate, utilizzare lo strumento NetApp Interoperability Matrix.

Prima di iniziare

Assicurati che il tuo sistema operativo soddisfi i requisiti minimi di versione del kernel di StorageGRID, come elencato di seguito. Utilizzare il comando `uname -r` per ottenere la versione del kernel del tuo sistema operativo oppure consulta il fornitore del sistema operativo.

Nota: il supporto per le versioni 18.04 e 20.04 di Ubuntu è stato deprecato e verrà rimosso in una versione futura.

Versione di Ubuntu	Versione minima del kernel	Nome del pacchetto del kernel
18.04.6 (obsoleto)	5.4.0-150-generic	linux-image-5.4.0-150-generic/bionic-updates,bionic-security,ora 5.4.0-150.167~18.04.1
20.04.5 (obsoleto)	5.4.0-131-generic	linux-image-5.4.0-131-generic/focal-updates, ora 5.4.0-131.147
22.04.1	5.15.0-47-generic	linux-image-5.15.0-47-generic/jammy-updates,jammy-security,ora 5.15.0-47.51
24,04	6.8.0-31-generic	linux-image-6.8.0-31-generic/noble, ora 6.8.0-31.31

Nota: il supporto per la versione 11 di Debian è stato deprecato e verrà rimosso in una versione futura.

versione Debian	Versione minima del kernel	Nome del pacchetto del kernel
11 (obsoleto)	5.10.0-18-amd64	linux-image-5.10.0-18-amd64/stable, ora 5.10.150-1
12	6.1.0-9-amd64	linux-image-6.1.0-9-amd64/stable, ora 6.1.27-1

Passi

1. Installare Linux su tutti gli host fisici o virtuali della griglia secondo le istruzioni del distributore o la procedura standard.



Non installare alcun ambiente desktop grafico. Quando si installa Ubuntu, è necessario selezionare **utilità di sistema standard**. Si consiglia di selezionare **Server OpenSSH** 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 Ubuntu o Debian.
3. Se lo swap è abilitato:
 - a. Eseguire il seguente comando: `$ sudo swapoff --all`
 - b. Rimuovi tutte le voci di swap da `/etc/fstab` per mantenere le impostazioni.



Se non si disattiva completamente lo swap, le prestazioni possono ridursi notevolmente.

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 contenitore di sistema StorageGRID, i profili AppArmor vengono bloccati. I pacchetti di base DHCP, MySQL, NTP e tcdump sono in conflitto con AppArmor e anche altri pacchetti di base potrebbero essere in conflitto.

Per gestire i profili AppArmor sono disponibili due opzioni:

- Disabilitare i singoli profili per i pacchetti installati sul sistema di base che si sovrappongono ai pacchetti nel contenitore del sistema StorageGRID. Quando si disabilitano singoli profili, nei file di registro 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
```

- Disattivare completamente AppArmor. Per Ubuntu 9.10 o versioni successive, seguire le istruzioni nella community online di Ubuntu: "[Disabilita AppArmor](#)". Potrebbe non essere possibile disabilitare completamente AppArmor nelle versioni più recenti di Ubuntu.

Dopo aver disabilitato AppArmor, nei file di registro StorageGRID non comparirà alcuna voce che indichi che AppArmor è abilitato.

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 alla mappatura nei nodi StorageGRID che verranno distribuiti in seguito.

Prima di iniziare

- Hai esaminato il ["Linee guida per la rete StorageGRID"](#) .
- Hai esaminato le informazioni su ["requisiti di migrazione del contenitore del nodo"](#) .
- Se si utilizzano host virtuali, è necessario leggere [considerazioni e raccomandazioni per la clonazione degli indirizzi MAC](#) prima di configurare la rete host.



Se si utilizzano VM come host, è necessario selezionare VMXNET 3 come scheda di rete virtuale. La scheda di rete VMware E1000 ha causato problemi di connettività con i container StorageGRID distribuiti su alcune distribuzioni di Linux.

Informazioni su questo compito

I nodi della griglia devono essere in grado di accedere alla rete della griglia e, facoltativamente, alle reti di amministrazione 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 la distribuzione su tutti gli host e 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 per l'accesso alla rete di amministrazione del nodo, per facilitare la manutenzione dell'host e del nodo. Sebbene la stessa interfaccia possa essere condivisa tra l'host e i singoli nodi, tutti devono avere indirizzi IP diversi. Gli indirizzi IP non possono essere condivisi tra i nodi o tra l'host e un nodo.

È possibile utilizzare la stessa interfaccia di rete host per fornire l'interfaccia di rete Grid per tutti i nodi StorageGRID sull'host; è possibile utilizzare un'interfaccia di rete host diversa per ciascun nodo; oppure è possibile fare una via di mezzo. Tuttavia, in genere non si fornisce la stessa interfaccia di rete host come interfaccia di rete Grid e Admin per un singolo nodo, oppure come interfaccia di rete Grid per un nodo e interfaccia di rete client per un altro.

Puoi completare questo compito in molti modi. Ad esempio, se gli host sono macchine virtuali e si distribuiscono uno o due nodi StorageGRID per ciascun host, è possibile creare il numero corretto di interfacce di rete nell'hypervisor e utilizzare una mappatura 1 a 1. Se si distribuiscono più nodi su host bare metal per uso produttivo, è possibile sfruttare il supporto dello stack di rete Linux per VLAN e LACP per la tolleranza agli errori e la condivisione della larghezza di banda. Le sezioni seguenti forniscono approcci dettagliati per entrambi gli esempi. Non è necessario utilizzare nessuno di questi esempi; puoi utilizzare qualsiasi approccio che soddisfi le tue esigenze.



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

Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC

La clonazione dell'indirizzo MAC fa sì che il contenitore utilizzi l'indirizzo MAC dell'host e che l'host utilizzi l'indirizzo MAC di un indirizzo specificato dall'utente o di uno generato casualmente. È consigliabile utilizzare la clonazione degli indirizzi MAC per evitare l'uso di configurazioni di rete in modalità promiscua.

Abilitazione della clonazione MAC

In determinati ambienti, la sicurezza può essere migliorata tramite la clonazione dell'indirizzo MAC, poiché consente di utilizzare una NIC virtuale dedicata per la rete amministrativa, la rete Grid e la rete client. Facendo in modo che il contenitore utilizzi l'indirizzo MAC della NIC dedicata sull'host, è possibile evitare di utilizzare configurazioni di rete in modalità promiscua.



La clonazione degli indirizzi MAC è pensata per essere utilizzata con installazioni di server virtuali e potrebbe non funzionare correttamente con tutte le configurazioni di dispositivi fisici.



Se un nodo non riesce ad avviarsi perché un'interfaccia di destinazione della clonazione MAC è 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 ad avviarsi perché un'interfaccia è occupata, impostare il collegamento su "inattivo" prima di avviare il nodo potrebbe risolvere il problema.

La clonazione dell'indirizzo MAC è disabilitata per impostazione predefinita e deve essere impostata tramite le chiavi di configurazione del nodo. Dovresti abilitarlo quando installi StorageGRID.

Esiste una chiave per ogni rete:

- 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 contenitore utilizzerà l'indirizzo MAC della scheda di rete dell'host. Inoltre, l'host utilizzerà l'indirizzo MAC della rete container specificata. Per impostazione predefinita, l'indirizzo del contenitore è un indirizzo generato casualmente, ma se ne hai impostato uno utilizzando `_NETWORK_MAC` chiave di configurazione del nodo, al suo posto viene utilizzato quell'indirizzo. L'host e il contenitore avranno sempre indirizzi MAC diversi.



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

Casi d'uso della clonazione MAC

Ci sono due casi d'uso da considerare con la clonazione MAC:

- Clonazione MAC non abilitata: quando il `_CLONE_MAC` chiave nel file di configurazione del nodo non è impostata o è impostata su "false", l'host utilizzerà il MAC della NIC dell'host e il contenitore avrà un MAC generato da StorageGRID a meno che non venga specificato un MAC nel `_NETWORK_MAC` chiave. Se un indirizzo è impostato nel `_NETWORK_MAC` chiave, il contenitore avrà l'indirizzo specificato nella `_NETWORK_MAC` chiave. Questa configurazione delle chiavi richiede l'uso della modalità promiscua.
- Clonazione MAC abilitata: quando il `_CLONE_MAC` la chiave nel file di configurazione del nodo è impostata su "true", il contenitore utilizza il MAC della NIC host e l'host utilizza un MAC generato da StorageGRID a meno che non venga specificato un MAC in `_NETWORK_MAC` chiave. Se un indirizzo è impostato nel `_NETWORK_MAC` chiave, l'host utilizza l'indirizzo specificato anziché uno generato. In questa configurazione di chiavi, non si dovrebbe utilizzare la modalità promiscua.



Se non si desidera utilizzare la clonazione degli indirizzi MAC e si preferisce 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 **Accetta** per Modalità promiscua, Modifiche indirizzo MAC e Trasmissioni contraffatte. 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 entrambi i punti.

Per abilitare la clonazione MAC, vedere ["Istruzioni per la creazione di file di configurazione del nodo"](#).

Esempio di clonazione MAC

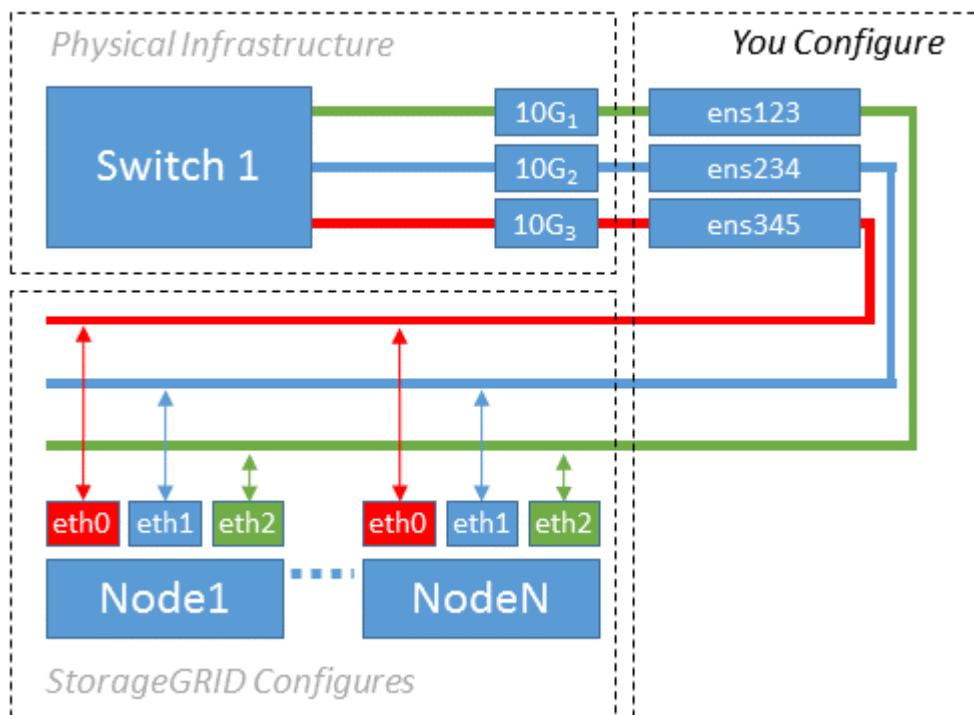
Esempio di clonazione MAC abilitata con un host con indirizzo MAC 11:22:33:44:55:66 per l'interfaccia ens256 e le seguenti chiavi nel file di configurazione del nodo:

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

Risultato: l'host MAC per ens256 è b2:9c:02:c2:27:10 e il MAC della rete di amministrazione 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 lato host minima o nulla.



Il sistema operativo Linux crea automaticamente le interfacce ensXYZ durante l'installazione o l'avvio, oppure quando le interfacce vengono aggiunte a caldo. Non è richiesta alcuna configurazione, se non quella di assicurarsi che le interfacce siano impostate per attivarsi automaticamente dopo l'avvio. È necessario determinare quale ensXYZ corrisponde a quale rete StorageGRID (Grid, Admin o Client) in modo da poter

fornire le mappature corrette in seguito nel processo di configurazione.

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

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

Esempio 2: VLAN che trasportano legami LACP

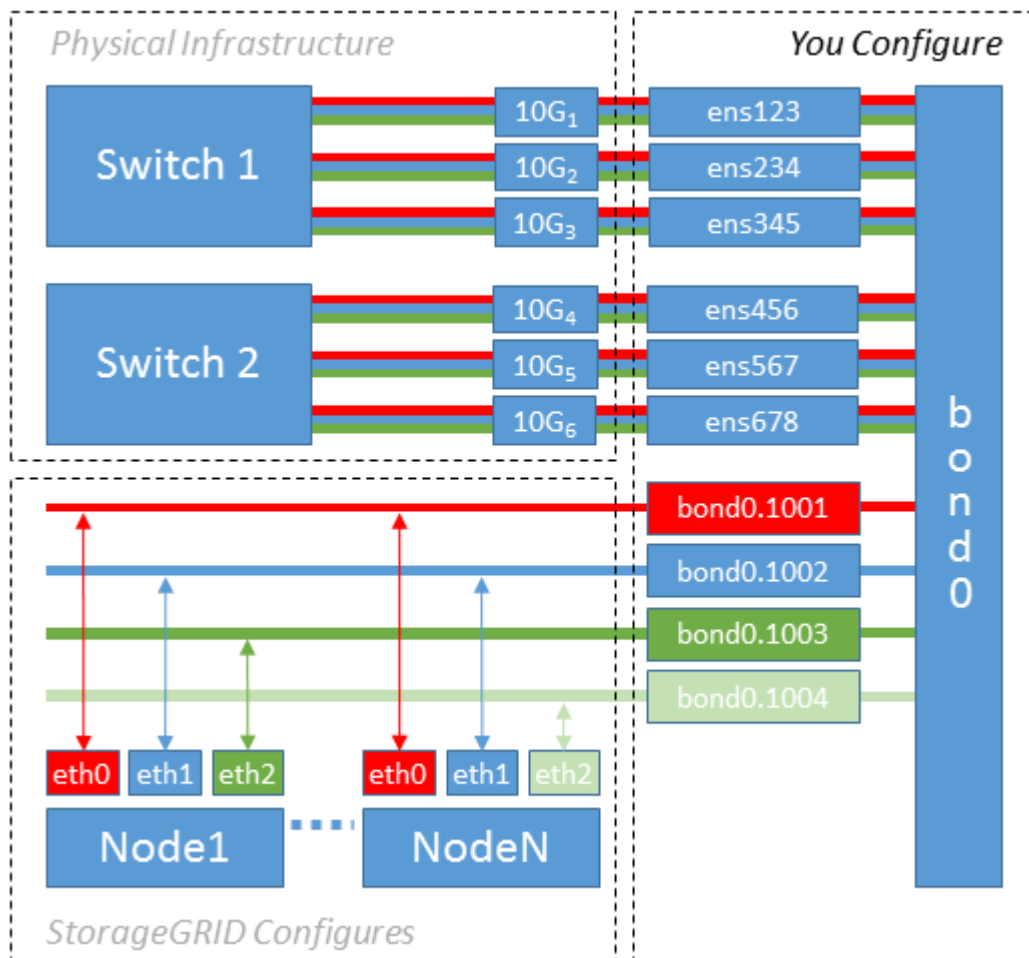
L'esempio 2 presuppone che tu abbia familiarità con il bonding delle interfacce di rete e con la creazione di interfacce VLAN sulla distribuzione Linux che stai utilizzando.

Informazioni su questo compito

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

Per comprendere questo esempio, supponiamo di avere tre subnet separate per la rete Grid, la rete Admin e la rete Client in ogni data center. Le subnet si trovano su VLAN separate (1001, 1002 e 1003) e vengono presentate all'host su una porta trunk legata a LACP (bond0). Dovresti configurare tre interfacce VLAN sul bond: bond0.1001, bond0.1002 e bond0.1003.

Se sono necessarie VLAN e subnet separate per le reti di nodi sullo stesso host, è possibile aggiungere interfacce VLAN sul bond e mapparle nell'host (mostrato come bond0.1004 nell'illustrazione).



Passi

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

Utilizzare lo stesso nome per il legame su ogni host, ad esempio bond0.

2. Creare interfacce VLAN che utilizzano questo legame come "dispositivo fisico" associato, utilizzando la convenzione di denominazione standard delle interfacce VLAN `physdev-name.VLAN ID`.

Si noti che i passaggi 1 e 2 richiedono una configurazione appropriata sugli switch edge che terminano le altre estremità dei collegamenti di rete. Anche le porte dello switch edge devono essere aggregate in un canale porta LACP, configurate come trunk e autorizzate a passare tutte le VLAN richieste.

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

Informazioni correlate

["Esempio /etc/network/interfaces"](#)

Configurare l'archiviazione host

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

Prima di iniziare

Hai esaminato i seguenti argomenti, che forniscono le informazioni necessarie per portare a termine questa attività:

- ["Requisiti di archiviazione e prestazioni"](#)
- ["Requisiti per la migrazione dei contenitori dei nodi"](#)

Informazioni su questo compito

Quando si assegnano volumi di archiviazione 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 distribuiti su tale host)
- Categoria di archiviazione per ciascun volume (ovvero, dati di sistema o dati oggetto)
- Dimensione di ogni volume

Queste informazioni, insieme al nome persistente assegnato da Linux a ciascun volume fisico, verranno utilizzate quando si distribuiscono i nodi StorageGRID sull'host.



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



Per i nodi di archiviazione solo metadati è richiesta una sola LUN di dati oggetto.

Evitare di utilizzare file di dispositivi speciali "raw" (`/dev/sdb`, ad esempio) mentre componi l'elenco dei nomi dei volumi. Questi file possono cambiare durante i riavvii dell'host, il che può influire sul corretto funzionamento del sistema. Se si utilizzano iSCSI LUN e Device Mapper Multipathing, valutare l'utilizzo di alias multipath in `/dev/mapper` directory, soprattutto se la topologia SAN include percorsi di rete ridondanti verso

l'archiviazione condivisa. In alternativa, è possibile utilizzare i collegamenti softlink creati dal sistema in `/dev/disk/by-path/` per i nomi dei tuoi dispositivi persistenti.

Per 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 archiviazione a blocchi per semplificare l'installazione iniziale StorageGRID e le future procedure di manutenzione. Se si utilizza il driver multipath del mapper del dispositivo per l'accesso ridondante ai volumi di archiviazione condivisi, è possibile utilizzare `alias` campo nel tuo `/etc/multipath.conf` file.

Per esempio:

```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-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
    }
    ...
}

```

Utilizzando il campo `alias` in questo modo, gli alias vengono visualizzati come dispositivi a blocchi in `/dev/mapper` directory sull'host, consentendo di specificare un nome descrittivo e facilmente convalidabile ogni volta che un'operazione di configurazione o manutenzione richiede di specificare un volume di archiviazione a blocchi.

Se si sta configurando un archivio condiviso per supportare la migrazione dei nodi StorageGRID e si utilizza Device Mapper Multipathing, è possibile creare e installare un archivio comune `/etc/multipath.conf` su tutti gli host co-localizzati. Assicurati solo di utilizzare un volume di archiviazione 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 archiviazione Docker renderanno tutto più facile da ricordare e sono consigliati.



Il supporto per Docker come motore di container per distribuzioni esclusivamente software è deprecato. Docker verrà sostituito con un altro motore di container in una versione futura.

Informazioni correlate

- ["Requisiti di archiviazione e prestazioni"](#)
- ["Requisiti per la migrazione dei contenitori dei nodi"](#)

Configurare il volume di archiviazione del motore del contenitore

Prima di installare il motore del contenitore (Docker o Podman), potrebbe essere necessario formattare il volume di archiviazione e montarlo.



Il supporto per Docker come motore di container per distribuzioni esclusivamente software è deprecato. Docker verrà sostituito con un altro motore di container in una versione futura.

Informazioni su questo compito

È possibile saltare questi passaggi se si prevede di utilizzare l'archiviazione locale per il volume di archiviazione Docker e si dispone di spazio sufficiente disponibile sulla partizione host contenente `/var/lib`.

Passi

1. Creare un file system sul volume di archiviazione Docker:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Montare il volume di archiviazione 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 archiviazione venga rimontato automaticamente dopo il riavvio dell'host.

Installa Docker

Il sistema StorageGRID funziona su Linux come una raccolta di container Docker. Prima di poter installare StorageGRID, è necessario installare Docker.



Il supporto per Docker come motore di container per distribuzioni esclusivamente software è deprecato. Docker verrà sostituito con un altro motore di container in una versione futura.

Passi

1. Installa Docker seguendo le istruzioni per la tua distribuzione Linux.



Se Docker non è incluso nella tua distribuzione Linux, puoi scaricarlo dal sito web di Docker.

2. Assicurati che Docker sia stato abilitato e avviato eseguendo i due comandi seguenti:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Conferma di aver installato la versione prevista di Docker immettendo quanto segue:

```
sudo docker version
```

Le versioni Client e Server devono essere 1.11.0 o successive.

Informazioni correlate

["Configurare l'archiviazione host"](#)

Installa i servizi host StorageGRID

Per installare i servizi host StorageGRID , utilizzare il pacchetto StorageGRID DEB.

Informazioni su questo compito

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 proprio sistema operativo Linux.

Passi

1. Copia i pacchetti DEB di StorageGRID su ciascuno dei tuoi host oppure rendili disponibili su un archivio condiviso.

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

2. Accedi a ciascun host come root o utilizzando un account con autorizzazione sudo ed esegui i seguenti comandi.

È necessario installare il `images` pacchetto prima, e il `service` secondo pacchetto. Se hai inserito i pacchetti in una directory diversa da `/tmp` , modifica 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
```



Per poter installare i pacchetti StorageGRID , è necessario che Python 2,7 sia già installato. IL `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` il comando fallirà finché non lo avrai fatto.

Automatizzare l'installazione (Ubuntu o Debian)

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

Informazioni su questo compito

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

- Utilizzi già un framework di orchestrazione standard, come Ansible, Puppet o Chef, per distribuire e configurare host fisici o virtuali.
- Si intende distribuire più istanze StorageGRID .
- Stai distribuendo un'istanza StorageGRID complessa e di grandi dimensioni.

Il servizio host StorageGRID viene installato da un pacchetto e gestito da file di configurazione che possono essere creati interattivamente durante un'installazione manuale oppure preparati in anticipo (o a livello di programmazione) per consentire l'installazione automatizzata mediante framework di orchestrazione standard. StorageGRID fornisce script Python opzionali per automatizzare la configurazione degli appliance StorageGRID e dell'intero sistema StorageGRID (la "griglia"). È possibile utilizzare questi script direttamente oppure esaminarli per apprendere come utilizzare l'API REST di installazione di StorageGRID negli strumenti di configurazione e distribuzione della griglia sviluppati autonomamente.

Automatizza l'installazione e la configurazione del servizio host StorageGRID

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

Il servizio host 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 automatizzata. Se utilizzi già un framework di orchestrazione standard per installare e configurare Ubuntu o Debian, aggiungere StorageGRID ai tuoi playbook o alle tue 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 dell'archiviazione host per soddisfare i requisiti StorageGRID
5. Installazione di Docker
6. Installazione del servizio host StorageGRID
7. Creazione di 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 ruolo e playbook di Ansible

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

Automatizza la configurazione di StorageGRID

Dopo aver distribuito i nodi della griglia, è possibile automatizzare la configurazione del sistema StorageGRID .

Prima di iniziare

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

Nome del 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

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

Informazioni su questo compito

Puoi usare il `configure-storagegrid.py` Script Python e il `configure-storagegrid.json` file di configurazione per automatizzare la configurazione del sistema StorageGRID .



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

Passi

1. Accedi al computer Linux che stai utilizzando per eseguire lo script Python.
2. Passare alla directory in cui è stato estratto l'archivio di installazione.

Per esempio:

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

Dove platform È `debs` , `rpms` , O `vsphere` .

3. Esegui lo script Python e utilizza il file di configurazione che hai creato.

Per esempio:

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

Risultato

Un pacchetto di recupero `.zip` Il file viene generato durante il processo di configurazione e scaricato nella directory in cui si sta eseguendo 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, copialo in una posizione di rete protetta e sottoposta a backup e in un archivio cloud protetto.



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 hai specificato che devono essere generate password casuali, apri il `Passwords.txt` file e cerca le password necessarie per accedere al tuo 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 è installato e configurato quando viene visualizzato un messaggio di conferma.

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

Informazioni correlate

["Installazione REST API"](#)

Distribuisci nodi di griglia virtuali (Ubuntu o Debian)

Crea 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 di cui il servizio host StorageGRID ha bisogno per avviare un nodo e connetterlo alle risorse di rete e di archiviazione a blocchi appropriate. I file di configurazione dei nodi vengono utilizzati per i nodi virtuali e non per i nodi appliance.

Posizione per i file di configurazione del nodo

Posizionare il file di configurazione per ciascun nodo StorageGRID nel `/etc/storagegrid/nodes` directory sull'host in cui verrà eseguito il nodo. Ad esempio, se si prevede di eseguire un nodo di amministrazione, un nodo gateway e un nodo di archiviazione su HostA, è necessario posizionare tre file di configurazione del nodo in `/etc/storagegrid/nodes` su HostA.

È possibile creare i file di configurazione direttamente su ciascun host utilizzando un editor di testo, come vim o nano, oppure è possibile 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 che assegna al nodo. Questo nome appare nel programma di installazione StorageGRID e viene utilizzato per le operazioni di manutenzione dei nodi, come la migrazione dei nodi.

I nomi dei nodi devono seguire queste regole:

- Deve essere unico
- Deve iniziare con una lettera
- Può contenere i caratteri dalla A alla Z e dalla a alla z
- Può contenere i numeri da 0 a 9
- Può contenere uno o più trattini (-)
- Non deve contenere più di 32 caratteri, escluso il `.conf` estensione

Tutti i file in `/etc/storagegrid/nodes` che non seguono queste convenzioni di denominazione non verranno analizzati dal servizio host.

Se hai pianificato una topologia multi-sito per la tua griglia, uno schema di denominazione tipico dei nodi potrebbe essere:

```
site-nodetype-nodenum.conf
```

Ad esempio, potresti usare `dc1-adm1.conf` per il primo nodo amministrativo nel Data Center 1 e `dc2-sn3.conf` per il terzo nodo di archiviazione nel Data Center 2. Tuttavia, puoi usare qualsiasi schema tu preferisca, 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, seguire queste regole:

- La chiave e il valore devono essere separati da un segno di uguale(=) e spazi vuoti facoltativi.
- Le chiavi non possono contenere spazi.
- I valori possono contenere spazi incorporati.
- Eventuali spazi iniziali o finali vengono ignorati.

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

- **Obbligatorio:** obbligatorio per ogni nodo o per i tipi di nodo specificati
- **Migliore pratica:** Facoltativo, sebbene consigliato
- **Facoltativo:** facoltativo per tutti i nodi

Chiavi di rete amministrative

ADMIN_IP

Valore	Designazione
Indirizzo IPv4 della rete Grid del nodo di amministrazione primario per la griglia a cui appartiene questo nodo. Utilizzare lo stesso valore specificato per GRID_NETWORK_IP per il nodo della griglia con NODE_TYPE = VM_Admin_Node e ADMIN_ROLE = Primary. Se si omette questo parametro, il nodo tenta di individuare un nodo amministrativo primario tramite mDNS. "Come i nodi della griglia scoprono il nodo di amministrazione primario" Nota: questo valore viene ignorato e potrebbe essere vietato sul nodo di amministrazione primario.	Le migliori pratiche

ADMIN_NETWORK_CONFIG

Valore	Designazione
DHCP, STATICO o DISABILITATO	Opzionale

ADMIN_NETWORK_ESL

Valore	Designazione
Elenco separato da virgole delle subnet in notazione CIDR con cui questo nodo deve comunicare tramite il gateway di rete di amministrazione. Esempio: 172.16.0.0/21, 172.17.0.0/21	Opzionale

GATEWAY DI RETE AMMINISTRATIVA

Valore	Designazione
Indirizzo IPv4 del gateway di rete di amministrazione 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 tramite DHCP. Esempi: 1.1.1.1 10.224.4.81	Obbligatorio se ADMIN_NETWORK_ESL è specificato. Altrimenti facoltativo.

IP_RETE_AMMINISTRATIVO

Valore	Designazione
Indirizzo IPv4 di questo nodo sulla rete di amministrazione. Questa chiave è richiesta solo quando ADMIN_NETWORK_CONFIG = STATIC; non specificarla per altri valori. Esempi: 1.1.1.1 10.224.4.81	Obbligatorio quando ADMIN_NETWORK_CONFIG = STATIC. Altrimenti facoltativo.

AMMINISTRAZIONE_RETE_MAC

Valore	Designazione
L'indirizzo MAC per l'interfaccia di rete di amministrazione nel contenitore. Questo campo è facoltativo. Se omissso, verrà generato automaticamente un indirizzo MAC. Deve essere composto da 6 coppie di cifre esadecimali separate da due punti. Esempio: b2:9c:02:c2:27:10	Opzionale

MASCHERA_DI_RETE_ADMIN

Valore	Designazione
Maschera di rete 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	Obbligatorio se è specificato ADMIN_NETWORK_IP e ADMIN_NETWORK_CONFIG = STATIC. Altrimenti facoltativo.

ADMIN_NETWORK_MTU

Valore	Designazione
L'unità di trasmissione massima (MTU) per questo nodo 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 1500. Se si desidera utilizzare i jumbo frame, impostare l'MTU su un valore adatto ai jumbo frame, ad esempio 9000. Altrimenti, mantieni 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 prestazioni di rete o perdita di pacchetti. Esempi: 1500 8192	Opzionale

AMMINISTRAZIONE_RETE_TARGET

Valore	Designazione
Nome del dispositivo host che verrà utilizzato per l'accesso alla rete di amministrazione da parte del 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) sul dispositivo di bonding oppure utilizzare un bridge e una coppia Ethernet virtuale (veth). Migliore pratica: specificare un valore anche se inizialmente questo nodo non avrà un indirizzo IP di rete amministrativa. Successivamente potrai aggiungere un indirizzo IP di rete amministrativa, senza dover riconfigurare il nodo sull'host. Esempi: bond0.1002 ens256	Le migliori pratiche

TIPO_TARGET_RETE_AMMINISTRAZIONE

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 far sì che il contenitore StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete di amministrazione. Migliore pratica: nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per maggiori dettagli sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione dell'indirizzo MAC (Ubuntu o Debian)"	Le migliori pratiche

RUOLO_AMMINISTRATORE

Valore	Designazione
Primario o non primario Questa chiave è richiesta solo quando NODE_TYPE = VM_Admin_Node; non specificarla per altri tipi di nodo.	Obbligatorio quando NODE_TYPE = VM_Admin_Node Altrimenti facoltativo.

Blocca le chiavi del dispositivo

BLOCK_DEVICE_AUDIT_LOGS

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi che questo nodo utilizzerà per l'archiviazione persistente dei registri di controllo. Esempi: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-audit-logs</pre>	Obbligatorio per i nodi con NODE_TYPE = VM_Admin_Node. Non specificarlo per altri tipi di nodo.

BLOCK_DEVICE_RANGEDB_nnn

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi che questo nodo utilizzerà per l'archiviazione persistente degli oggetti. Questa chiave è richiesta solo per i nodi con NODE_TYPE = VM_Storage_Node; non specificarla per altri tipi di nodo. È obbligatorio 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 spazi vuoti. Se si specifica BLOCK_DEVICE_RANGEDB_005, è necessario specificare anche BLOCK_DEVICE_RANGEDB_004. Nota: per garantire la compatibilità con le distribuzioni esistenti, per i nodi aggiornati sono supportate chiavi a due cifre. Esempi: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-rangedb-000</pre>	Necessario: 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

TABELLE_DISPOSITIVI_BLOCCHI

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi che questo nodo utilizzerà per l'archiviazione persistente delle tabelle del database. Questa chiave è richiesta 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-adml-tables	Necessario

BLOCK_DEVICE_VAR_LOCAL

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi che questo nodo utilizzerà per il suo /var/local archiviazione 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	Necessario

Chiavi di rete del cliente

CLIENT_NETWORK_CONFIG

Valore	Designazione
DHCP, STATICO o DISABILITATO	Opzionale

GATEWAY_RETE_CLIENT

Valore	Designazione

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

IP_RETE_CLIENTE

Valore	Designazione
Indirizzo IPv4 di questo nodo sulla rete client. Questa chiave è richiesta solo quando CLIENT_NETWORK_CONFIG = STATIC; non specificarla per altri valori. Esempi: 1.1.1.1 10.224.4.81	Obbligatorio quando CLIENT_NETWORK_CONFIG = STATIC Altrimenti facoltativo.

CLIENT_NETWORK_MAC

Valore	Designazione
L'indirizzo MAC per l'interfaccia di rete client nel contenitore. Questo campo è facoltativo. Se omissso, verrà generato automaticamente un indirizzo MAC. Deve essere composto da 6 coppie di cifre esadecimali separate da due punti. Esempio: b2:9c:02:c2:27:20	Opzionale

CLIENT_NETWORK_MASK

Valore	Designazione
Maschera di rete 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	Obbligatorio se è specificato CLIENT_NETWORK_IP e CLIENT_NETWORK_CONFIG = STATIC Altrimenti facoltativo.

CLIENT_NETWORK_MTU

Valore	Designazione
L'unità di trasmissione massima (MTU) 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 jumbo frame, impostare l'MTU su un valore adatto ai jumbo frame, ad esempio 9000. Altrimenti, mantieni 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 prestazioni di rete o perdita di pacchetti. Esempi: 1500 8192	Opzionale

CLIENT_NETWORK_TARGET

Valore	Designazione
Nome del dispositivo host che verrà utilizzato per l'accesso alla rete client da parte del 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) sul dispositivo di bonding oppure utilizzare un bridge e una coppia Ethernet virtuale (veth). Procedura consigliata: specificare un valore anche se inizialmente questo nodo non avrà un indirizzo IP di rete client. Successivamente è possibile aggiungere un indirizzo IP di rete client, senza dover riconfigurare il nodo sull'host. Esempi: bond0.1003 ens423	Le migliori pratiche

TIPO_DESTINAZIONE_RETE_CLIENT

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

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o falso Impostare la chiave su "true" per far sì che il contenitore StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete client. Migliore pratica: nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per maggiori dettagli sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione dell'indirizzo MAC (Ubuntu o Debian)"	Le migliori pratiche

Chiavi di rete della griglia

GRID_NETWORK_CONFIG

Valore	Designazione
STATICO o DHCP Se non specificato, il valore predefinito è STATIC.	Le migliori pratiche

GRID_NETWORK_GATEWAY

Valore	Designazione
Indirizzo IPv4 del gateway di rete Grid locale per questo nodo, che deve trovarsi nella subnet definita da GRID_NETWORK_IP e GRID_NETWORK_MASK. Questo valore viene ignorato per le reti configurate tramite DHCP. Se la rete Grid è una singola subnet senza gateway, utilizzare l'indirizzo gateway standard per la subnet (XYZ1) o il valore GRID_NETWORK_IP di questo nodo; entrambi i valori semplificheranno le potenziali espansioni future della rete Grid.	Necessario

IP_RETE_GRIGLIA

Valore	Designazione
Indirizzo IPv4 di questo nodo sulla rete Grid. Questa chiave è richiesta solo quando GRID_NETWORK_CONFIG = STATIC; non specificarla per altri valori. Esempi: 1.1.1.1 10.224.4.81	Obbligatorio quando GRID_NETWORK_CONFIG = STATIC Altrimenti facoltativo.

GRID_NETWORK_MAC

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

GRID_NETWORK_MASK

Valore	Designazione
Maschera di rete IPv4 per questo nodo sulla rete Grid. Specificare questa chiave quando GRID_NETWORK_CONFIG = STATIC; non specificarla per altri valori. Esempi: 255.255.255.0 255.255.248.0	Obbligatorio quando è specificato GRID_NETWORK_IP e GRID_NETWORK_CONFIG = STATIC. Altrimenti facoltativo.

GRID_NETWORK_MTU

Valore	Designazione
L'unità di trasmissione massima (MTU) per questo nodo sulla rete Grid. Non specificare se GRID_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omissso, viene utilizzato 1500. Se si desidera utilizzare i jumbo frame, impostare l'MTU su un valore adatto ai jumbo frame, ad esempio 9000. Altrimenti, mantieni 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 prestazioni di rete o perdita di pacchetti. IMPORTANTE: Per ottenere le migliori prestazioni di rete, tutti i nodi devono essere configurati con valori MTU simili sulle loro interfacce di rete Grid. L'avviso Mancata corrispondenza MTU della rete Grid viene attivato se si verifica una differenza significativa nelle impostazioni MTU per la rete Grid sui singoli nodi. I valori MTU non devono essere gli stessi 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 Grid da parte del 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) sul dispositivo di bonding oppure utilizzare un bridge e una coppia Ethernet virtuale (veth). Esempi: <pre>bond0.1001</pre> <pre>ens192</pre>	Necessario

TIPO_TARGET_RETE_GRIGLIA

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 far sì che il contenitore StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete Grid. Migliore pratica: nelle reti in cui sarebbe richiesta la modalità promiscua, utilizzare invece la chiave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Per maggiori dettagli sulla clonazione MAC: • "Considerazioni e raccomandazioni per la clonazione degli indirizzi MAC (Red Hat Enterprise Linux)" • "Considerazioni e raccomandazioni per la clonazione dell'indirizzo MAC (Ubuntu o Debian)"	Le migliori pratiche

Chiave password di installazione (temporanea)

HASH_PASSWORD_TEMPORANEO_PERSONALIZZATO

Valore	Designazione
Per il nodo di amministrazione primario, impostare una password temporanea predefinita per l'API di installazione StorageGRID durante l'installazione. Nota: impostare una password di installazione solo sul nodo di amministrazione primario. Se si tenta di impostare una password su un altro tipo di nodo, la convalida del file di configurazione del nodo fallirà. L'impostazione di questo valore non ha alcun effetto al termine dell'installazione. Se questa chiave viene omessa, per impostazione predefinita non viene impostata alcuna password temporanea. In alternativa, è possibile impostare una password temporanea utilizzando l'API di installazione StorageGRID . Deve essere un <code>crypt()</code> Hash della password SHA-512 con formato <code>\$6\$<salt>\$<password hash></code> per una password di almeno 8 e non più di 32 caratteri. Questo hash può essere generato utilizzando strumenti CLI, come <code>openssl passwd</code> comando in modalità SHA-512.	Le migliori pratiche

Chiave delle interfacce

INTERFACCIA_DESTINAZIONE_nnnn

Valore	Designazione
Nome e descrizione facoltativa per un'interfaccia aggiuntiva che si desidera aggiungere a questo nodo. È possibile aggiungere più interfacce extra a ciascun nodo. Per <i>nnnn</i>, specificare un numero univoco per ogni voce <code>INTERFACE_TARGET</code> 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 Interfacce VLAN e nella pagina Gruppi HA. Esempio: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Se si aggiunge un'interfaccia trunk, 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

RAM MASSIMA

Valore	Designazione
La quantità massima di RAM che questo nodo può consumare. Se questa chiave viene omessa, il nodo non ha restrizioni di memoria. Quando si imposta questo campo per un nodo di livello di produzione, specificare un valore pari ad almeno 24 GB e da 16 a 32 GB in meno rispetto alla RAM totale del sistema. Nota: il valore della RAM influisce sullo spazio effettivo riservato ai metadati di un nodo. Vedi il "descrizione di cosa è lo spazio riservato ai metadati". Il formato per questo campo è <i>numberunit</i>, Dove <i>unit</i> 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 cgroup di memoria.	Opzionale

Chiavi di tipo nodo

TIPO_NODO

Valore	Designazione
Tipo di nodo: • Nodo amministratore VM • Nodo di archiviazione VM • VM_Archive_Node • Gateway VM_API	Necessario

TIPO_DI_ARCHIVIAZIONE

Valore	Designazione
Definisce il tipo di oggetti contenuti in un nodo di archiviazione. Per ulteriori informazioni, consultare "Tipi di nodi di archiviazione". Questa chiave è richiesta solo per i nodi con NODE_TYPE = VM_Storage_Node; non specificarla per altri tipi di nodo. Tipi di archiviazione: • combinato • dati • metadati Nota: se STORAGE_TYPE non è specificato, per impostazione predefinita il tipo di nodo di archiviazione è impostato su combinato (dati e metadati).	Opzionale

Tasti di rimappatura delle porte

PORT_REMAP

Valore	Designazione
Riassegna qualsiasi porta utilizzata da un nodo per le comunicazioni interne del nodo della griglia o per le comunicazioni esterne. La rimappatura delle porte è necessaria se i criteri di rete aziendale limitano una o più porte utilizzate da StorageGRID, come descritto in "Comunicazioni interne al nodo della griglia" O "Comunicazioni esterne". IMPORTANTE: non rimappare le porte che intendi utilizzare per configurare gli endpoint del bilanciatore del carico. Nota: se è impostato solo PORT_REMAP, la mappatura specificata viene utilizzata sia per le comunicazioni in entrata che per quelle in uscita. Se viene specificato anche PORT_REMAP_INBOUND, PORT_REMAP si applica solo alle comunicazioni in uscita. Il formato utilizzato è: <i>network type/protocol/default port used by grid node/new port</i>, Dove <i>network type</i> è griglia, amministratore o client e <i>protocol</i> è tcp o udp. Esempio: PORT_REMAP = client/tcp/18082/443 È anche possibile rimappare più porte utilizzando un elenco separato da virgole. Esempio: PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80	Opzionale

PORT_REMAP_INBOUND

Valore	Designazione
Riassegna 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 intendi utilizzare per configurare gli endpoint del bilanciatore del carico. Il formato utilizzato è: <i>network type/protocol/remapped port /default port used by grid node</i>, Dove <i>network type</i> è griglia, amministratore o client e <i>protocol</i> è tcp o udp. Esempio: PORT_REMAP_INBOUND = grid/tcp/3022/22 È anche possibile rimappare più porte in ingresso utilizzando un elenco separato da virgole. Esempio: PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22	Opzionale

Come i nodi della griglia scoprono il nodo di amministrazione primario

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

Per garantire che un nodo della griglia possa accedere al nodo di amministrazione primario, è possibile effettuare una delle seguenti operazioni durante la distribuzione del nodo:

- È possibile utilizzare il parametro ADMIN_IP per immettere manualmente l'indirizzo IP del nodo di amministrazione primario.
- È possibile omettere il parametro ADMIN_IP per fare in modo che il nodo della griglia rilevi automaticamente il valore. La rilevazione automatica è particolarmente utile quando la rete Grid utilizza DHCP per assegnare l'indirizzo IP al nodo di amministrazione primario.

Il rilevamento automatico del nodo di amministrazione primario viene eseguito tramite un sistema di nomi di dominio multicast (mDNS). Quando il nodo di amministrazione primario viene avviato per la prima volta, pubblica il suo indirizzo IP tramite mDNS. Altri nodi sulla stessa subnet possono quindi richiedere l'indirizzo IP e acquisirlo automaticamente. Tuttavia, poiché il traffico IP multicast non è normalmente instradabile tra subnet, i nodi su altre subnet non possono acquisire direttamente l'indirizzo IP del nodo amministrativo primario.

Se si utilizza la rilevazione automatica:



- È necessario includere l'impostazione `ADMIN_IP` per almeno un nodo della griglia su tutte le subnet a cui il nodo di amministrazione primario non è direttamente collegato. Questo nodo della griglia pubblicherà quindi l'indirizzo IP del nodo di amministrazione primario affinché altri nodi sulla subnet possano individuarlo con mDNS.
- Assicurati che la tua infrastruttura di rete supporti il passaggio del traffico IP multicast all'interno di una subnet.

File di configurazione dei nodi di esempio

È possibile utilizzare i file di configurazione dei nodi di esempio per impostare 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 della griglia.

Per la maggior parte dei nodi, è possibile aggiungere informazioni sull'indirizzamento di rete dell'amministratore e del client (IP, maschera, gateway e così via) quando si configura la griglia tramite Grid Manager o l'API di installazione. L'eccezione è il nodo di amministrazione primario. Se si desidera accedere all'IP della rete amministrativa del nodo amministrativo primario per completare la configurazione della griglia (ad esempio perché la rete della griglia non è instradata), è necessario configurare la connessione alla rete amministrativa per il nodo amministrativo primario nel relativo file di configurazione del nodo. Ciò è mostrato nell'esempio.



Negli esempi, la destinazione Client Network è stata configurata come best practice, anche se Client Network è disabilitata per impostazione predefinita.

Esempio per il nodo di amministrazione primario

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

Esempio di contenuto del file:

```

NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adml-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adml-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adml-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 archiviazione

Nome file di esempio: /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 il nodo gateway

Nome file di esempio: /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/dcl-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 per un nodo di amministrazione non primario

Nome file di esempio: /etc/storagegrid/nodes/dcl-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/dcl-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dcl-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dcl-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
```

Convalida 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 ogni file di configurazione, come mostrato nell'esempio.



Quando si utilizza una sola LUN su 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 dcl-adm1... PASSED
Checking configuration file for node dcl-gw1... PASSED
Checking configuration file for node dcl-sn1... PASSED
Checking configuration file for node dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes... PASSED
```



Per un'installazione automatizzata, è possibile sopprimere questo output utilizzando `-q` o `--quiet` opzioni nel `storagegrid` comando (ad esempio, `storagegrid --quiet...`). Se si sopprime 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** ed **ERROR**, come mostrato nell'esempio. Se vengono rilevati errori di configurazione, è necessario correggerli prima di continuare con l'installazione.

```

Checking for misnamed node configuration files...
WARNING: ignoring /etc/storagegrid/nodes/dcl-adml
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
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 dcl-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 dcl-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 dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
ERROR: GRID_NETWORK_IP = 10.1.0.4
      dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Avviare il servizio host StorageGRID

Per avviare i nodi StorageGRID e assicurarsi che si riavviino dopo un riavvio dell'host, è necessario abilitare e avviare il servizio host StorageGRID .

Passi

1. Eseguire i seguenti comandi su ciascun host:

```

sudo systemctl enable storagegrid
sudo systemctl start storagegrid

```


2. Eseguire il seguente comando per assicurarsi che la distribuzione proceda:

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

3. Se un nodo restituisce lo stato "Non in esecuzione" o "Arrestato", eseguire il seguente comando:

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

4. Se in precedenza hai abilitato e avviato il servizio host StorageGRID (o se non sei sicuro che il servizio sia stato abilitato e avviato), esegui anche il seguente comando:

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

Configurare la griglia e completare l'installazione (Ubuntu o Debian)

Vai al Grid Manager

Utilizzare Grid Manager per definire tutte le informazioni necessarie per configurare il sistema StorageGRID .

Prima di iniziare

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

Passi

1. Apri il tuo browser web e vai su:

```
https://primary_admin_node_ip
```

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

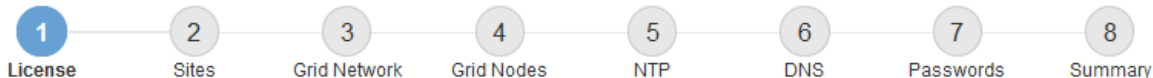
```
https://primary_admin_node_ip:8443
```

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

2. Gestisci una password di installazione temporanea secondo necessità:
 - Se è già stata impostata una password utilizzando uno di questi metodi, immetterla per procedere.
 - Un utente ha impostato la password durante l'accesso al programma di installazione in precedenza
 - La password è stata importata automaticamente dal file di configurazione del nodo in `/etc/storagegrid/nodes/<node_name>.conf`
 - Se non è stata impostata una password, impostarne una facoltativamente per proteggere il programma di installazione StorageGRID .
3. Selezionare ***Installa un sistema StorageGRID ***.

Viene visualizzata la pagina utilizzata per configurare un sistema StorageGRID .

Install



License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Browse

Specificare le informazioni sulla licenza StorageGRID

È necessario specificare il nome del sistema StorageGRID e caricare il file di licenza fornito da NetApp.

Passi

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 Nodi.

2. Selezionare **Sfogli**, individuare il file di licenza NetApp(*NLF-unique-id.txt*) e seleziona **Apri**.

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



L'archivio di installazione StorageGRID include una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto. Dopo l'installazione è possibile effettuare l'aggiornamento a una licenza che offra supporto.

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File NLF-959007-Internal.txt

License Serial Number

3. Selezionare **Avanti**.

Aggiungi siti

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

Passi

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

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

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top is a blue header with 'NetApp® StorageGRID®' and a 'Help' dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites (highlighted in blue), 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Below the progress bar, the 'Sites' section is active. It contains two paragraphs of text explaining single-site and multi-site deployments. Below the text are two input fields for site names. The first field is labeled 'Site Name 1' and contains the text 'Raleigh', with a red 'x' icon to its right. The second field is labeled 'Site Name 2' and contains the text 'Atlanta', with a red '+ x' icon to its right.

3. Fare clic su **Avanti**.

Specificare le subnet della rete Grid

È necessario specificare le subnet utilizzate nella rete Grid.

Informazioni su questo compito

Le voci di subnet includono le subnet per la rete Grid per ciascun sito nel sistema StorageGRID, insieme a tutte le subnet che devono essere raggiungibili tramite la rete Grid.

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

Passi

1. Specificare l'indirizzo di rete CIDR per almeno una rete Grid nella casella di testo **Subnet 1**.
2. Fare clic sul segno più accanto all'ultima voce per aggiungere un'ulteriore voce di rete. È necessario specificare tutte le subnet per tutti i siti nella rete Grid.
 - Se hai già distribuito almeno un nodo, fai clic su **Scopri subnet di Grid Networks** per popolare automaticamente l'elenco delle subnet di Grid Network con le subnet segnalate dai nodi di Grid che si

sono registrati con Grid Manager.

- È necessario aggiungere manualmente eventuali subnet per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway Grid Network.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.
Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1

172.16.0.0/21

+

Discover Grid Network subnets

3. Fare clic su **Avanti**.

Approva i nodi della griglia in sospenso

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

Prima di iniziare

Sono stati distribuiti tutti i nodi griglia virtuali e degli appliance StorageGRID .



È più efficiente eseguire un'unica installazione di tutti i nodi, piuttosto che installare alcuni nodi ora e altri in seguito.

Passi

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



Se un nodo della griglia risulta mancante, verificare che sia stato distribuito correttamente e che abbia impostato l'IP di rete della griglia corretto del nodo di amministrazione primario per ADMIN_IP.

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



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve		✖ Remove		Search		Q
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit

Reset

Remove

Search

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21

3. Fare clic su **Approva**.

4. Nelle Impostazioni generali, modificare le impostazioni per le seguenti proprietà, se necessario:

- **Sito:** il nome di sistema del sito per questo nodo della griglia.
- **Nome:** il nome di sistema per il nodo. Il nome predefinito è quello specificato durante la configurazione del nodo.

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

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



Assicurarsi che almeno due nodi in ogni sito possano accedere ad almeno quattro fonti NTP esterne. Se solo un nodo in un sito riesce a raggiungere le sorgenti NTP, si verificheranno problemi di temporizzazione se quel nodo non funziona. Inoltre, la designazione di due nodi per sito come fonti NTP primarie garantisce una temporizzazione accurata se un sito è isolato dal resto della griglia.

- **Tipo di archiviazione** (solo nodi di archiviazione): specifica che un nuovo nodo di archiviazione deve essere utilizzato esclusivamente per i dati, solo per i metadati o per entrambi. Le opzioni sono **Dati e metadati** ("combinati"), **Solo dati** e **Solo metadati**.



Vedere "[Tipi di nodi di archiviazione](#)" per informazioni sui requisiti per questi tipi di nodo.

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

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

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

Il gateway è necessario se sono presenti più subnet della griglia.



Se hai selezionato DHCP per la configurazione della rete Grid e modifichi il valore qui, il nuovo valore verrà configurato come indirizzo statico sul nodo. È necessario assicurarsi che l'indirizzo IP configurato non sia compreso in un pool di indirizzi DHCP.

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

Immettere le subnet di destinazione delle rotte in uscita da questa interfaccia nella casella di testo **Subnet (CIDR)**. Se sono presenti più subnet di amministrazione, è necessario il gateway di amministrazione.



Se hai selezionato DHCP per la configurazione della rete di amministrazione e modifichi il valore qui, il nuovo valore verrà configurato come indirizzo statico sul nodo. È necessario assicurarsi che l'indirizzo IP configurato non sia compreso in un pool di indirizzi DHCP.

Appliance: per un'appliance StorageGRID, se la rete di amministrazione non è stata configurata durante l'installazione iniziale tramite StorageGRID Appliance Installer, non può essere configurata in questa finestra di dialogo Grid Manager. Invece, devi seguire questi passaggi:

1. Riavviare l'appliance: nell'Appliance Installer, selezionare **Avanzate > Riavvia**.

Il riavvio può richiedere diversi minuti.

2. Selezionare **Configura rete > Configurazione collegamento** e abilitare le reti appropriate.
3. Selezionare **Configura rete > Configurazione IP** e configurare le reti abilitate.
4. Torna alla Home page e clicca su **Avvia installazione**.

- e. In Grid Manager: se il nodo è elencato nella tabella Nodi approvati, rimuoverlo.
- f. Rimuovere il nodo dalla tabella Nodi in sospeso.
- g. Attendi che il nodo riappaia nell'elenco dei nodi in sospeso.
- h. Verificare di poter configurare le reti appropriate. Dovrebbero già essere compilati con le informazioni fornite nella pagina Configurazione IP dell'Appliance Installer.

Per ulteriori informazioni, vedere il ["Avvio rapido per l'installazione dell'hardware"](#) per trovare le istruzioni per il tuo elettrodomestico.

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



Se hai selezionato DHCP per la configurazione della rete client e modifichi il valore qui, il nuovo valore verrà configurato come indirizzo statico sul nodo. È necessario assicurarsi che l'indirizzo IP configurato non sia compreso in un pool di indirizzi DHCP.

Appliance: per un'appliance StorageGRID , se la rete client non è stata configurata durante l'installazione iniziale tramite StorageGRID Appliance Installer, non può essere configurata in questa finestra di dialogo Grid Manager. Invece, devi seguire questi passaggi:

- a. Riavviare l'appliance: nell'Appliance Installer, selezionare **Avanzate > Riavvia**.

Il riavvio può richiedere diversi minuti.

- b. Selezionare **Configura rete > Configurazione collegamento** e abilitare le reti appropriate.
- c. Selezionare **Configura rete > Configurazione IP** e configurare le reti abilitate.
- d. Torna alla Home page e clicca su **Avvia installazione**.
- e. In Grid Manager: se il nodo è elencato nella tabella Nodi approvati, rimuoverlo.
- f. Rimuovere il nodo dalla tabella Nodi in sospeso.
- g. Attendi che il nodo riappaia nell'elenco dei nodi in sospeso.
- h. Verificare di poter configurare le reti appropriate. Dovrebbero già essere compilati con le informazioni fornite nella pagina Configurazione IP dell'Appliance Installer.

Per informazioni su come installare gli apparecchi StorageGRID , vedere ["Avvio rapido per l'installazione dell'hardware"](#) per trovare le istruzioni per il tuo elettrodomestico.

8. Fare clic su **Salva**.

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



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

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

Devi approvare tutti i nodi che desideri nella griglia. Tuttavia, puoi 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 della griglia, fare clic su **Avanti**.

Specificare le informazioni del server Network Time Protocol

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

Informazioni su questo compito

È necessario specificare gli indirizzi IPv4 per i server NTP.

È necessario specificare server NTP esterni. I server NTP specificati devono utilizzare il protocollo NTP.

Per evitare problemi di deriva temporale, è necessario specificare quattro riferimenti al server NTP di Stratum 3 o superiore.



Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Ora di Windows (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio orario delle versioni precedenti di Windows non è sufficientemente preciso e non è supportato da Microsoft per l'uso in ambienti ad alta precisione, come StorageGRID.

["Limite di supporto per configurare il servizio Ora di Windows per ambienti ad alta precisione"](#)

I server NTP esterni vengono utilizzati dai nodi a cui sono stati precedentemente assegnati ruoli NTP primari.



Assicurarsi che almeno due nodi in ogni sito possano accedere ad almeno quattro fonti NTP esterne. Se solo un nodo in un sito riesce a raggiungere le sorgenti NTP, si verificheranno problemi di temporizzazione se quel nodo non funziona. Inoltre, la designazione di due nodi per sito come fonti NTP primarie garantisce una temporizzazione accurata se un sito è isolato dal resto della griglia.

Passi

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 ulteriori voci del server.

The screenshot shows the NetApp StorageGRID installation wizard. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a navigation bar with "Install" and a progress indicator. The progress indicator shows eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP (highlighted in blue), 6. DNS, 7. Passwords, and 8. Summary. Below the progress bar, the "Network Time Protocol" section is visible. It contains the instruction: "Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync." There are four input fields labeled "Server 1" through "Server 4". The values entered are: Server 1: 10.60.248.183, Server 2: 10.227.204.142, Server 3: 10.235.48.111, and Server 4: 0.0.0.0. To the right of the "Server 4" field is a plus sign (+) to add more servers.

Server	IP Address
Server 1	10.60.248.183
Server 2	10.227.204.142
Server 3	10.235.48.111
Server 4	0.0.0.0

3. Selezionare **Avanti**.

Informazioni correlate

["Linee guida per il networking"](#)

Specificare le informazioni del server DNS

È necessario specificare le informazioni DNS per il sistema StorageGRID , in modo da

poter accedere ai server esterni utilizzando nomi host anziché indirizzi IP.

Informazioni su questo compito

Specificando ["Informazioni sul server DNS"](#) consente di utilizzare nomi host FQDN (Fully Qualified Domain Name) anziché indirizzi IP per le notifiche e-mail e AutoSupport.

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

Se possibile, utilizzare server DNS a cui ogni sito possa accedere localmente per garantire che un sito isolato possa risolvere gli FQDN per le destinazioni esterne.

Passi

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 ulteriori voci del server.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (currently active), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is displayed. It contains a text box for "Server 1" with the value "10.224.223.130" and a red "X" icon. Below that is a text box for "Server 2" with the value "10.224.223.136" and a red "X" icon. A plus sign icon is visible next to the "Server 2" text box, indicating that more servers can be added.

La procedura migliore è specificare almeno due server DNS. È possibile specificare fino a sei server DNS.

3. Selezionare **Avanti**.

Specificare le password del sistema StorageGRID

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

Informazioni su questo compito

Utilizzare la pagina Installa password per specificare la passphrase di provisioning e la password dell'utente root per la 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 conservare la passphrase di provisioning in un luogo sicuro.

- È possibile modificare la passphrase di provisioning da Grid Manager se si dispone di quella attuale.
- La password dell'utente root per la gestione della griglia può essere modificata tramite Grid Manager.
- Le password della console della riga di comando e SSH generate casualmente vengono memorizzate nel `Passwords.txt` file nel pacchetto di ripristino.

Passi

1. In **Provisioning Passphrase**, immettere la passphrase di provisioning che sarà necessaria per apportare modifiche alla topologia della griglia del sistema StorageGRID .

Conservare la passphrase di provisioning in un luogo sicuro.



Se dopo il completamento dell'installazione si desidera modificare la passphrase di provisioning in un secondo momento, è possibile utilizzare Grid Manager. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.

2. In **Conferma passphrase di provisioning**, reinserisci la passphrase di provisioning per confermarla.
3. In **Password utente root di Grid Management**, immettere la password da utilizzare per accedere a Grid Manager come utente "root".

Conservare la password in un luogo sicuro.

4. In **Conferma password utente root**, reinserisci la password di Grid Manager per confermarla.

The screenshot shows the 'NetApp® StorageGRID®' installation wizard. At the top, a blue header bar contains the product name and a 'Help' link. Below the header, a progress bar shows eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords (highlighted in blue), and 8. Summary. The main content area is titled 'Passwords' and includes the instruction: 'Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.' There are four password input fields, each with a label and a masked input box (dots): 'Provisioning Passphrase', 'Confirm Provisioning Passphrase', 'Grid Management Root User Password', and 'Confirm Root User Password'. At the bottom, there is a checkbox labeled 'Create random command line passwords' which is checked.

5. Se si installa una griglia a scopo dimostrativo o di prova del concetto, è possibile deselezionare la casella di controllo **Crea password casuali per la riga di comando**.

Per le distribuzioni di produzione, per motivi di sicurezza è sempre opportuno utilizzare password casuali. Deseleziona **Crea password casuali per la riga di comando** solo per le griglie demo se vuoi utilizzare

password predefinite per accedere ai nodi della griglia dalla riga di comando utilizzando l'account "root" o "admin".



Ti verrà chiesto di scaricare il file del pacchetto di ripristino(`sgws-recovery-package-id-revision.zip`) dopo aver cliccato su **Installa** nella pagina Riepilogo. Devi [scaricare questo file](#) per completare l'installazione. Le password necessarie per accedere al sistema sono memorizzate nel `Passwords.txt` file, contenuto nel file Recovery Package.

6. Fare clic su **Avanti**.

Rivedi la tua configurazione e completa l'installazione

È necessario rivedere attentamente le informazioni di configurazione immesse per garantire che l'installazione venga completata correttamente.

Passi

1. Visualizza la pagina **Riepilogo**.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name

Grid1

Modify License

Passwords

Auto-generated random command line passwords

Modify Passwords

Networking

NTP

10.60.248.183 10.227.204.142 10.235.48.111

Modify NTP

DNS

10.224.223.130 10.224.223.136

Modify DNS

Grid Network

172.16.0.0/21

Modify Grid Network

Topology

Topology

Atlanta

Modify Sites

Modify Grid Nodes

Raleigh

dc1-adm1 dc1-g1 dc1-s1 dc1-s2 dc1-s3 NetApp-SGA

2. Verificare che tutte le informazioni sulla configurazione della griglia siano corrette. Utilizzare i link Modifica nella pagina 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 Grid alla rete client quando si fa clic su **Installa**. Se si perde la connettività, è necessario assicurarsi di accedere al nodo di amministrazione primario tramite una subnet accessibile. Vedere "[Linee guida per il networking](#)" per i dettagli.

4. Fare clic su **Scarica pacchetto di ripristino**.

Quando l'installazione procede fino al punto in cui viene definita la topologia della griglia, viene richiesto di scaricare il file del pacchetto di ripristino(. zip) e conferma di poter accedere correttamente al contenuto di questo file. È necessario scaricare il file Recovery Package per poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi della griglia. L'installazione continua in background, ma non sarà possibile completarla e accedere al sistema StorageGRID finché non si scarica e si verifica questo file.

5. Verificare che sia possibile estrarre il contenuto del . zip file e salvarlo in due posizioni sicure, protette 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. Seleziona la casella di controllo **Ho scaricato e verificato correttamente il file del pacchetto di ripristino** e fai 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.

Installation Status

If necessary, you may [Download the Recovery Package](#) file again.

Name	IT	Site	IT	Grid Network IPv4 Address	▼	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21				Starting services	
dc1-g1		Site1		172.16.4.216/21				Complete	
dc1-s1		Site1		172.16.4.217/21				Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21				Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21				Downloading hotfix from primary Admin if needed	

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

7. Sign in a Grid Manager utilizzando l'utente "root" e la password specificati durante l'installazione.

Linee guida post-installazione

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

- Se è stato utilizzato DHCP per assegnare gli indirizzi IP, configurare una prenotazione DHCP per ciascun indirizzo IP sulle reti utilizzate.

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



I nodi si riavviano quando la configurazione della rete Grid viene modificata da DHCP, il che può causare interruzioni se una modifica DHCP interessa più nodi contemporaneamente.

- È necessario utilizzare le procedure di modifica IP se si desidera modificare gli indirizzi IP, le maschere di sottorete e i gateway predefiniti per un nodo della griglia. Vedere "[Configurare gli indirizzi IP](#)".
- Se si apportano modifiche alla configurazione di rete, tra cui 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 apportate alla rete, potrebbe essere necessario ristabilire queste connessioni.

Installazione REST API

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

L'API utilizza la piattaforma API open source Swagger per fornire la documentazione API. Swagger consente sia agli sviluppatori sia ai non sviluppatori di interagire con l'API tramite un'interfaccia utente che illustra come l'API risponde a parametri e opzioni. Questa documentazione presuppone che tu abbia familiarità con le tecnologie web standard e con il formato dati JSON.



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

Ogni comando API REST include l'URL dell'API, un'azione HTTP, eventuali parametri URL obbligatori o facoltativi e una risposta API prevista.

API di installazione StorageGRID

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

Per accedere alla documentazione API, vai alla pagina web di installazione sul nodo di amministrazione principale e seleziona **Aiuto > Documentazione API** dalla barra dei menu.

L'API di installazione StorageGRID include le seguenti sezioni:

- **config** — Operazioni relative alla versione del prodotto e alle versioni dell'API. È possibile elencare la versione del prodotto e le principali versioni dell'API supportate da tale versione.
- **grid** — Operazioni di configurazione a livello di griglia. È possibile ottenere e aggiornare le impostazioni della griglia, inclusi i dettagli della griglia, le subnet della rete Grid, 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 della griglia, eliminare un nodo della griglia, configurare un nodo della griglia, visualizzare un nodo della griglia e reimpostare la configurazione di un nodo della griglia.
- **provision** — Operazioni di provisioning. È possibile avviare l'operazione di provisioning e visualizzarne lo stato.
- **recupero** — Operazioni di recupero del nodo amministrativo primario. È possibile reimpostare 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.
- **siti** — Operazioni di configurazione a livello di sito. È possibile creare, visualizzare, eliminare e modificare un sito.
- **temporary-password** — Operazioni sulla password temporanea per proteggere mgmt-api durante l'installazione.

Informazioni correlate

["Automatizzare l'installazione"](#)

Dove andare dopo

Dopo aver completato l'installazione, eseguire le attività di integrazione e configurazione richieste. È possibile eseguire le attività facoltative in base alle proprie esigenze.

Compiti richiesti

- ["Crea un account inquilino"](#) per il protocollo client S3 che verrà utilizzato per archiviare gli oggetti sul sistema StorageGRID .
- ["Controllo dell'accesso al sistema"](#) configurando gruppi e account utente. Facoltativamente, puoi ["configurare una fonte di identità federata"](#) (ad esempio Active Directory o OpenLDAP), in modo da poter importare gruppi di amministrazione e utenti. Oppure puoi ["creare gruppi e utenti locali"](#) .
- Integrare e testare il ["S3 API"](#) applicazioni client che utilizzerai per caricare oggetti sul tuo sistema StorageGRID .
- ["Configurare le regole di gestione del ciclo di vita delle informazioni \(ILM\) e la politica ILM"](#) che si desidera utilizzare per proteggere i dati degli oggetti.
- Se l'installazione include nodi di archiviazione dell'appliance, utilizzare SANtricity OS per completare le seguenti attività:
 - Connettersi a ciascun dispositivo StorageGRID .
 - Verificare la ricezione dei dati AutoSupport .

Vedere ["Configurare l'hardware"](#) .
- Rivedi e segui il ["Linee guida per il rafforzamento del sistema StorageGRID"](#) per eliminare i rischi per la sicurezza.
- ["Configurare le notifiche e-mail per gli avvisi di sistema"](#) .

Attività facoltative

- ["Aggiorna gli indirizzi IP dei nodi della griglia"](#) se sono cambiati da quando hai pianificato la distribuzione e generato il pacchetto di ripristino.
- ["Configurare la crittografia dell'archiviazione"](#), se necessario.
- ["Configurare la compressione dell'archiviazione"](#) per ridurre le dimensioni degli oggetti memorizzati, se necessario.
- ["Configurare le interfacce VLAN"](#) per isolare e partizionare il traffico di rete, se necessario.
- ["Configurare gruppi ad alta disponibilità"](#) per migliorare la disponibilità della connessione per i client Grid Manager, Tenant Manager e S3, se necessario.
- ["Configurare gli endpoint del bilanciamento del carico"](#) per la connettività client S3, se necessario.

Risolvere i problemi di installazione

Se si verificano problemi durante l'installazione del sistema StorageGRID , è possibile accedere ai file di registro dell'installazione. Potrebbe anche essere necessario che il supporto tecnico utilizzi i file di registro dell'installazione per risolvere i problemi.

I seguenti file di registro di installazione sono disponibili dal contenitore che esegue ciascun nodo:

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

I seguenti file di registro dell'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 ["Raccogli file di registro e dati di sistema"](#) .

Informazioni correlate

["Risoluzione dei problemi di un sistema StorageGRID"](#)

Esempio `/etc/network/interfaces`

IL `/etc/network/interfaces` Il file include tre sezioni, che definiscono le interfacce fisiche, l'interfaccia di collegamento e le interfacce VLAN. È possibile combinare le tre sezioni di esempio in un singolo file, che aggregherà quattro interfacce fisiche Linux in un singolo legame LACP e quindi stabilirà tre interfacce VLAN che sottendono il legame per l'uso come interfacce StorageGRID Grid, Admin e Client Network.

Interfacce fisiche

Si noti che gli switch alle altre estremità dei collegamenti devono anche trattare le quattro porte come un singolo trunk LACP o canale porta e devono passare almeno le tre VLAN referenziate 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 di legame

```
# 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
```

Installa StorageGRID su VMware

Guida rapida all'installazione di StorageGRID su VMware

Per installare un nodo VMware StorageGRID , seguire questi passaggi generali.

1

Preparazione

- Scopri di più ["Architettura StorageGRID e topologia di rete"](#) .
- Scopri le specifiche di ["Rete StorageGRID"](#) .
- Raccogliere e preparare il ["Informazioni e materiali richiesti"](#) .
- Installa e configura ["VMware vSphere Hypervisor, vCenter e gli host ESX"](#) .
- Preparare il necessario ["CPU e RAM"](#) .
- Provvedere a ["requisiti di archiviazione e prestazioni"](#) .

2

Distribuzione

Distribuisci i nodi della griglia. Quando si distribuiscono i nodi della griglia, questi vengono creati come parte del sistema StorageGRID e connessi a una o più reti.

- Utilizzare VMware vSphere Web Client, un file .vmdk e un set di modelli di file .ovf per ["distribuire i nodi basati su software come macchine virtuali \(VM\)"](#) sui server preparati nel passaggio 1.
- Per distribuire i nodi dell'appliance StorageGRID , seguire le istruzioni ["Avvio rapido per l'installazione dell'hardware"](#) .

3

Configurazione

Quando tutti i nodi sono stati distribuiti, utilizzare Grid Manager per ["configurare la griglia e completare l'installazione"](#) .

Automatizzare l'installazione

Per risparmiare tempo e garantire coerenza, è possibile automatizzare la distribuzione e la configurazione dei nodi della griglia e la configurazione del sistema StorageGRID .

- ["Automatizza la distribuzione dei nodi della griglia utilizzando VMware vSphere"](#) .
- Dopo aver distribuito i nodi della griglia, ["automatizzare la configurazione del sistema StorageGRID"](#) utilizzando lo script di configurazione Python fornito nell'archivio di installazione.
- ["Automatizzare l'installazione e la configurazione dei nodi della griglia degli elettrodomestici"](#)
- Se sei uno sviluppatore avanzato di distribuzioni StorageGRID , automatizza l'installazione dei nodi della griglia utilizzando ["installazione REST API"](#) .

Pianificare e preparare l'installazione su VMware

Informazioni e materiali richiesti

Prima di installare StorageGRID, raccogliere e preparare le informazioni e i materiali richiesti.

Informazioni richieste

Piano di rete

Quali reti intendi collegare a ciascun nodo StorageGRID . StorageGRID supporta più reti per la separazione del traffico, la sicurezza e la praticità amministrativa.

Vedi StorageGRID ["Linee guida per il networking"](#) .

Informazioni di rete

Indirizzi IP da assegnare a ciascun nodo della griglia e gli indirizzi IP dei server DNS e NTP.

Server per nodi di griglia

Identifica un set di server (fisici, virtuali o entrambi) che, nel complesso, forniscano risorse sufficienti a supportare il numero e il tipo di nodi StorageGRID che intendi distribuire.



Se l'installazione StorageGRID non utilizzerà i nodi StorageGRID (hardware) dell'appliance StorageGRID, è necessario utilizzare un archivio RAID hardware con cache di scrittura con batteria di backup (BBWC). StorageGRID non supporta l'uso di reti di archiviazione virtuali (vSAN), RAID software o nessuna protezione RAID.

Informazioni correlate

["Strumento matrice di interoperabilità NetApp"](#)

Materiali richiesti

Licenza NetApp StorageGRID

È necessario disporre di una licenza NetApp valida e firmata digitalmente.



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

Archivio di installazione di StorageGRID

["Scarica l'archivio di installazione StorageGRID ed estrai i file"](#) .

Computer portatile di servizio

Il sistema StorageGRID viene installato tramite un laptop di servizio.

Il portatile di servizio deve avere:

- Porta di rete
- Client SSH (ad esempio, PuTTY)
- ["Browser web supportato"](#)

Documentazione StorageGRID

- ["Note di rilascio"](#)
- ["Istruzioni per la gestione di StorageGRID"](#)

Scarica ed estrai i file di installazione StorageGRID

È necessario scaricare gli archivi di installazione StorageGRID ed estrarre i file. Facoltativamente, è possibile verificare manualmente i file nel pacchetto di installazione.

Passi

1. Vai al ["Pagina di download di NetApp per StorageGRID"](#) .
2. Seleziona il pulsante per scaricare l'ultima versione oppure seleziona un'altra versione dal menu a discesa e seleziona **Vai**.
3. Sign in con il nome utente e la password del tuo account NetApp .
4. Se viene visualizzata una dichiarazione di Attenzione/Lettura obbligatoria, leggerla e selezionare la casella di controllo.



Dopo aver installato la versione StorageGRID , è necessario applicare tutti gli hotfix richiesti. Per maggiori informazioni, vedere il ["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 **Accetta e continua**.
6. Nella colonna **Installa StorageGRID**, seleziona l'archivio di installazione .tgz o .zip per VMware.



Utilizzare il .zip file se si utilizza Windows sul portatile di servizio.

7. Salvare l'archivio di installazione.
8. Se è necessario verificare l'archivio di installazione:
 - a. Scarica il pacchetto di verifica della firma del codice StorageGRID . Il nome del file per questo pacchetto utilizza il formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , Dove `<version-number>` è la versione del software StorageGRID .
 - b. Segui i passaggi per ["verificare manualmente i file di installazione"](#) .
9. Estrarre i file dall'archivio di installazione.

10. Scegli i file di cui hai bisogno.

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



I percorsi elencati nella tabella sono relativi alla directory di livello superiore 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 StorageGRID .
	Una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	File del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodi di griglia.
	Il file modello Open Virtualization Format(.ovf) e file manifesto(.mf) per distribuire il nodo di amministrazione primario.
	Il file modello(.ovf) e file manifesto(.mf) per distribuire nodi amministrativi non primari.
	Il file modello(.ovf) e file manifesto(.mf) per la distribuzione dei nodi gateway.
	Il file modello(.ovf) e file manifesto(.mf) per distribuire nodi di archiviazione basati su macchine virtuali.
Strumento di scripting di distribuzione	Descrizione
	Uno script shell Bash utilizzato per automatizzare la distribuzione di nodi di griglia virtuali.
	Un file di configurazione di esempio da utilizzare con <code>deploy-vsphere-ovftool.sh</code> sceneggiatura.
	Uno script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID .
	Uno script Python utilizzato per automatizzare la configurazione degli appliance StorageGRID .

Percorso e nome del file	Descrizione
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO). È possibile utilizzare questo script anche per l'integrazione di Ping Federate.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO) tramite Active Directory o Ping Federate.
	Uno script di supporto chiamato dal compagno <code>storagegrid-ssoauth-azure.py</code> Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: prima di eseguire un aggiornamento, puoi utilizzare questi schemi per confermare che il codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova versione StorageGRID se non disponi di un ambiente StorageGRID non di produzione per i test di compatibilità dell'aggiornamento.

Verifica manuale dei file di installazione (facoltativo)

Se necessario, è possibile verificare manualmente i file nell'archivio di installazione StorageGRID .

Prima di iniziare

Hai [scaricato il pacchetto di verifica](#) dal ["Pagina di download di NetApp per StorageGRID"](#) .

Passi

1. Estrarre gli artefatti dal pacchetto di verifica:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Assicurarsi che questi artefatti siano stati estratti:

- Certificato fogliare: `Leaf-Cert.pem`
- Catena di certificati: `CA-Int-Cert.pem`

- Catena di risposta del timestamp: TS-Cert.pem
- File di checksum: sha256sum
- Firma di checksum: sha256sum.sig
- File di risposta con timestamp: sha256sum.sig.tsr

3. Utilizzare la catena per verificare che il certificato fogliare sia valido.

Esempio: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Risultati previsti: Leaf-Cert.pem: OK

4. Se il passaggio 2 non è riuscito a causa di un certificato foglia scaduto, utilizzare tsr file da verificare.

Esempio: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

I risultati previsti includono: Verification: OK

5. Creare un file di chiave pubblica dal certificato foglia.

Esempio: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Risultato previsto: *nessuno*

6. Utilizzare la chiave pubblica per verificare il sha256sum presentare ricorso contro sha256sum.sig .

Esempio: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Risultati previsti: Verified OK

7. Verificare il sha256sum il contenuto del file rispetto ai checksum appena creati.

Esempio: `sha256sum -c sha256sum`

Risultati previsti: *<filename>*: OK
<filename> è il nome del file di archivio che hai scaricato.

8. ["Completa i passaggi rimanenti"](#) per estrarre e scegliere i file di installazione appropriati.

Requisiti software per VMware

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

VMware vSphere Hypervisor

È necessario installare VMware vSphere Hypervisor su un server fisico preparato. Prima di installare il software VMware, è necessario configurare correttamente l'hardware (incluse le versioni del firmware e le impostazioni del BIOS).

- Configurare la rete nell'hypervisor come richiesto per supportare la 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 poter 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 l'ora dell'host non è corretta, potrebbero verificarsi effetti negativi, tra cui la perdita di dati.

Requisiti di configurazione VMware

Prima di distribuire i nodi StorageGRID è necessario installare e configurare VMware vSphere e vCenter.

Per le versioni supportate del software VMware vSphere Hypervisor e VMware vCenter Server, vedere ["Strumento matrice di interoperabilità NetApp"](#).

Per i passaggi necessari per installare questi prodotti VMware, consultare la documentazione VMware.

Requisiti CPU e RAM

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

Ogni nodo StorageGRID richiede le seguenti risorse minime:

- Core CPU: 8 per nodo
- RAM: Dipende dalla RAM totale disponibile e dalla quantità di software non StorageGRID in esecuzione sul sistema
 - In genere, almeno 24 GB per nodo e da 2 a 16 GB in meno rispetto alla RAM totale del sistema
 - Un minimo di 64 GB per ogni tenant che avrà circa 5.000 bucket

Le risorse dei nodi basati solo su metadati software devono corrispondere alle risorse dei nodi di archiviazione esistenti. Per esempio:

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

Quando si aggiunge un nuovo sito StorageGRID , la capacità totale dei metadati del nuovo sito deve corrispondere almeno ai siti StorageGRID esistenti e le risorse del nuovo sito devono corrispondere ai nodi di archiviazione nei siti StorageGRID esistenti.

VMware supporta un nodo per macchina virtuale. Assicurarsi che il nodo StorageGRID non superi la RAM fisica disponibile. Ogni macchina virtuale deve essere dedicata all'esecuzione di StorageGRID.



Monitora regolarmente l'utilizzo della CPU e della memoria per assicurarti che queste risorse continuino a soddisfare il tuo carico di lavoro. Ad esempio, raddoppiando l'allocazione di RAM e CPU per i nodi di archiviazione virtuali si otterrebbero risorse simili a quelle fornite per i nodi dell'appliance StorageGRID . Inoltre, se la quantità di metadati per nodo supera i 500 GB, valutare di aumentare la RAM per nodo a 48 GB o più. Per informazioni sulla gestione dell'archiviazione dei metadati degli oggetti, sull'aumento dell'impostazione Spazio riservato ai metadati e sul monitoraggio dell'utilizzo della CPU e della memoria, vedere le istruzioni per ["amministrare"](#) , ["monitoraggio"](#) , E ["aggiornamento"](#) StorageGRID.

Se l'hyperthreading è abilitato sugli host fisici sottostanti, è possibile fornire 8 core virtuali (4 core fisici) per nodo. Se l'hyperthreading non è abilitato 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 VM, è consigliabile utilizzare una singola VM per ogni nodo StorageGRID e dimensionare la VM di conseguenza.

Vedere anche ["Requisiti di archiviazione e prestazioni"](#) .

Requisiti di archiviazione e prestazioni

È necessario comprendere i requisiti di archiviazione e prestazioni per i nodi StorageGRID ospitati da macchine virtuali, in modo da poter fornire spazio sufficiente per supportare la configurazione iniziale e la futura espansione dell'archiviazione.

Requisiti di prestazione

Le prestazioni del volume del sistema operativo e del primo volume di archiviazione influiscono in modo significativo sulle prestazioni complessive del sistema. Assicurarsi che forniscano prestazioni del disco adeguate in termini di latenza, operazioni di input/output al secondo (IOPS) e throughput.

Tutti i nodi StorageGRID richiedono che l'unità del sistema operativo e tutti i volumi di archiviazione abbiano la memorizzazione nella cache write-back abilitata. La cache deve trovarsi su un supporto protetto o persistente.

Requisiti per le macchine virtuali che utilizzano lo storage NetApp ONTAP

Se si distribuisce un nodo StorageGRID come macchina virtuale con storage assegnato da un sistema NetApp ONTAP , è stato verificato che il volume non ha un criterio di suddivisione in livelli FabricPool abilitato. Ad esempio, se un nodo StorageGRID è in esecuzione come macchina virtuale su un host VMware, assicurarsi che il volume che supporta il datastore per il nodo non abbia un criterio di suddivisione in livelli FabricPool abilitato. La disattivazione della suddivisione in livelli FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di archiviazione.



Non utilizzare mai FabricPool per riportare i dati relativi a StorageGRID a StorageGRID stesso. Il riordino dei dati StorageGRID su StorageGRID aumenta la complessità operativa e la risoluzione dei problemi.

Numero di macchine virtuali richieste

Ogni sito StorageGRID richiede un minimo di tre nodi di archiviazione.

Requisiti di archiviazione 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.



Gli snapshot del disco non possono essere utilizzati per ripristinare i nodi della griglia. Fare invece riferimento al "[ripristino del nodo della griglia](#)" procedure per ogni tipo di nodo.

Tipo di nodo	Magazzinaggio
Nodo di amministrazione	LUN da 100 GB per il sistema operativo LUN da 200 GB per le tabelle dei nodi di amministrazione LUN da 200 GB per il registro di controllo del nodo di amministrazione
Nodo di archiviazione	LUN da 100 GB per il sistema operativo 3 LUN per ogni nodo di archiviazione su questo host Nota: un nodo di archiviazione può avere da 1 a 16 LUN di archiviazione; si consigliano almeno 3 LUN di archiviazione. Dimensione minima per LUN: 4 TB Dimensione massima LUN testata: 39 TB.
Nodo di archiviazione (solo metadati)	LUN da 100 GB per il sistema operativo 1 LUN Dimensione minima per LUN: 4 TB Dimensione massima LUN testata: 39 TB. Nota: per i nodi di archiviazione solo metadati è richiesto un solo rangedb.
Nodo Gateway	LUN da 100 GB per il sistema operativo



A seconda del livello di controllo configurato, delle dimensioni degli input utente, come il nome della chiave dell'oggetto S3, e della quantità di dati del registro di controllo da conservare, potrebbe essere necessario aumentare le dimensioni della LUN del registro di controllo su ciascun nodo di amministrazione. In genere, una griglia genera circa 1 KB di dati di controllo per operazione S3, il che significa che una LUN da 200 GB supporterebbe 70 milioni di operazioni al giorno o 800 operazioni al secondo per due o tre giorni.

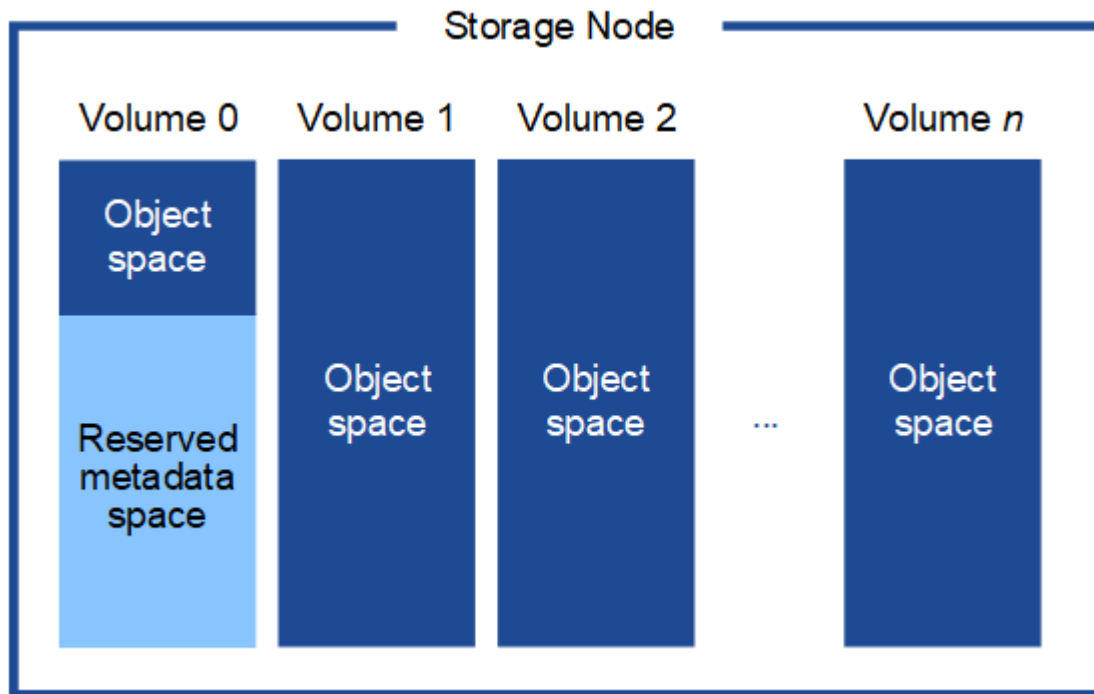
Requisiti di archiviazione per i nodi di archiviazione

Un nodo di archiviazione basato su software può avere da 1 a 16 volumi di archiviazione; si consigliano 3 o più volumi di archiviazione. Ogni volume di archiviazione deve essere pari o superiore a 4 TB.



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

Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di archiviazione 0 di ciascun nodo di archiviazione. Tutto lo spazio rimanente sul volume di archiviazione 0 e su tutti gli altri volumi di archiviazione nel nodo di archiviazione viene utilizzato esclusivamente per i dati degli oggetti.



Per garantire ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti nel sistema in ogni sito. Le tre copie dei metadati degli oggetti vengono distribuite uniformemente tra tutti i nodi di archiviazione di ciascun sito.

Quando si installa una griglia con nodi di archiviazione solo metadati, la griglia deve contenere anche un numero minimo di nodi per l'archiviazione degli oggetti. Vedere ["Tipi di nodi di archiviazione"](#) per ulteriori informazioni sui nodi di archiviazione solo metadati.

- Per una griglia a sito singolo, sono configurati almeno due nodi di archiviazione per oggetti e metadati.
- Per una griglia multi-sito, almeno un nodo di archiviazione per sito è configurato per oggetti e metadati.

Quando si assegna spazio al volume 0 di un nuovo nodo di archiviazione, è necessario assicurarsi che vi sia spazio adeguato per la porzione di tutti i metadati degli oggetti di quel nodo.

- Come minimo, è necessario assegnare almeno 4 TB al volume 0.



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



Se si assegnano meno di 500 GB al volume 0 (solo per uso non produttivo), il 10% della capacità del volume di archiviazione è riservato ai metadati.

- Le risorse dei nodi basati solo su metadati software devono corrispondere alle risorse dei nodi di archiviazione esistenti. Per esempio:
 - Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo su software devono soddisfare i seguenti requisiti minimi:
 - 128 GB di RAM
 - CPU a 8 core
 - SSD da 8 TB o spazio di archiviazione equivalente per il database Cassandra (rangedb/0)
 - Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuali con 24 GB di RAM, CPU a 8 core e 3 TB o 4 TB di spazio di archiviazione dei metadati, i nodi basati solo su software devono utilizzare risorse simili (24 GB di RAM, CPU a 8 core e 4 TB di spazio di archiviazione dei metadati (rangedb/0).

Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve corrispondere almeno ai siti StorageGRID esistenti e le risorse del nuovo sito devono corrispondere ai nodi di archiviazione nei siti StorageGRID esistenti.

- Se si installa un nuovo sistema (StorageGRID 11.6 o versione successiva) e ogni nodo di archiviazione dispone di 128 GB o più di RAM, assegnare 8 TB o più al volume 0. Utilizzando un valore maggiore per il volume 0 è possibile aumentare lo spazio consentito per i metadati su ciascun nodo di archiviazione.
- Quando si configurano diversi nodi di archiviazione per un sito, utilizzare la stessa impostazione per il volume 0, se possibile. Se un sito contiene nodi di archiviazione di dimensioni diverse, il nodo di archiviazione con il volume più piccolo, 0, determinerà la capacità dei metadati di quel sito.

Per i dettagli, vai a ["Gestire l'archiviazione dei metadati degli oggetti"](#).

Automatizzare l'installazione (VMware)

È possibile utilizzare VMware OVF Tool per automatizzare la distribuzione dei nodi della griglia. È anche possibile automatizzare la configurazione di StorageGRID.

Automatizza la distribuzione dei nodi della griglia

Utilizzare lo strumento VMware OVF per automatizzare la distribuzione dei nodi della griglia.

Prima di iniziare

- Hai accesso a un sistema Linux/Unix con Bash 3.2 o versione successiva.
- Hai VMware vSphere con vCenter
- VMware OVF Tool 4.1 è installato e configurato correttamente.
- Conosci il nome utente e la password per accedere a VMware vSphere utilizzando lo strumento OVF
- Si dispone delle autorizzazioni sufficienti per distribuire VM dai file OVF e accenderle, nonché delle autorizzazioni per creare volumi aggiuntivi da collegare alle VM. Vedi il `ovftool` documentazione per i dettagli.
- Conosci l'URL dell'infrastruttura virtuale (VI) per la posizione in vSphere in cui desideri distribuire le macchine virtuali StorageGRID. In genere questo URL sarà una vApp o un pool di risorse. Ad esempio:
`vi://vcenter.example.com/vi/sghs`



Puoi usare VMware `ovftool` utilità per determinare questo valore (vedere il `ovftool` documentazione per i dettagli).



Se si esegue la distribuzione su una vApp, le macchine virtuali non si avvieranno automaticamente la prima volta e sarà necessario accenderle manualmente.

- Hai raccolto tutte le informazioni necessarie per il file di configurazione della distribuzione. Vedere "[Raccogli informazioni sul tuo ambiente di distribuzione](#)" per informazioni.
- È possibile accedere ai seguenti file dall'archivio di installazione VMware per StorageGRID:

Nome del file	Descrizione
NetApp-SG-versione-SHA.vmdk	File del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodi di griglia. Nota: Questo file deve trovarsi nella stessa cartella del <code>.ovf</code> e <code>.mf</code> file.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Il file modello Open Virtualization Format(<code>.ovf</code>) e file manifesto(<code>.mf</code>) per distribuire il nodo di amministrazione primario.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Il file modello(<code>.ovf</code>) e file manifesto(<code>.mf</code>) per distribuire nodi amministrativi non primari.
vsphere-gateway.ovf vsphere-gateway.mf	Il file modello(<code>.ovf</code>) e file manifesto(<code>.mf</code>) per la distribuzione dei nodi gateway.
vsphere-storage.ovf vsphere-storage.mf	Il file modello(<code>.ovf</code>) e file manifesto(<code>.mf</code>) per distribuire nodi di archiviazione basati su macchine virtuali.
distribuire-vsphere-ovftool.sh	Lo script shell Bash utilizzato per automatizzare la distribuzione dei nodi della griglia virtuale.
deploy-vsphere-ovftool-sample.ini	Il file di configurazione di esempio da utilizzare con <code>deploy-vsphere-ovftool.sh</code> sceneggiatura.

Definisci il file di configurazione per la tua distribuzione

È possibile specificare le informazioni necessarie per distribuire i nodi della griglia virtuale 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.

Passi

1. Crea una copia del file di configurazione di esempio(`deploy-vsphere-ovftool.sample.ini`). Salva il nuovo file come `deploy-vsphere-ovftool.ini` nella stessa directory di `deploy-vsphere-ovftool.sh`.

2. Aprire `deploy-vsphere-ovftool.ini`.
3. Inserisci tutte le informazioni necessarie per distribuire i nodi della griglia virtuale VMware.

Vedere [Impostazioni del file di configurazione](#) per informazioni.

4. Dopo aver inserito e verificato 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 distribuire i nodi della griglia virtuale.

Il file di configurazione elenca prima i parametri globali, quindi elenca 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.
- I parametri specifici del nodo sostituiscono i parametri globali.

Parametri globali

I parametri globali vengono applicati a tutti i nodi della griglia, a meno che non vengano sovrascritti dalle impostazioni nelle singole sezioni. Inserire i parametri che si applicano a più nodi nella sezione dei parametri globali, quindi sovrascrivere queste impostazioni, se necessario, nelle sezioni per i singoli nodi.

- **OVFTOOL_ARGUMENTS:** È possibile specificare `OVFTOOL_ARGUMENTS` come impostazioni globali oppure applicare argomenti singolarmente a nodi specifici. Per esempio:

```
OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
--datastore='datastore_name'
```

Puoi usare il `--powerOffTarget` E `--overwrite` opzioni per arrestare e sostituire le macchine virtuali esistenti.



Dovresti distribuire i nodi su diversi datastore e specificare `OVFTOOL_ARGUMENTS` per ogni nodo, anziché globalmente.

- **FONTE:** Il percorso al modello della macchina virtuale `StorageGRID(.vmdk)` file e il `.ovf` E `.mf` file per singoli nodi della griglia. Per impostazione predefinita, viene utilizzata la directory corrente.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **TARGET:** URL dell'infrastruttura virtuale VMware vSphere (vi) per la posizione in cui verrà distribuito `StorageGRID`. Per esempio:

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG:** Metodo utilizzato per acquisire gli indirizzi IP, STATICO o DHCP. L'impostazione predefinita è STATICO. Se tutti o la maggior parte dei nodi utilizzano lo stesso metodo per

acquisire gli indirizzi IP, è possibile specificare tale metodo qui. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
GRID_NETWORK_CONFIG = STATIC
```

- **GRID_NETWORK_TARGET:** Nome di una rete VMware esistente da utilizzare per la rete Grid. Se tutti o la maggior parte dei nodi utilizzano lo stesso nome di rete, è possibile specificarlo qui. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
GRID_NETWORK_TARGET = SG Admin Network
```

- **GRID_NETWORK_MASK:** Maschera di rete per la rete Grid. Se tutti o la maggior parte dei nodi utilizzano la stessa maschera di rete, è possibile specificarla qui. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY:** Gateway di rete per la rete Grid. Se tutti o la maggior parte dei nodi utilizzano lo stesso gateway di rete, è possibile specificarlo qui. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU:** Facoltativo. L'unità di trasmissione massima (MTU) sulla rete elettrica. Se specificato, il valore deve essere compreso tra 1280 e 9216. Per esempio:

```
GRID_NETWORK_MTU = 9000
```

Se omissso, viene utilizzato 1400.

Se si desidera utilizzare i jumbo frame, impostare l'MTU su un valore adatto ai jumbo frame, ad esempio 9000. Altrimenti, mantieni il valore predefinito.



Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch virtuale in vSphere a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di prestazioni di rete o perdita di pacchetti.



Per ottenere le migliori prestazioni di rete, tutti i nodi devono essere configurati con valori MTU simili sulle loro interfacce Grid Network. L'avviso **Mancata corrispondenza MTU della rete Grid** viene attivato se si verifica una differenza significativa nelle impostazioni MTU per la rete Grid sui singoli nodi. I valori MTU non devono essere gli stessi per tutti i tipi di rete.

- **ADMIN_NETWORK_CONFIG:** Metodo utilizzato per acquisire gli indirizzi IP, DISABILITATO, STATICO o DHCP. L'impostazione predefinita è DISABILITATO. Se tutti o la maggior parte dei nodi utilizzano lo stesso

metodo per acquisire gli indirizzi IP, è possibile specificare tale metodo qui. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET:** Nome di una rete VMware esistente da utilizzare per la rete di amministrazione. Questa impostazione è obbligatoria a meno che la rete di amministrazione non sia disabilitata. Se tutti o la maggior parte dei nodi utilizzano lo stesso nome di rete, è possibile specificarlo qui. A differenza della rete Grid, non è necessario che tutti i nodi siano connessi alla stessa rete di amministrazione. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- **ADMIN_NETWORK_MASK:** 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 sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY:** Gateway di rete per la rete di amministrazione. Questa impostazione è obbligatoria se si utilizza l'indirizzamento IP statico e si specificano subnet esterne nell'impostazione ADMIN_NETWORK_ESL. (Ciò significa che 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 sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL:** Elenco delle subnet esterne (routes) per la rete di amministrazione, specificato come elenco separato da virgole di destinazioni di route CIDR. Se tutti o la maggior parte dei nodi utilizzano lo stesso elenco di subnet esterne, è possibile specificarlo qui. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU:** Facoltativo. 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 omissso, viene utilizzato 1400. Se si desidera utilizzare i jumbo frame, impostare l'MTU su un valore adatto ai jumbo frame, ad esempio 9000. Altrimenti, mantieni il valore predefinito. Se tutti o la maggior parte dei nodi utilizzano lo stesso MTU per la rete di amministrazione, è possibile specificarlo qui. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:


```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG:** metodo utilizzato per acquisire gli indirizzi IP, DISABILITATO, STATICO o DHCP. L'impostazione predefinita è DISABILITATO. Se tutti o la maggior parte dei nodi utilizzano lo stesso metodo per acquisire gli indirizzi IP, è possibile specificare tale metodo qui. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET:** Nome di una rete VMware esistente da utilizzare per la rete client. Questa impostazione è obbligatoria a meno che la rete client non sia disabilitata. Se tutti o la maggior parte dei nodi utilizzano lo stesso nome di rete, è possibile specificarlo qui. A differenza della rete Grid, non è necessario che tutti i nodi siano connessi alla stessa rete client. È quindi possibile sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- **CLIENT_NETWORK_MASK:** 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 sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per 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 sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU:** Facoltativo. 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 jumbo frame, impostare l'MTU su un valore adatto ai jumbo frame, ad esempio 9000. Altrimenti, mantieni 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 sovrascrivere l'impostazione globale specificando impostazioni diverse per uno o più nodi individuali. Per esempio:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP:** Riassegna qualsiasi porta utilizzata da un nodo per le comunicazioni interne del nodo della griglia o per le comunicazioni esterne. La rimappatura delle porte è necessaria se i criteri di rete aziendale limitano una o più porte utilizzate da StorageGRID. Per l'elenco delle porte utilizzate da

StorageGRID, vedere le comunicazioni interne del nodo della griglia e le comunicazioni esterne in "[Linee guida per il networking](#)".



Non rimappare le porte che intendi utilizzare per configurare gli endpoint del bilanciatore del carico.



Se è impostato solo PORT_REMAP, la mappatura specificata viene utilizzata sia per le comunicazioni in entrata che per quelle 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.

Per esempio:

```
PORT_REMAP = client/tcp/18082/443
```

Se utilizzata da sola, questa impostazione di esempio mappa in modo simmetrico le comunicazioni in entrata e in uscita per il nodo della griglia dalla porta 18082 alla porta 443. Se utilizzata insieme a PORT_REMAP_INBOUND, questa impostazione di esempio mappa le comunicazioni in uscita dalla porta 18082 alla porta 443.

È anche possibile rimappare più porte utilizzando un elenco separato da virgole.

Per esempio:

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- **PORT_REMAP_INBOUND:** Riassegna 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 intendi utilizzare per configurare gli endpoint del bilanciatore 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.

Per esempio:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

Questo esempio prende il traffico inviato alla porta 443 per superare un firewall interno e lo indirizza alla porta 18082, dove il nodo della griglia è in ascolto delle richieste S3.

È anche possibile rimappare più porte in ingresso utilizzando un elenco separato da virgole.

Per esempio:

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- **TEMPORARY_PASSWORD_TYPE**: Tipo di password di installazione temporanea da utilizzare quando si accede alla console della VM o all'API di installazione StorageGRID , oppure tramite 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 dei parametri globali. Quindi, se lo si desidera, utilizzare un'impostazione diversa per un singolo nodo. Ad esempio, se selezioni **Usa password personalizzata** a livello globale, puoi usare **CUSTOM_TEMPORARY_PASSWORD=<password>** per impostare la password per ciascun nodo.

TEMPORARY_PASSWORD_TYPE può essere uno dei seguenti:

- **Usa nome nodo**: il nome del nodo viene utilizzato come password di installazione temporanea e fornisce l'accesso alla console della VM, all'API di installazione StorageGRID e a SSH.
- **Disabilita password**: non verrà utilizzata alcuna password di installazione temporanea. Se è necessario accedere alla macchina virtuale per risolvere i 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 e fornisce l'accesso alla console della VM, all'API di installazione StorageGRID e a SSH.



Facoltativamente, è possibile omettere il parametro **TEMPORARY_PASSWORD_TYPE** e specificare solo **CUSTOM_TEMPORARY_PASSWORD=<password>**.

- **CUSTOM_TEMPORARY_PASSWORD=<password>** Facoltativo. Password temporanea da utilizzare durante l'installazione per accedere alla console della VM, all'API di installazione StorageGRID e a SSH. Ignorato se **TEMPORARY_PASSWORD_TYPE** è impostato su **Usa nome nodo** o **Disabilita password**.

Parametri specifici del nodo

Ogni nodo si trova nella propria sezione del file di configurazione. Ogni nodo richiede le seguenti impostazioni:

- L'intestazione della sezione definisce il nome del nodo che verrà visualizzato in Grid Manager. È possibile sovrascrivere tale valore specificando il parametro facoltativo **NODE_NAME** per il nodo.
- **NODE_TYPE**: VM_Admin_Node, VM_Storage_Node o VM_API_Gateway_Node
- **STORAGE_TYPE**: combinato, dati o metadati. Se non specificato, questo parametro facoltativo per i nodi di archiviazione è impostato di default su combinato (dati e metadati). Per ulteriori informazioni, consultare ["Tipi di nodi di archiviazione"](#) .
- **GRID_NETWORK_IP**: l'indirizzo IP del nodo sulla rete Grid.
- **ADMIN_NETWORK_IP**: l'indirizzo IP del nodo sulla 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 di amministrazione 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 tramite mDNS. Per ulteriori informazioni, consultare ["Come i nodi della griglia scoprono 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 a livello globale. 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 di amministrazione primario

Per il nodo di amministrazione primario sono necessarie le seguenti impostazioni aggiuntive:

- **NODE_TYPE:** VM_Admin_Node
- **ADMIN_ROLE:** Primario

Questa voce di esempio è per un nodo di amministrazione primario presente su tutte e tre le reti:

```
[DC1-ADM1]
ADMIN_ROLE = Primary
NODE_TYPE = VM_Admin_Node
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd

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 amministrativi vengono assegnati due dischi rigidi aggiuntivi da 200 GB per l'utilizzo di database e audit. È possibile aumentare queste impostazioni utilizzando il parametro DISK. Per esempio:

```
DISK = INSTANCES=2, CAPACITY=300
```



Per i nodi di amministrazione, ISTANZA deve sempre essere uguale a 2.

Nodo di archiviazione

Per i nodi di archiviazione è richiesta la seguente impostazione aggiuntiva:

- **NODE_TYPE:** VM_Storage_Node

Questa voce di esempio è per un nodo di archiviazione che si trova sulla rete Grid e sulla rete di amministrazione, ma non sulla rete client. Questo nodo utilizza l'impostazione ADMIN_IP per specificare l'indirizzo IP del nodo di amministrazione primario sulla rete Grid.

```
[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
```

Questa seconda voce di esempio riguarda un nodo di archiviazione su una rete client in cui la politica di rete aziendale del cliente stabilisce che un'applicazione client S3 può accedere al nodo di archiviazione solo tramite la porta 80 o 443. Il file di configurazione di esempio utilizza PORT_REMAP per consentire al nodo di archiviazione 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 una rimappatura simmetrica per il traffico ssh dalla porta 22 alla porta 3022, ma imposta esplicitamente i valori sia per il traffico in entrata che per quello 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
```

Le seguenti impostazioni aggiuntive sono facoltative per i nodi di archiviazione:

- **DISCO:** Per impostazione predefinita, ai nodi di archiviazione vengono assegnati tre dischi da 4 TB per l'utilizzo di RangeDB. È possibile aumentare queste impostazioni con il parametro DISK. Per esempio:

```
DISK = INSTANCES=16, CAPACITY=4096
```

- **STORAGE_TYPE:** Per impostazione predefinita, tutti i nuovi nodi di archiviazione sono configurati per

archiviare sia i dati degli oggetti che i metadati, noti come nodi di archiviazione *combinati*. È possibile modificare il tipo di nodo di archiviazione per archiviare solo dati o metadati con il parametro `STORAGE_TYPE`. Per esempio:

```
STORAGE_TYPE = data
```

Nodo Gateway

Per i nodi gateway è richiesta la seguente impostazione aggiuntiva:

- **NODE_TYPE:** VM_API_Gateway

Questa voce di esempio è per un nodo gateway di esempio su tutte e tre le reti. In questo esempio, non sono stati specificati parametri di rete client nella sezione globale del file di configurazione, quindi devono essere specificati 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 amministratore non primario

Per i nodi amministrativi non primari sono necessarie le seguenti impostazioni aggiuntive:

- **NODE_TYPE:** VM_Admin_Node
- **ADMIN_ROLE:** Non primario

Questa voce di esempio è per un nodo di amministrazione non primario che non si trova sulla 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 amministrativi non primari:

- **DISCO:** Per impostazione predefinita, ai nodi amministrativi vengono assegnati due dischi rigidi aggiuntivi da 200 GB per l'utilizzo di database e audit. È possibile aumentare queste impostazioni utilizzando il parametro DISK. Per esempio:

```
DISK = INSTANCES=2, CAPACITY=300
```



Per i nodi di amministrazione, ISTANZA deve sempre essere uguale a 2.

Esegui lo script Bash

Puoi usare il `deploy-vsphere-ovftool.sh` Script Bash e file di configurazione `deploy-vsphere-ovftool.ini` modificati per automatizzare la distribuzione dei nodi StorageGRID in VMware vSphere.

Prima di iniziare

Hai creato un file di configurazione `deploy-vsphere-ovftool.ini` per il tuo ambiente.

È possibile utilizzare la guida disponibile con lo script Bash immettendo i comandi di aiuto (`-h/--help`). Per esempio:

```
./deploy-vsphere-ovftool.sh -h
```

O

```
./deploy-vsphere-ovftool.sh --help
```

Passi

1. Accedi al computer Linux che stai utilizzando per eseguire lo script Bash.
2. Passare alla directory in cui è stato estratto l'archivio di installazione.

Per esempio:

```
cd StorageGRID-Webscale-version/vsphere
```

3. Per distribuire tutti i nodi della griglia, eseguire lo script Bash con le opzioni appropriate per il proprio ambiente.

Per esempio:

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-  
vsphere-ovftool.ini
```

4. Se la distribuzione di un nodo della griglia non riesce a causa di un errore, risolvere l'errore ed eseguire nuovamente lo script Bash solo per quel nodo.

Per esempio:

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single  
-node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

La distribuzione è completa quando lo stato di ciascun nodo è "Superato".

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

Automatizza la configurazione di StorageGRID

Dopo aver distribuito i nodi della griglia, è possibile automatizzare la configurazione del sistema StorageGRID .

Prima di iniziare

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

Nome del file	Descrizione
configure-storagegrid.py	Script Python utilizzato per automatizzare la configurazione

Nome del 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

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

Puoi usare il `configure-storagegrid.py` Script Python e il `configure-storagegrid.json` file di configurazione della griglia per automatizzare la configurazione del sistema StorageGRID .



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

Passi

1. Accedi al computer Linux che stai utilizzando per eseguire lo script Python.
2. Passare alla directory in cui è stato estratto l'archivio di installazione.

Per esempio:

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

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

3. Esegui lo script Python e utilizza il file di configurazione che hai creato.

Per esempio:

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

Risultato

Un pacchetto di recupero `.zip` Il file viene generato durante il processo di configurazione e scaricato nella directory in cui si sta eseguendo 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, copialo in una posizione di rete protetta e sottoposta a backup e in un archivio cloud protetto.



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 hai specificato che devono essere generate password casuali, apri il `Passwords.txt` file e cerca le password necessarie per accedere al tuo 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 è installato e configurato quando viene visualizzato un messaggio di conferma.

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

Informazioni correlate

- ["Vai al Grid Manager"](#)
- ["Installazione REST API"](#)

Distribuisci nodi di griglia di macchine virtuali (VMware)

Raccogli informazioni sul tuo ambiente di distribuzione

Prima di distribuire i nodi della griglia, è necessario raccogliere informazioni sulla configurazione di rete e sull'ambiente VMware.



È più efficiente eseguire un'unica installazione di tutti i nodi, piuttosto che installare alcuni nodi ora e altri in seguito.

Informazioni VMware

È necessario accedere all'ambiente di distribuzione e raccogliere informazioni sull'ambiente VMware, sulle reti create per Grid, Admin e Client Network e sui tipi di volumi di archiviazione che si intende utilizzare per i nodi di archiviazione.

È necessario raccogliere informazioni sul proprio ambiente VMware, tra cui:

- Nome utente e password per un account VMware vSphere dotato delle autorizzazioni appropriate per completare la distribuzione.
- Informazioni sulla configurazione di host, datastore e rete per ogni macchina virtuale del nodo StorageGRID .



VMware Live vMotion provoca un salto temporale nella macchina virtuale e non è supportato per nodi di griglia di alcun tipo. Anche se raramente, orari errati possono causare la perdita di dati o di aggiornamenti della configurazione.

Informazioni sulla rete Grid

È necessario raccogliere informazioni sulla rete VMware creata per StorageGRID Grid Network (obbligatorio), tra cui:

- Il nome della rete.
- Metodo utilizzato per assegnare gli indirizzi IP, statico 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 di amministrazione primario sulla rete Grid. Vedere ["Come i nodi della griglia scoprono il nodo di amministrazione primario"](#) per maggiori informazioni.

Informazioni sulla rete di amministrazione

Per i nodi che saranno connessi alla rete di amministrazione StorageGRID opzionale, è necessario raccogliere informazioni sulla rete VMware creata per questa rete, tra cui:

- Il nome della rete.
- Metodo utilizzato per assegnare gli indirizzi IP, statico 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 di amministrazione primario sulla rete Grid. Vedere ["Come i nodi della griglia scoprono il nodo di amministrazione primario"](#) per maggiori informazioni.
- L'elenco delle subnet esterne (ESL) per la rete di amministrazione.

Informazioni sulla rete del cliente

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 gli indirizzi IP, statico 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 sulle interfacce aggiuntive

Dopo aver installato il nodo, è possibile aggiungere facoltativamente interfacce trunk o di accesso alla VM in vCenter. Ad esempio, potresti voler aggiungere un'interfaccia trunk a un nodo di amministrazione o gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico appartenente a diverse applicazioni o tenant. In alternativa, potresti voler aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (HA).

Le interfacce aggiunte vengono visualizzate nella pagina Interfacce VLAN e nella pagina Gruppi HA in Grid Manager.

- Se si aggiunge un'interfaccia trunk, configurare una o più interfacce VLAN per ogni nuova interfaccia padre. Vedere ["configurare le interfacce VLAN"](#).
- Se si aggiunge un'interfaccia di accesso, è necessario aggiungerla direttamente ai gruppi HA. Vedere ["configurare gruppi ad alta disponibilità"](#).

Volumi di archiviazione per nodi di archiviazione virtuali

È necessario raccogliere le seguenti informazioni per i nodi di archiviazione basati su macchine virtuali:

- Il numero e la dimensione dei volumi di archiviazione (LUN di archiviazione) che intendi aggiungere. Vedi ["Requisiti di archiviazione e prestazioni"](#) .

Informazioni sulla configurazione della griglia

È necessario raccogliere informazioni per configurare la griglia:

- licenza di rete
- Indirizzi IP del server NTP (Network Time Protocol)
- Indirizzi IP del server DNS

Come i nodi della griglia scoprono il nodo di amministrazione primario

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

Per garantire che un nodo della griglia possa accedere al nodo di amministrazione primario, è possibile effettuare una delle seguenti operazioni durante la distribuzione del nodo:

- È possibile utilizzare il parametro ADMIN_IP per immettere manualmente l'indirizzo IP del nodo di amministrazione primario.
- È possibile omettere il parametro ADMIN_IP per fare in modo che il nodo della griglia rilevi automaticamente il valore. La rilevazione automatica è particolarmente utile quando la rete Grid utilizza DHCP per assegnare l'indirizzo IP al nodo di amministrazione primario.

Il rilevamento automatico del nodo di amministrazione primario viene eseguito tramite un sistema di nomi di dominio multicast (mDNS). Quando il nodo di amministrazione primario viene avviato per la prima volta, pubblica il suo indirizzo IP tramite mDNS. Altri nodi sulla stessa subnet possono quindi richiedere l'indirizzo IP e acquisirlo automaticamente. Tuttavia, poiché il traffico IP multicast non è normalmente instradabile tra subnet, i nodi su altre subnet non possono acquisire direttamente l'indirizzo IP del nodo amministrativo primario.

Se si utilizza la rilevazione automatica:



- È necessario includere l'impostazione ADMIN_IP per almeno un nodo della griglia su tutte le subnet a cui il nodo di amministrazione primario non è direttamente collegato. Questo nodo della griglia pubblicherà quindi l'indirizzo IP del nodo di amministrazione primario affinché altri nodi sulla subnet possano individuarlo con mDNS.
- Assicurati che la tua infrastruttura di rete supporti il passaggio del traffico IP multicast all'interno di una subnet.

Distribuisci un nodo StorageGRID come macchina virtuale

Per distribuire ogni nodo della griglia come macchina virtuale, si utilizza VMware vSphere Web Client. Durante la distribuzione, ogni nodo della griglia viene creato e connesso a una o più reti StorageGRID .

Se è necessario distribuire qualsiasi nodo di archiviazione dell'appliance StorageGRID , vedere ["Distribuisci il nodo di archiviazione dell'appliance"](#) .

Facoltativamente, è possibile rimappare le porte del nodo o aumentare le impostazioni della CPU o della memoria per il nodo prima di accenderlo.

Prima di iniziare

- Hai esaminato come ["pianificare e preparare l'installazione"](#) e comprendi i requisiti per software, CPU e RAM, nonché per archiviazione e prestazioni.
- Hai familiarità con VMware vSphere Hypervisor e hai esperienza nella distribuzione 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.

- Hai scaricato ed estratto la versione corretta dell'archivio di installazione StorageGRID per VMware.



Se si distribuisce il nuovo nodo come parte di un'operazione di espansione o ripristino, è necessario utilizzare la versione di StorageGRID attualmente in esecuzione sulla griglia.

- Hai il disco della macchina virtuale StorageGRID(`.vmdk`) file:

`NetApp-SG-version-SHA.vmdk`

- Tu hai il `.ovf` E `.mf` file per ogni tipo di nodo della griglia che stai distribuendo:

Nome del file	Descrizione
<code>vsphere-primary-admin.ovf</code> <code>vsphere-primary-admin.mf</code>	Il file modello e il file manifest per il nodo di amministrazione primario.
<code>vsphere-non-primary-admin.ovf</code> <code>vsphere-non-primary-admin.mf</code>	Il file modello e il file manifest per un nodo di amministrazione non primario.
<code>vsphere-storage.ovf</code> <code>vsphere-storage.mf</code>	Il file modello e il file manifesto per un nodo di archiviazione.
<code>vsphere-gateway.ovf</code> <code>vsphere-gateway.mf</code>	Il file modello e il file manifest per un nodo gateway.

- IL `.vmdk` , `.ovf` , E `.mf` i file sono tutti nella stessa directory.
- Hai un piano per ridurre al minimo i domini di errore. Ad esempio, non dovresti distribuire tutti i nodi gateway su un singolo host vSphere ESXi.



In una distribuzione di produzione, non eseguire più di un nodo di archiviazione su una singola macchina virtuale. Non eseguire più macchine virtuali sullo stesso host ESXi se ciò potrebbe creare un problema di dominio di errore inaccettabile.

- Se si sta distribuendo un nodo come parte di un'operazione di espansione o di ripristino, si ha la ["istruzioni per espandere un sistema StorageGRID"](#) o il ["istruzioni per il recupero e la manutenzione"](#) .

- Se si distribuisce un nodo StorageGRID come macchina virtuale con storage assegnato da un sistema NetApp ONTAP , è stato verificato che il volume non ha un criterio di suddivisione in livelli FabricPool abilitato. Ad esempio, se un nodo StorageGRID è in esecuzione come macchina virtuale su un host VMware, assicurarsi che il volume che supporta il datastore per il nodo non abbia un criterio di suddivisione in livelli FabricPool abilitato. La disattivazione della suddivisione in livelli FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di archiviazione.



Non utilizzare mai FabricPool per riportare i dati relativi a StorageGRID a StorageGRID stesso. Il riordino dei dati StorageGRID su StorageGRID aumenta la complessità operativa e la risoluzione dei problemi.

Informazioni su questo compito

Seguire queste istruzioni per distribuire inizialmente i nodi VMware, aggiungere un nuovo nodo VMware in un'espansione o sostituire un nodo VMware come parte di un'operazione di ripristino. Salvo quanto indicato nei passaggi, la procedura di distribuzione dei nodi è la stessa per tutti i tipi di nodi, inclusi i nodi amministrativi, i nodi di archiviazione e i nodi gateway.

Se si sta installando un nuovo sistema StorageGRID :

- È possibile distribuire i nodi in qualsiasi ordine.
- È necessario assicurarsi che ogni macchina virtuale possa connettersi al nodo di amministrazione primario tramite la rete Grid.
- È necessario distribuire tutti i nodi della griglia prima di configurare la griglia.

Se si sta eseguendo un'operazione di espansione o di ripristino:

- È necessario assicurarsi che la nuova macchina virtuale possa connettersi a tutti gli altri nodi sulla rete Grid.

Se è necessario rimappare una qualsiasi delle porte del nodo, non accendere il nuovo nodo finché la configurazione della rimappatura delle porte non è completa.

Passi

1. Utilizzando VCenter, distribuire un modello OVF.

Se specifichi un URL, punta a una cartella contenente i seguenti file. Altrimenti, seleziona ciascuno di questi file da una directory locale.

```
NetApp-SG-version-SHA.vmdk  
vsphere-node.ovf  
vsphere-node.mf
```

Ad esempio, se questo è il primo nodo che stai distribuendo, usa questi file per distribuire il nodo di amministrazione primario per il tuo sistema StorageGRID :

```
NetApp-SG-version-SHA.vmdk
vsphere-primary-admin.ovf
vsphere-primary-admin.mf
```

2. Fornire un nome per la macchina virtuale.

La prassi standard è quella di utilizzare lo stesso nome sia per la macchina virtuale che per il nodo della griglia.

3. Posizionare la macchina virtuale nella vApp o nel pool di risorse appropriato.

4. Se si sta distribuendo il nodo di amministrazione primario, leggere e accettare il Contratto di licenza con l'utente finale.

A seconda della versione di vCenter in uso, l'ordine dei passaggi per accettare il Contratto di licenza con l'utente finale, specificare il nome della macchina virtuale e selezionare un datastore varierà.

5. Selezionare l'archiviazione per la macchina virtuale.

Se si sta distribuendo un nodo come parte di un'operazione di ripristino, eseguire le istruzioni [infase di recupero dell'archiviazione](#) per aggiungere nuovi dischi virtuali, ricollegare i dischi rigidi virtuali dal nodo della griglia non riuscito o entrambe le cose.

Quando si distribuisce un nodo di archiviazione, utilizzare 3 o più volumi di archiviazione, ciascuno dei quali deve avere una dimensione pari o superiore a 4 TB. È necessario assegnare almeno 4 TB al volume 0.



Il file .ovf del nodo di archiviazione definisce diversi VMDK per l'archiviazione. A meno che questi VMDK non soddisfino i requisiti di archiviazione, è necessario rimuoverli e assegnare VMDK o RDM appropriati per l'archiviazione prima di accendere il nodo. I VMDK sono più comunemente utilizzati negli ambienti VMware e sono più facili da gestire, mentre gli RDM potrebbero offrire prestazioni migliori per carichi di lavoro che utilizzano dimensioni di oggetti maggiori (ad esempio, superiori a 100 MB).



Alcune installazioni StorageGRID potrebbero utilizzare volumi di archiviazione più grandi e più attivi rispetto ai tipici carichi di lavoro virtualizzati. Potrebbe essere necessario regolare alcuni parametri dell'hypervisor, come ad esempio `MaxAddressableSpaceTB`, per ottenere prestazioni ottimali. Se riscontri scarse prestazioni, contatta la risorsa di supporto alla virtualizzazione per determinare se il tuo ambiente potrebbe trarre vantaggio dall'ottimizzazione della configurazione specifica del carico di lavoro.

6. Seleziona le reti.

Determina quali reti StorageGRID utilizzerà il nodo selezionando una rete di destinazione per ciascuna rete di origine.

- È richiesta la rete Grid. È necessario selezionare una rete di destinazione nell'ambiente vSphere. + La rete Grid viene utilizzata per tutto il traffico StorageGRID interno. Fornisce connettività tra tutti i nodi della griglia, in tutti i siti e le subnet. Tutti i nodi della rete Grid devono essere in grado di comunicare con tutti gli altri nodi.
- Se si utilizza la rete di amministrazione, selezionare una rete di destinazione diversa nell'ambiente vSphere. Se non si utilizza la rete di amministrazione, selezionare la stessa destinazione selezionata

per la rete Grid.

- Se si utilizza la rete client, selezionare una rete di destinazione diversa nell'ambiente vSphere. Se non si utilizza la rete client, selezionare la stessa destinazione selezionata per la rete Grid.
- Se si utilizza una rete Admin o Client, i nodi non devono trovarsi sulla stessa rete Admin o Client.

7. Per **Personalizza modello**, configurare le proprietà richieste del nodo StorageGRID .

a. Inserisci il **Nome del nodo**.



Se si sta ripristinando un nodo della griglia, 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 della VM o all'API di installazione StorageGRID , oppure 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 che un nodo è stato aggiunto alla griglia, è possibile accedervi utilizzando "[password della console del nodo](#)", che è elencato nel `Passwords.txt` file 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:** come password di installazione temporanea viene utilizzata una password personalizzata.
 - **Disabilita password:** non verrà utilizzata alcuna password di installazione temporanea. Se è necessario accedere alla macchina virtuale per risolvere i problemi di installazione, vedere "[Risolvere i problemi di installazione](#)".
- c. Se hai selezionato **Usa password personalizzata**, specifica la password di installazione temporanea che desideri utilizzare nel campo **Password personalizzata**.
- d. Nella sezione **Rete Grid (eth0)**, selezionare STATICO o DHCP per la **Configurazione IP della rete Grid**.
- Se si seleziona STATICO, immettere **IP di rete griglia**, **Maschera di rete griglia**, **Gateway di rete griglia** e **MTU di rete griglia**.
 - Se si seleziona DHCP, **IP di rete griglia**, **Maschera di rete griglia** e **Gateway di rete griglia** vengono assegnati automaticamente.
- e. Nel campo **IP amministratore primario**, immettere l'indirizzo IP del nodo amministratore primario per la rete Grid.



Questo passaggio non si applica se il nodo che si sta distribuendo è il nodo di amministrazione primario.

Se si omette l'indirizzo IP del nodo di amministrazione primario, 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 subnet. Tuttavia, si consiglia di impostare qui l'indirizzo IP del nodo di amministrazione primario.

a. Nella sezione **Rete amministrativa (eth1)**, selezionare STATICO, DHCP o DISABILITATO per la **configurazione IP della rete amministrativa**.

- Se non si desidera utilizzare la rete di amministrazione, selezionare **DISABILITATO** e immettere **0.0.0.0** come IP della rete di amministrazione. Puoi lasciare vuoti gli altri campi.
- Se si seleziona **STATICO**, immettere **IP rete amministratore**, **Maschera rete amministratore**, **Gateway rete amministratore** e **MTU rete amministratore**.
- Se si seleziona **STATICO**, immettere l'**Elenco subnet esterne della rete amministrativa**. È necessario configurare anche un gateway.
- Se si seleziona **DHCP**, **IP di rete amministratore**, **Maschera di rete amministratore** e **Gateway di rete amministratore** vengono assegnati automaticamente.

b. Nella sezione **Rete client (eth2)**, selezionare **STATICO**, **DHCP** o **DISABILITATO** per la **Configurazione IP della rete client**.

- Se non si desidera utilizzare la rete client, selezionare **DISABILITATO** e immettere **0.0.0.0** come IP della rete client. Puoi lasciare vuoti gli altri campi.
- Se si seleziona **STATICO**, immettere **IP di rete client**, **Maschera di rete client**, **Gateway di rete client** e **MTU di rete client**.
- Se si seleziona **DHCP**, **IP di rete client**, **Maschera di rete client** e **Gateway di rete client** vengono assegnati automaticamente.

8. Rivedere la configurazione della macchina virtuale e apportare le modifiche necessarie.

9. Quando sei pronto per completare, seleziona **Fine** per avviare il caricamento della macchina virtuale.

10. Se hai distribuito questo nodo come parte di un'operazione di ripristino e non si tratta di un ripristino del nodo completo, esegui questi passaggi al termine della distribuzione:

- Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Modifica impostazioni**.
- Selezionare ciascun disco rigido virtuale predefinito designato per l'archiviazione e selezionare **Rimuovi**.
- A seconda delle circostanze del ripristino dei dati, aggiungi nuovi dischi virtuali in base ai requisiti di archiviazione, ricollega eventuali dischi rigidi virtuali conservati dal nodo griglia non riuscito rimosso in precedenza, oppure esegui entrambe le operazioni.

Si prega di notare le seguenti importanti linee guida:

- Se si aggiungono nuovi dischi, è necessario utilizzare lo stesso tipo di dispositivo di archiviazione utilizzato prima del ripristino del nodo.
- Il file **.ovf** del nodo di archiviazione definisce diversi **VMDK** per l'archiviazione. A meno che questi **VMDK** non soddisfino i requisiti di archiviazione, è necessario rimuoverli e assegnare **VMDK** o **RDM** appropriati per l'archiviazione prima di accendere il nodo. I **VMDK** sono più comunemente utilizzati negli ambienti **VMware** e sono più facili da gestire, mentre gli **RDM** potrebbero offrire prestazioni migliori per carichi di lavoro che utilizzano dimensioni di oggetti maggiori (ad esempio, superiori a 100 MB).

11. Se è necessario rimappare le porte utilizzate da questo nodo, seguire questi passaggi.

Potrebbe essere necessario rimappare una porta se i criteri di rete aziendali limitano l'accesso a una o più porte utilizzate da **StorageGRID**. Vedi il ["linee guida per il networking"](#) per le porte utilizzate da **StorageGRID**.



Non rimappare le porte utilizzate negli endpoint del bilanciatore del carico.

a. Selezionare la nuova VM.

- b. Dalla scheda Configura, seleziona **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 in modo simmetrico sia le comunicazioni in entrata che quelle in uscita per una porta, selezionare **PORT_REMAP**.



Se è impostato solo **PORT_REMAP**, la mappatura specificata si applica sia alle comunicazioni in entrata che a quelle in uscita. Se viene specificato anche **PORT_REMAP_INBOUND**, **PORT_REMAP** si applica solo alle comunicazioni in uscita.

- i. Selezionare **Imposta valore**.
- ii. Inserisci la mappatura delle porte:

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

<network type> è griglia, amministratore 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
```

È possibile rimappare più porte utilizzando un elenco separato da virgole.

Per esempio:

```
client/tcp/18082/443, client/tcp/18083/80
```

- 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. Selezionare **Imposta valore**.
- ii. Inserisci la mappatura delle porte:

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>
```

<network type> è griglia, amministratore 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 sulla porta 22 dal nodo della griglia, immettere quanto segue:

```
client/tcp/3022/22
```

È possibile rimappare più porte in ingresso utilizzando un elenco separato da virgole.

Per esempio:

grid/tcp/3022/22, admin/tcp/3022/22

i. Seleziona **OK**

12. Se si desidera aumentare la CPU o la memoria del nodo rispetto alle impostazioni predefinite:

a. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Modifica impostazioni**.

b. Modificare il numero di CPU o la quantità di memoria in base alle esigenze.

Impostare la **Riserva di memoria** sulla stessa dimensione della **Memoria** assegnata alla macchina virtuale.

c. Selezionare **OK**.

13. Accendere la macchina virtuale.

Dopo aver finito

Se hai distribuito questo nodo come parte di una procedura di espansione o ripristino, torna a quelle istruzioni per completare la procedura.

Configurare la griglia e completare l'installazione (VMware)

Vai al Grid Manager

Utilizzare Grid Manager per definire tutte le informazioni necessarie per configurare il sistema StorageGRID .

Prima di iniziare

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

Passi

1. Apri il tuo browser web e vai su:

`https://primary_admin_node_ip`

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

`https://primary_admin_node_ip:8443`

È possibile utilizzare l'indirizzo IP per l'IP del nodo di amministrazione primario sulla rete Grid o sulla rete di amministrazione, a seconda della configurazione di rete. Potrebbe essere necessario utilizzare l'opzione di sicurezza/avanzata del browser per accedere a un certificato non attendibile.

2. Gestisci una password di installazione temporanea secondo necessità:

- Se è già stata impostata una password utilizzando uno di questi metodi, immetterla per procedere.
 - Un utente ha impostato la password durante l'accesso al programma di installazione in precedenza
 - La password SSH/console è stata importata automaticamente dalle proprietà OVF
- Se non è stata impostata una password, impostarne una facoltativamente per proteggere il programma di installazione StorageGRID .

3. Selezionare ***Installa un sistema StorageGRID ***.

Viene visualizzata la pagina utilizzata per configurare una griglia StorageGRID .

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, a blue header bar contains the text "NetApp® StorageGRID®" and a "Help" link with a dropdown arrow. Below the header is a horizontal progress bar with eight steps, each represented by a numbered circle: 1 (License), 2 (Sites), 3 (Grid Network), 4 (Grid Nodes), 5 (NTP), 6 (DNS), 7 (Passwords), and 8 (Summary). The "License" step is currently selected and highlighted. Below the progress bar, the section is titled "License" with the instruction: "Enter a grid name and upload the license file provided by NetApp for your StorageGRID system." There are two input fields: "Grid Name" with an empty text box, and "License File" with a "Browse" button.

Specificare le informazioni sulla licenza StorageGRID

È necessario specificare il nome del sistema StorageGRID e caricare il file di licenza fornito da NetApp.

Passi

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 Nodi.

2. Selezionare **Sfogliare**, individuare il file di licenza NetApp(*NLF-unique-id.txt*) e seleziona **Apri**.

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



L'archivio di installazione StorageGRID include una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto. Dopo l'installazione è possibile effettuare l'aggiornamento a una licenza che offra supporto.

This screenshot shows the same "License" step of the NetApp StorageGRID installation wizard, but with the fields filled out. The "Grid Name" field now contains the text "StorageGRID". The "License File" field has a "Browse" button and the filename "NLF-959007-Internal.txt" displayed next to it. Below these fields, a new field labeled "License Serial Number" contains the value "959007". The progress bar at the top remains the same, with step 1 highlighted.

3. Selezionare **Avanti**.

Aggiungi siti

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

Passi

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

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

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Sites

In a single-site deployment, infrastructure and operations are centralized in one site.

In a multi-site deployment, infrastructure can be distributed asymmetrically across sites, and proportional to the needs of each site. Typically, sites are located in geographically different locations. Having multiple sites also allows the use of distributed replication and erasure coding for increased availability and resiliency.

Site Name 1 Raleigh x

Site Name 2 Atlanta + x

3. Fare clic su **Avanti**.

Specificare le subnet della rete Grid

È necessario specificare le subnet utilizzate nella rete Grid.

Informazioni su questo compito

Le voci di subnet includono le subnet per la rete Grid per ciascun sito nel sistema StorageGRID , insieme a tutte le subnet che devono essere raggiungibili tramite la rete Grid.

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

Passi

1. Specificare l'indirizzo di rete CIDR per almeno una rete Grid nella casella di testo **Subnet 1**.
2. Fare clic sul segno più accanto all'ultima voce per aggiungere un'ulteriore voce di rete. È necessario specificare tutte le subnet per tutti i siti nella rete Grid.

- Se hai già distribuito almeno un nodo, fai clic su **Scopri subnet di Grid Networks** per popolare automaticamente l'elenco delle subnet di Grid Network con le subnet segnalate dai nodi di Grid che si sono registrati con Grid Manager.
- È necessario aggiungere manualmente eventuali subnet per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway Grid Network.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 **Grid Network** 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1 +

3. Fare clic su **Avanti**.

Approva i nodi della griglia in sospeso

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

Prima di iniziare

Sono stati distribuiti tutti i nodi griglia virtuali e degli appliance StorageGRID .



È più efficiente eseguire un'unica installazione di tutti i nodi, piuttosto che installare alcuni nodi ora e altri in seguito.

Passi

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



Se un nodo della griglia risulta mancante, verificare che sia stato distribuito correttamente e che abbia impostato l'IP di rete della griglia corretto del nodo di amministrazione primario per ADMIN_IP.

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



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve		✖ Remove		Search		
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit		Reset		✖ Remove		Search	
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address	
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21	
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21	
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21	
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21	
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21	

3. Fare clic su **Approva**.

4. Nelle Impostazioni generali, modificare le impostazioni per le seguenti proprietà, se necessario:

- **Sito:** il nome di sistema del sito per questo nodo della griglia.
- **Nome:** il nome di sistema per il nodo. Il nome predefinito è quello specificato durante la configurazione del nodo.

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



Per un nodo VMware, è possibile modificare il nome qui, ma questa azione non modificherà il nome della macchina virtuale in vSphere.

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



Assicurarsi che almeno due nodi in ogni sito possano accedere ad almeno quattro fonti NTP esterne. Se solo un nodo in un sito riesce a raggiungere le sorgenti NTP, si verificheranno problemi di temporizzazione se quel nodo non funziona. Inoltre, la designazione di due nodi per sito come fonti NTP primarie garantisce una temporizzazione accurata se un sito è isolato dal resto della griglia.

- **Tipo di archiviazione** (solo nodi di archiviazione): specifica che un nuovo nodo di archiviazione deve essere utilizzato esclusivamente per i dati, solo per i metadati o per entrambi. Le opzioni sono **Dati e metadati** ("combinati"), **Solo dati** e **Solo metadati**.



Vedere "[Tipi di nodi di archiviazione](#)" per informazioni sui requisiti per questi tipi di nodo.

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

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

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



Il gateway è necessario se sono presenti più subnet della griglia.



Se hai selezionato DHCP per la configurazione della rete Grid e modifichi il valore qui, il nuovo valore verrà configurato come indirizzo statico sul nodo. È necessario assicurarsi che l'indirizzo IP configurato non sia compreso in un pool di indirizzi DHCP.

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

Immettere le subnet di destinazione delle rotte in uscita da questa interfaccia nella casella di testo **Subnet (CIDR)**. Se sono presenti più subnet di amministrazione, è necessario il gateway di amministrazione.



Se hai selezionato DHCP per la configurazione della rete di amministrazione e modifichi il valore qui, il nuovo valore verrà configurato come indirizzo statico sul nodo. È necessario assicurarsi che l'indirizzo IP configurato non sia compreso in un pool di indirizzi DHCP.

Appliance: per un'appliance StorageGRID, se la rete di amministrazione non è stata configurata durante l'installazione iniziale tramite StorageGRID Appliance Installer, non può essere configurata in questa finestra di dialogo Grid Manager. Invece, devi seguire questi passaggi:

- a. Riavviare l'appliance: nell'Appliance Installer, selezionare **Avanzate > Riavvia**.

Il riavvio può richiedere diversi minuti.

- b. Selezionare **Configura rete > Configurazione collegamento** e abilitare le reti appropriate.
- c. Selezionare **Configura rete > Configurazione IP** e configurare le reti abilitate.
- d. Torna alla Home page e clicca su **Avvia installazione**.

- e. In Grid Manager: se il nodo è elencato nella tabella Nodi approvati, rimuoverlo.
- f. Rimuovere il nodo dalla tabella Nodi in sospeso.
- g. Attendi che il nodo riappaia nell'elenco dei nodi in sospeso.
- h. Verificare di poter configurare le reti appropriate. Dovrebbero già essere compilati con le informazioni fornite nella pagina Configurazione IP dell'Appliance Installer.

Per ulteriori informazioni, vedere il ["Avvio rapido per l'installazione dell'hardware"](#) per trovare le istruzioni per il tuo elettrodomestico.

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



Se hai selezionato DHCP per la configurazione della rete client e modifichi il valore qui, il nuovo valore verrà configurato come indirizzo statico sul nodo. È necessario assicurarsi che l'indirizzo IP configurato non sia compreso in un pool di indirizzi DHCP.

Appliance: per un'appliance StorageGRID , se la rete client non è stata configurata durante l'installazione iniziale tramite StorageGRID Appliance Installer, non può essere configurata in questa finestra di dialogo Grid Manager. Invece, devi seguire questi passaggi:

- a. Riavviare l'appliance: nell'Appliance Installer, selezionare **Avanzate > Riavvia**.

Il riavvio può richiedere diversi minuti.

- b. Selezionare **Configura rete > Configurazione collegamento** e abilitare le reti appropriate.
- c. Selezionare **Configura rete > Configurazione IP** e configurare le reti abilitate.
- d. Torna alla Home page e clicca su **Avvia installazione**.
- e. In Grid Manager: se il nodo è elencato nella tabella Nodi approvati, rimuoverlo.
- f. Rimuovere il nodo dalla tabella Nodi in sospeso.
- g. Attendi che il nodo riappaia nell'elenco dei nodi in sospeso.
- h. Verificare di poter configurare le reti appropriate. Dovrebbero già essere compilati con le informazioni fornite nella pagina Configurazione IP dell'Appliance Installer.

Per ulteriori informazioni, vedere il ["Avvio rapido per l'installazione dell'hardware"](#) per trovare le istruzioni per il tuo elettrodomestico.

8. Fare clic su **Salva**.

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



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

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

Devi approvare tutti i nodi che desideri nella griglia. Tuttavia, puoi 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 della griglia, fare clic su **Avanti**.

Specificare le informazioni del server Network Time Protocol

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

Informazioni su questo compito

È necessario specificare gli indirizzi IPv4 per i server NTP.

È necessario specificare server NTP esterni. I server NTP specificati devono utilizzare il protocollo NTP.

Per evitare problemi di deriva temporale, è necessario specificare quattro riferimenti al server NTP di Stratum 3 o superiore.



Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Ora di Windows (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio orario delle versioni precedenti di Windows non è sufficientemente preciso e non è supportato da Microsoft per l'uso in ambienti ad alta precisione, come StorageGRID.

"Limite di supporto per configurare il servizio Ora di Windows per ambienti ad alta precisione"

I server NTP esterni vengono utilizzati dai nodi a cui sono stati precedentemente assegnati ruoli NTP primari.



Assicurarsi che almeno due nodi in ogni sito possano accedere ad almeno quattro fonti NTP esterne. Se solo un nodo in un sito riesce a raggiungere le sorgenti NTP, si verificheranno problemi di temporizzazione se quel nodo non funziona. Inoltre, la designazione di due nodi per sito come fonti NTP primarie garantisce una temporizzazione accurata se un sito è isolato dal resto della griglia.

Eseguire controlli aggiuntivi per VMware, ad esempio assicurandosi che l'hypervisor utilizzi la stessa origine NTP della macchina virtuale e utilizzando VMTools per disabilitare la sincronizzazione oraria tra l'hypervisor e le macchine virtuali StorageGRID .

Passi

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 ulteriori voci del server.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1

10.60.248.183

Server 2

10.227.204.142

Server 3

10.235.48.111

Server 4

0.0.0.0

+

3. Selezionare **Avanti**.

Specificare le informazioni del server DNS

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

Informazioni su questo compito

Specificando ["Informazioni sul server DNS"](#) consente di utilizzare nomi host FQDN (Fully Qualified Domain Name) anziché indirizzi IP per le notifiche e-mail e AutoSupport.

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

Se possibile, utilizzare server DNS a cui ogni sito possa accedere localmente per garantire che un sito isolato possa risolvere gli FQDN per le destinazioni esterne.

Passi

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 ulteriori voci del server.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is visible. It contains a text box for "Server 1" with the IP address "10.224.223.130" and a red "X" icon. Below that is a text box for "Server 2" with the IP address "10.224.223.136" and a red "X" icon. To the left of the text boxes are labels "Server 1" and "Server 2".

La procedura migliore è specificare almeno due server DNS. È possibile specificare fino a sei server DNS.

3. Selezionare **Avanti**.

Specificare le password del sistema StorageGRID

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

Informazioni su questo compito

Utilizzare la pagina Installa password per specificare la passphrase di provisioning e la password dell'utente root per la 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 conservare la passphrase di provisioning in un luogo sicuro.
- È possibile modificare la passphrase di provisioning da Grid Manager se si dispone di quella attuale.
- La password dell'utente root per la gestione della griglia può essere modificata tramite Grid Manager.
- Le password della console della riga di comando e SSH generate casualmente vengono memorizzate nel `Passwords.txt` file nel pacchetto di ripristino.

Passi

1. In **Provisioning Passphrase**, immettere la passphrase di provisioning che sarà necessaria per apportare modifiche alla topologia della griglia del sistema StorageGRID .

Conservare la passphrase di provisioning in un luogo sicuro.



Se dopo il completamento dell'installazione si desidera modificare la passphrase di provisioning in un secondo momento, è possibile utilizzare Grid Manager. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.

2. In **Conferma passphrase di provisioning**, reinserisci la passphrase di provisioning per confermarla.
3. In **Password utente root di Grid Management**, immettere la password da utilizzare per accedere a Grid Manager come utente "root".

Conservare la password in un luogo sicuro.

4. In **Conferma password utente root**, reinserisci la password di Grid Manager per confermarla.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning Passphrase	
Confirm Provisioning Passphrase	
Grid Management Root User Password	
Confirm Root User Password	

☒ Create random command line passwords.

5. Se si installa una griglia a scopo dimostrativo o di prova del concetto, è possibile deselezionare la casella

di controllo **Crea password casuali per la riga di comando.**

Per le distribuzioni di produzione, per motivi di sicurezza è sempre opportuno utilizzare password casuali. Deseleziona **Crea password casuali per la riga di comando** solo per le griglie demo se vuoi utilizzare password predefinite per accedere ai nodi della griglia dalla riga di comando utilizzando l'account "root" o "admin".



Ti verrà chiesto di scaricare il file del pacchetto di ripristino(`sgws-recovery-package-id-revision.zip`) dopo aver cliccato su **Installa** nella pagina Riepilogo. Devi ["scarica questo file"](#) per completare l'installazione. Le password necessarie per accedere al sistema sono memorizzate nel `Passwords.txt` file, contenuto nel file Recovery Package.

6. Fare clic su **Avanti**.

Rivedi la tua configurazione e completa l'installazione

È necessario rivedere attentamente le informazioni di configurazione immesse per garantire che l'installazione venga completata correttamente.

Passi

1. Visualizza la pagina **Riepilogo**.

NetApp® StorageGRID®

Help ▾

Install

1

2

3

4

5

6

7

8

License

Sites

Grid Network

Grid Nodes

NTP

DNS

Passwords

Summary

Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name

Grid1

Modify License

Passwords

Auto-generated random command line passwords

Modify Passwords

Networking

NTP

10.60.248.183 10.227.204.142 10.235.48.111

Modify NTP

DNS

10.224.223.130 10.224.223.136

Modify DNS

Grid Network

172.16.0.0/21

Modify Grid Network

Topology

Topology

Atlanta

Modify Sites

Modify Grid Nodes

Raleigh

dc1-adm1

dc1-g1

dc1-s1

dc1-s2

dc1-s3

NetApp-SGA

2. Verificare che tutte le informazioni sulla configurazione della griglia siano corrette. Utilizzare i link Modifica nella pagina Riepilogo per tornare indietro e correggere eventuali errori.

259

3. Fare clic su **Installa**.



Se un nodo è configurato per utilizzare la rete client, il gateway predefinito per quel nodo passa dalla rete Grid alla rete client quando si fa clic su **Installa**. Se si perde la connettività, è necessario assicurarsi di accedere al nodo di amministrazione primario tramite una subnet accessibile. Vedere "[Linee guida per il networking](#)" per i dettagli.

4. Fare clic su **Scarica pacchetto di ripristino**.

Quando l'installazione procede fino al punto in cui viene definita la topologia della griglia, viene richiesto di scaricare il file del pacchetto di ripristino (.zip) e conferma di poter accedere correttamente al contenuto di questo file. È necessario scaricare il file Recovery Package per poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi della griglia. L'installazione continua in background, ma non sarà possibile completarla e accedere al sistema StorageGRID finché non si scarica e si verifica questo file.

5. Verificare che sia possibile estrarre il contenuto del .zip file e salvarlo in due posizioni sicure, protette 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. Seleziona la casella di controllo **Ho scaricato e verificato correttamente il file del pacchetto di ripristino** e fai 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.

Installation Status

If necessary, you may [Download the Recovery Package](#) file again.

							Search	
Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21			Starting services	
dc1-g1		Site1		172.16.4.216/21			Complete	
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed	

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

7. Sign in a Grid Manager utilizzando l'utente "root" e la password specificati durante l'installazione.

Linee guida post-installazione

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

- Se è stato utilizzato DHCP per assegnare gli indirizzi IP, configurare una prenotazione DHCP per ciascun indirizzo IP sulle reti utilizzate.

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



I nodi si riavviano quando la configurazione della rete Grid viene modificata da DHCP, il che può causare interruzioni se una modifica DHCP interessa più nodi contemporaneamente.

- È necessario utilizzare le procedure di modifica IP se si desidera modificare gli indirizzi IP, le maschere di sottorete e i gateway predefiniti per un nodo della griglia. Vedere "[Configurare gli indirizzi IP](#)".
- Se si apportano modifiche alla configurazione di rete, tra cui 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 apportate alla rete, potrebbe essere necessario ristabilire queste connessioni.

Installazione REST API

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

L'API utilizza la piattaforma API open source Swagger per fornire la documentazione API. Swagger consente sia agli sviluppatori sia ai non sviluppatori di interagire con l'API tramite un'interfaccia utente che illustra come l'API risponde a parametri e opzioni. Questa documentazione presuppone che tu abbia familiarità con le tecnologie web standard e con il formato dati JSON.



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

Ogni comando API REST include l'URL dell'API, un'azione HTTP, eventuali parametri URL obbligatori o facoltativi e una risposta API prevista.

API di installazione StorageGRID

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

Per accedere alla documentazione API, vai alla pagina web di installazione sul nodo di amministrazione principale e seleziona **Aiuto > Documentazione API** dalla barra dei menu.

L'API di installazione StorageGRID include le seguenti sezioni:

- **config** — Operazioni relative alla versione del prodotto e alle versioni dell'API. È possibile elencare la versione del prodotto e le principali versioni dell'API supportate da tale versione.
- **grid** — Operazioni di configurazione a livello di griglia. È possibile ottenere e aggiornare le impostazioni della griglia, inclusi i dettagli della griglia, le subnet della rete Grid, 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 della griglia, eliminare un nodo della griglia, configurare un nodo della griglia, visualizzare un nodo della griglia e reimpostare la configurazione di un nodo della griglia.
- **provision** — Operazioni di provisioning. È possibile avviare l'operazione di provisioning e visualizzarne lo stato.
- **recupero** — Operazioni di recupero del nodo amministrativo primario. È possibile reimpostare 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.
- **siti** — Operazioni di configurazione a livello di sito. È possibile creare, visualizzare, eliminare e modificare un sito.
- **temporary-password** — Operazioni sulla password temporanea per proteggere mgmt-api durante l'installazione.

Dove andare dopo

Dopo aver completato l'installazione, eseguire le attività di integrazione e configurazione richieste. È possibile eseguire le attività facoltative in base alle proprie esigenze.

Compiti richiesti

- Configurare VMware vSphere Hypervisor per il riavvio automatico.

È necessario configurare l'hypervisor in modo che riavvii 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 maggiori dettagli, consultare la documentazione di VMware vSphere Hypervisor.

- ["Crea un account inquilino"](#) per il protocollo client S3 che verrà utilizzato per archiviare gli oggetti sul sistema StorageGRID .
- ["Controllo dell'accesso al sistema"](#) configurando gruppi e account utente. Facoltativamente, puoi ["configurare una fonte di identità federata"](#) (ad esempio Active Directory o OpenLDAP), in modo da poter importare gruppi di amministrazione e utenti. Oppure puoi ["creare gruppi e utenti locali"](#) .
- Integrare e testare il ["S3 API"](#) applicazioni client che utilizzerai per caricare oggetti sul tuo sistema StorageGRID .
- ["Configurare le regole di gestione del ciclo di vita delle informazioni \(ILM\) e la politica ILM"](#) che si desidera utilizzare per proteggere i dati degli oggetti.
- Se l'installazione include nodi di archiviazione dell'appliance, utilizzare SANtricity OS per completare le seguenti attività:
 - Connettersi a ciascun dispositivo StorageGRID .
 - Verificare la ricezione dei dati AutoSupport .

Vedere ["Configurare l'hardware"](#) .

- Rivedi e segui il ["Linee guida per il rafforzamento del sistema StorageGRID"](#) per eliminare i rischi per la sicurezza.
- ["Configurare le notifiche e-mail per gli avvisi di sistema"](#) .

Attività facoltative

- ["Aggiorna gli indirizzi IP dei nodi della griglia"](#) se sono cambiati da quando hai pianificato la distribuzione e generato il pacchetto di ripristino.
- ["Configurare la crittografia dell'archiviazione"](#), se necessario.
- ["Configurare la compressione dell'archiviazione"](#) per ridurre le dimensioni degli oggetti memorizzati, se necessario.
- ["Configurare le interfacce VLAN"](#) per isolare e partizionare il traffico di rete, se necessario.
- ["Configurare gruppi ad alta disponibilità"](#) per migliorare la disponibilità della connessione per i client Grid

Manager, Tenant Manager e S3, se necessario.

- ["Configurare gli endpoint del bilanciatore del carico"](#) per la connettività client S3, se necessario.

Risolvere i problemi di installazione

Se si verificano problemi durante l'installazione del sistema StorageGRID, è possibile accedere ai file di registro dell'installazione.

Di seguito sono riportati i principali file di registro dell'installazione, di cui il supporto tecnico potrebbe aver bisogno per risolvere i problemi.

- `/var/local/log/install.log` (presente 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 ["Riferimento ai file di registro"](#).

Se hai bisogno di ulteriore assistenza, contatta ["Supporto NetApp"](#).

La prenotazione delle risorse della macchina virtuale richiede una regolazione

I file OVF includono una riserva di risorse progettata per garantire che ogni nodo della griglia disponga di RAM e CPU sufficienti per funzionare in modo efficiente. Se si creano macchine virtuali distribuendo questi file OVF su VMware e il numero predefinito di risorse non è disponibile, le macchine virtuali non si avvieranno.

Informazioni su questo compito

Se si è certi che l'host della macchina virtuale disponga di risorse sufficienti per ciascun nodo della griglia, regolare manualmente le risorse assegnate a ciascuna macchina virtuale, quindi provare ad avviare le macchine virtuali.

Passi

1. Nella struttura client VMware vSphere Hypervisor, selezionare la macchina virtuale non avviata.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Modifica impostazioni**.
3. Dalla finestra Proprietà macchine virtuali, selezionare la scheda **Risorse**.
4. Regola le risorse assegnate alla macchina virtuale:
 - a. Selezionare **CPU**, quindi utilizzare il cursore Prenotazione per regolare i MHz riservati per questa macchina virtuale.
 - b. Selezionare **Memoria**, quindi utilizzare il cursore Prenotazione per regolare i MB riservati per questa macchina virtuale.
5. Fare clic su **OK**.
6. Ripetere l'operazione, se necessario, per le altre macchine virtuali ospitate sullo stesso host VM.

La password di installazione temporanea è stata disabilitata

Quando si distribuisce un nodo VMware, è possibile specificare facoltativamente una password di installazione temporanea. È necessario disporre di questa password per accedere alla console della VM oppure utilizzare SSH prima che il nuovo nodo si unisca alla griglia.

Se hai scelto di disabilitare la password di installazione temporanea, dovrai eseguire ulteriori passaggi per

risolvere i problemi di installazione.

Puoi procedere in uno dei seguenti modi:

- Ridistribuisci la VM, ma specifica 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. Spegnerla la macchina virtuale.
 - b. Vai a **VM**, seleziona la scheda **Configura** e seleziona **Opzioni vApp**.
 - c. Specificare il tipo di password di installazione temporanea da impostare:
 - Selezionare **CUSTOM_TEMPORARY_PASSWORD** per impostare una password temporanea personalizzata.
 - Selezionare **TEMPORARY_PASSWORD_TYPE** per utilizzare il nome del nodo come password temporanea.
 - d. Selezionare **Imposta valore**.
 - e. Imposta la password temporanea:
 - Sostituisci **CUSTOM_TEMPORARY_PASSWORD** con un valore di password personalizzato.
 - Aggiorna **TEMPORARY_PASSWORD_TYPE** con il valore **Usa nome nodo**.
 - f. Riavviare la macchina virtuale per applicare la nuova password.

Aggiorna il software StorageGRID

Aggiorna il software StorageGRID

Utilizzare queste istruzioni per aggiornare un sistema StorageGRID a una nuova versione.

Quando esegui l'aggiornamento, tutti i nodi del tuo sistema StorageGRID vengono aggiornati.

Prima di iniziare

Esamina questi argomenti per scoprire le nuove funzionalità e i miglioramenti di StorageGRID 11.9, determinare se alcune funzionalità sono state deprecate o rimosse e scoprire le modifiche apportate alle API StorageGRID .

- ["Novità di StorageGRID 11.9"](#)
- ["Funzionalità rimosse o deprecate"](#)
- ["Modifiche all'API di gestione della griglia"](#)
- ["Modifiche all'API di gestione degli inquilini"](#)

Novità di StorageGRID 11.9

Questa versione di StorageGRID introduce le seguenti funzionalità e modifiche funzionali.

Scalabilità

Nodi di archiviazione solo dati

Per consentire un ridimensionamento più granulare, ora puoi installare ["nodi di archiviazione solo dati"](#) . Laddove l'elaborazione dei metadati non è critica, è possibile ottimizzare l'infrastruttura in modo economicamente vantaggioso. Questa flessibilità aiuta ad adattarsi a carichi di lavoro e modelli di crescita variabili.

Miglioramenti del Cloud Storage Pool

Ruoli IAM ovunque

StorageGRID ora supporta le credenziali a breve termine utilizzando ["Ruoli IAM ovunque in Amazon S3 per pool di archiviazione cloud"](#) .

L'utilizzo di credenziali a lungo termine per accedere ai bucket S3 comporta rischi per la sicurezza se tali credenziali vengono compromesse. Le credenziali a breve termine hanno una durata limitata, il che riduce il rischio di accessi non autorizzati.

Bucket di blocco degli oggetti S3

Ora puoi ["configurare un Cloud Storage Pool utilizzando un endpoint Amazon S3"](#) . S3 Object Lock aiuta a prevenire l'eliminazione accidentale o dolosa degli oggetti. Se si suddividono i dati da StorageGRID ad Amazon S3, l'abilitazione del blocco degli oggetti su entrambi i sistemi migliora la protezione dei dati durante l'intero ciclo di vita dei dati.

Multi-tenancy

Limiti del bucket

Di ["impostazione dei limiti sui bucket S3"](#) , è possibile impedire agli inquilini di monopolizzare la capacità. Inoltre, una crescita incontrollata può comportare costi imprevisti. Avendo dei limiti definiti, è possibile stimare meglio le spese di deposito degli inquilini.

5.000 bucket per inquilino

Per migliorare la scalabilità, StorageGRID ora supporta fino a ["5.000 bucket S3 per tenant"](#) . Ogni griglia può avere un massimo di 100.000 bucket.

Per supportare 5.000 bucket, ogni nodo di archiviazione nella griglia deve disporre di almeno 64 GB di RAM.

Miglioramenti al blocco degli oggetti S3

Le funzionalità di configurazione per tenant garantiscono il giusto equilibrio tra flessibilità e sicurezza dei dati. Ora puoi configurare le impostazioni di conservazione per tenant per:

- Consenti o non consenti la modalità di conformità
- Imposta un periodo massimo di conservazione

Fare riferimento a:

- ["Gestisci gli oggetti con S3 Object Lock"](#)
- ["Come gli amministratori della griglia controllano la conservazione degli oggetti"](#)

- ["Crea un account inquilino"](#)

Compatibilità S3

checksum x-amz-checksum-sha256

- L'API REST S3 ora fornisce supporto per `x-amz-checksum-sha256` [somma di controllo](#).
- StorageGRID ora supporta il checksum SHA-256 per le operazioni PUT, GET e HEAD. Questi checksum migliorano l'integrità dei dati.

Modifiche al supporto del protocollo S3

- Aggiunto il supporto per Mountpoint per Amazon S3, che consente alle applicazioni di connettersi direttamente ai bucket S3 come se fossero file system locali. Ora puoi utilizzare StorageGRID con più applicazioni e più casi d'uso.
- Come parte dell'aggiunta del supporto per Mountpoint, StorageGRID 11.9 contiene ["ulteriori modifiche al supporto del protocollo S3"](#).

Manutenzione e supporto

AutoSupport

["AutoSupport"](#) ora crea automaticamente casi di guasto hardware per gli apparecchi legacy.

Operazioni di clonazione dei nodi espansive

L'usabilità del clone del nodo è stata ampliata per supportare nodi di archiviazione più grandi.

Migliorata la gestione ILM dei marcatori di eliminazione scaduti

Le regole temporali di acquisizione ILM con un periodo di tempo di giorni ora rimuovono anche i marcatori di eliminazione degli oggetti scaduti. I marcatori di eliminazione vengono rimossi solo quando è trascorso un periodo di tempo di Giorni e l'attuale creatore di eliminazione è scaduto (non ci sono versioni non correnti).

Fare riferimento a ["Come vengono eliminati gli oggetti con versione S3"](#) E ["Esempio di ciclo di vita del bucket che ha la priorità sulla policy ILM"](#).

Dismissione migliorata dei nodi

Per garantire una transizione fluida ed efficiente all'hardware di nuova generazione StorageGRID, ["dismissione del nodo"](#) è stato migliorato.

Syslog per gli endpoint del bilanciamento del carico

I registri di accesso agli endpoint del bilanciamento del carico contengono informazioni per la risoluzione dei problemi, come i codici di stato HTTP. StorageGRID ora supporta ["esportare questi registri su un server syslog esterno"](#). Questo miglioramento consente una gestione più efficiente dei registri e l'integrazione con i sistemi di monitoraggio e avviso esistenti.

Ulteriori miglioramenti per la manutenzione e la supportabilità

- Aggiornamento dell'interfaccia utente delle metriche
- Nuove qualifiche del sistema operativo

- Supporto per nuovi componenti di terze parti

Sicurezza

Rotazione delle chiavi di accesso SSH

Gli amministratori della rete possono ora ["aggiornare e ruotare le chiavi SSH"](#) . La possibilità di ruotare le chiavi SSH è una buona pratica di sicurezza e un meccanismo di difesa proattivo.

Avvisi per gli accessi root

Quando un'entità sconosciuta accede a Grid Manager come root, ["viene attivato un avviso"](#) . Monitorare gli accessi root SSH è un passo proattivo verso la salvaguardia della tua infrastruttura.

Miglioramenti di Grid Manager

Pagina dei profili di codifica di cancellazione spostata

La pagina dei profili di codifica di cancellazione si trova ora in **CONFIGURAZIONE > Sistema > Codifica di cancellazione**. In passato era presente nel menu ILM.

Miglioramenti della ricerca

IL ["campo di ricerca nel Grid Manager"](#) ora include una logica di corrispondenza migliore, che consente di trovare le pagine cercando abbreviazioni comuni e in base ai nomi di determinate impostazioni all'interno di una pagina. Puoi anche cercare altri tipi di elementi, come nodi, utenti e account tenant.

Funzionalità e capacità rimosse o deprecate

Alcune funzionalità e capacità sono state rimosse o deprecate in questa versione. Esaminare questi elementi per capire se è necessario aggiornare le applicazioni client o modificare la configurazione prima di eseguire l'aggiornamento.

Definizioni

Obsoleto

La funzionalità **non dovrebbe** essere utilizzata nei nuovi ambienti di produzione. Gli ambienti di produzione esistenti possono continuare a utilizzare la funzionalità.

Fine della vita

Ultima versione distribuita che supporta la funzionalità. In alcuni casi, la documentazione relativa alla funzionalità potrebbe essere rimossa in questa fase.

RIMOSSO

Prima versione che **non** supporta la funzionalità.

Supporto per la fine delle funzionalità StorageGRID

Le funzionalità deprecate verranno rimosse nelle versioni principali N+2. Ad esempio, se una funzionalità è obsoleta nella versione N (ad esempio, 6.3), l'ultima versione in cui la funzionalità sarà presente sarà N+1 (ad esempio, 6.4). La versione N+2 (ad esempio, 6.5) è la prima versione quando la funzionalità non è presente nel prodotto.

Vedi il ["Pagina di supporto della versione software"](#) per ulteriori informazioni.



In determinate situazioni, NetApp potrebbe interrompere il supporto per determinate funzionalità prima del previsto.

Caratteristica	Obsoleto	Fine della vita	RIMOSSO	Link alla documentazione precedente
Allarmi legacy (<i>non avvisi</i>)	11,7	11,8	11,9	"Riferimento allarmi (StorageGRID 11.8)"
Supporto del nodo di archivio	11,7	11,8	11,9	"Considerazioni sulla dismissione dei nodi di archivio (StorageGRID 11.8)" Nota: prima di iniziare l'aggiornamento, è necessario: 1. Disattivare tutti i nodi di archivio. Vedere "Dismissione del nodo di rete (sito di documentazione StorageGRID 11.8)" . 2. Rimuovere tutti i riferimenti al nodo di archivio dai pool di archiviazione e dai criteri ILM. Vedere "Base di conoscenza NetApp : guida alla risoluzione dell'aggiornamento del software StorageGRID 11.9" .
Esportazione di audit tramite CIFS/Samba	11,1	11,6	11,7	
Servizio CLB	11,4	11,6	11,7	
Motore per container Docker	11,8	11,9	Da definire	Il supporto per Docker come motore di container per distribuzioni esclusivamente software è deprecato. Docker verrà sostituito con un altro motore di container in una versione futura. Fare riferimento al "elenco delle versioni di Docker attualmente supportate" .
Esportazione di controllo NFS	11,8	11,9	12,0	"Configurare l'accesso client di audit per NFS (StorageGRID 11.8)"
Supporto API Swift	11,7	11,9	12,0	"Utilizzare Swift REST API (StorageGRID 11.8)"
RHEL 8.8	11,9	11,9	12,0	

Caratteristica	Obsoleto	Fine della vita	RIMOSSO	Link alla documentazione precedente
RHEL 9.0	11,9	11,9	12,0	
RHEL 9.2	11,9	11,9	12,0	
Ubuntu 18,04	11,9	11,9	12,0	
Ubuntu 20,04	11,9	11,9	12,0	
Debian 11	11,9	11,9	12,0	

Vedere anche:

- ["Modifiche all'API di gestione della griglia"](#)
- ["Modifiche all'API di gestione degli inquilini"](#)

Modifiche all'API di gestione della griglia

StorageGRID 11.9 utilizza la versione 4 della Grid Management API. La versione 4 deprecia 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 con StorageGRID 11.9; tuttavia, il supporto per queste versioni dell'API verrà rimosso in una futura versione di StorageGRID. Dopo l'aggiornamento a StorageGRID 11.9, è possibile disattivare le API deprecate utilizzando `PUT /grid/config/management API`.

Per saperne di più, vai a ["Utilizzare l'API di gestione della griglia"](#).

Rivedere le impostazioni di conformità dopo aver abilitato il blocco globale degli oggetti S3

Dopo aver abilitato l'impostazione globale Blocco oggetti S3, rivedere le impostazioni di conformità dei tenant esistenti. Quando si abilita questa impostazione, le impostazioni di S3 Object Lock per tenant dipendono dalla versione StorageGRID al momento della creazione del tenant.

Richieste mgmt-api legacy rimosse

Queste richieste legacy sono state rimosse:

`/grid/server-types`

`/grid/ntp-roles`

Modifiche a `GET /private/storage-usage` API

- Una nuova proprietà, `usageCacheDuration`, è stato aggiunto al corpo della risposta. Questa proprietà specifica la durata (in secondi) per cui la cache di ricerca dell'utilizzo rimane valida. Questo valore si applica quando si verifica l'utilizzo rispetto alla quota di archiviazione del tenant e ai limiti di capacità del bucket.

- IL GET `/api/v4/private/storage-usage` il comportamento è stato corretto per corrispondere all'annidamento dello schema.
- Queste modifiche si applicano solo all'API privata.

Modifiche a GET `cross-grid-replication` API

L'API GET `/org/containers/:name/cross-grid-replication` non richiede più l'accesso Root(`rootAccess`) autorizzazione; tuttavia, è necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione Gestisci tutti i bucket(`manageAllContainers`) o Visualizza tutti i bucket(`viewAllContainers`) permesso.

L'API PUT `/org/containers/:name/cross-grid-replication` non è cambiata e richiede ancora l'accesso Root(`rootAccess`) permesso.

Modifiche all'API di gestione degli inquilini

StorageGRID 11.9 utilizza la versione 4 dell'API Tenant Management. La versione 4 deprecia la versione 3; tuttavia, le versioni 1, 2 e 3 sono ancora supportate.



È possibile continuare a utilizzare le versioni obsolete dell'API Tenant Management con StorageGRID 11.9; tuttavia, il supporto per queste versioni dell'API verrà rimosso in una futura versione di StorageGRID. Dopo l'aggiornamento a StorageGRID 11.9, è possibile disattivare le API deprecate utilizzando PUT `/grid/config/management` API.

Per saperne di più, vai a ["Comprendere l'API di gestione degli inquilini"](#).

Nuova API per il limite di capacità del bucket

Puoi usare il `/org/containers/{bucketName}/quota-object-bytes` API con operazioni GET/PUT per ottenere e impostare il limite di capacità di archiviazione per un bucket.

Pianificare e preparare l'aggiornamento

Stimare il tempo necessario per completare un aggiornamento

Valuta quando effettuare l'aggiornamento, in base al tempo che potrebbe richiedere. Siate consapevoli delle operazioni che potete e non potete eseguire durante ogni fase dell'aggiornamento.

Informazioni su questo compito

Il tempo necessario per completare un aggiornamento StorageGRID dipende da diversi fattori, tra cui il carico del client e le prestazioni dell'hardware.

La tabella riassume le principali attività di aggiornamento e indica il tempo approssimativo necessario per ciascuna attività. I passaggi successivi alla tabella forniscono istruzioni utili per stimare i tempi di aggiornamento del sistema.

Attività di aggiornamento	Descrizione	Tempo approssimativo richiesto	Durante questo compito
Eseguire controlli preliminari e aggiornare il nodo di amministrazione primario	Vengono eseguiti i controlli preliminari all'aggiornamento e il nodo di amministrazione primario viene arrestato, aggiornato e riavviato.	Da 30 minuti a 1 ora, con i nodi degli appliance di servizi che richiedono più tempo. Gli errori di pre-controllo non risolti aumenteranno questa volta.	Non è possibile accedere al nodo di amministrazione primario. Potrebbero essere segnalati errori di connessione, che puoi ignorare. L'esecuzione dei controlli preliminari all'aggiornamento prima di avviarlo consente di risolvere eventuali errori prima della finestra di manutenzione programmata per l'aggiornamento.
Avvia il servizio di aggiornamento	Il file software viene distribuito e il servizio di aggiornamento viene avviato.	3 minuti per nodo della griglia	
Aggiorna altri nodi della griglia	Il software su tutti gli altri nodi della griglia viene aggiornato nell'ordine in cui si approvano i nodi. Ogni nodo del tuo sistema verrà disattivato uno alla volta.	Da 15 minuti a 1 ora per nodo, con i nodi appliance che richiedono più tempo Nota: per i nodi appliance, StorageGRID Appliance Installer viene aggiornato automaticamente all'ultima versione.	• Non modificare la configurazione della griglia. • Non modificare la configurazione del livello di controllo. • Non aggiornare la configurazione ILM. • Non è possibile eseguire altre procedure di manutenzione, come hotfix, dismissione o espansione. Nota: se è necessario eseguire un ripristino, contattare l'assistenza tecnica.
Abilita funzionalità	Le nuove funzionalità della nuova versione sono abilitate.	Meno di 5 minuti	• Non modificare la configurazione della griglia. • Non modificare la configurazione del livello di controllo. • Non aggiornare la configurazione ILM. • Non è possibile eseguire un'altra procedura di manutenzione.

Attività di aggiornamento	Descrizione	Tempo approssimativo richiesto	Durante questo compito
Aggiorna il database	Il processo di aggiornamento controlla ogni nodo per verificare che il database Cassandra non debba essere aggiornato.	10 secondi per nodo o pochi minuti per l'intera griglia	L'aggiornamento da StorageGRID 11.8 a 11.9 non richiede un aggiornamento del database Cassandra; tuttavia, il servizio Cassandra verrà arrestato e riavviato su ciascun nodo di archiviazione. Per le future versioni delle funzionalità StorageGRID, il completamento della fase di aggiornamento del database Cassandra potrebbe richiedere diversi giorni.
Passaggi finali di aggiornamento	I file temporanei vengono rimossi e l'aggiornamento alla nuova versione viene completato.	5 minuti	Una volta completata l'attività Fasi finali di aggiornamento , è possibile eseguire tutte le procedure di manutenzione.

Passi

1. Stimare il tempo necessario per aggiornare tutti i nodi della griglia.
 - a. Moltiplica il numero di nodi nel tuo sistema StorageGRID per 1 ora/nodo.

Di norma, l'aggiornamento dei nodi appliance richiede più tempo rispetto ai nodi basati su software.
 - b. Aggiungere 1 ora a questo tempo per tenere conto del tempo necessario per scaricare il .upgrade file, eseguire le convalide preliminari e completare i passaggi finali di 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. Calcolare il tempo totale stimato per l'aggiornamento sommando i risultati dei passaggi 1 e 2.

Esempio: tempo stimato per l'aggiornamento a StorageGRID 11.9

Supponiamo che il tuo sistema abbia 14 nodi di griglia, di cui 8 sono 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 tenere conto del tempo necessario per installare il pacchetto RPM o DEB sui nodi Linux.

Il tempo stimato per questa fase è di 2 ore.

4. Sommare i valori.

Per completare l'aggiornamento del sistema a StorageGRID 11.9.0 potrebbero essere necessarie fino a 17 ore.



Se necessario, è possibile suddividere la finestra di manutenzione in finestre più piccole approvando sottoinsiemi di nodi della griglia da aggiornare in più sessioni. Ad esempio, potresti preferire aggiornare i nodi nel sito A in una sessione e poi aggiornare i nodi nel sito B in una sessione successiva. Se si sceglie di eseguire l'aggiornamento in più sessioni, tenere presente che non sarà possibile iniziare a utilizzare le nuove funzionalità finché tutti i nodi non saranno stati aggiornati.

Come viene influenzato il tuo sistema durante l'aggiornamento

Scopri come l'aggiornamento interesserà il tuo sistema StorageGRID .

Gli aggiornamenti StorageGRID non sono dirompenti

Il sistema StorageGRID può acquisire e recuperare dati dalle applicazioni client durante l'intero processo di aggiornamento. Se si approva l'aggiornamento di tutti i nodi dello stesso tipo (ad esempio, nodi di archiviazione), i nodi vengono disattivati uno alla volta, quindi non c'è un momento in cui tutti i nodi della griglia o tutti i nodi della griglia di un certo tipo non sono disponibili.

Per garantire una disponibilità continua, assicurati che la policy ILM contenga regole che specifichino l'archiviazione di più copie di ciascun oggetto. È inoltre necessario assicurarsi che tutti i client S3 esterni siano configurati per inviare richieste a uno dei seguenti:

- Un indirizzo IP virtuale di gruppo ad alta disponibilità (HA)
- Un bilanciatore di carico di terze parti ad alta disponibilità
- Più nodi gateway per ogni client
- Più nodi di archiviazione per ogni client

Le applicazioni client potrebbero subire interruzioni a breve termine

Il sistema StorageGRID può acquisire e recuperare dati dalle applicazioni client durante l'intero processo di aggiornamento; tuttavia, le connessioni client ai singoli nodi gateway o nodi di archiviazione potrebbero essere temporaneamente interrotte se l'aggiornamento richiede il riavvio dei servizi su tali nodi. La connettività verrà ripristinata al termine del processo di aggiornamento e i servizi saranno ripresi sui singoli nodi.

Potrebbe essere necessario pianificare un periodo 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 quando aggiornare determinati nodi.



È possibile utilizzare più gateway e gruppi ad alta disponibilità (HA) per garantire il failover automatico durante il processo di aggiornamento. Vedi le istruzioni per "[configurazione di gruppi ad alta disponibilità](#)".

Il firmware dell'apparecchio è aggiornato

Durante l'aggiornamento StorageGRID 11.9:

- Tutti i nodi dell'appliance StorageGRID vengono automaticamente aggiornati alla versione 3.9 del firmware StorageGRID Appliance Installer.
- Gli apparecchi SG6060 e SGF6024 vengono automaticamente aggiornati alla versione firmware BIOS 3B08.EX e alla versione firmware BMC 4.00.07.
- Gli apparecchi SG100 e SG1000 vengono automaticamente aggiornati alla versione firmware BIOS

3B13.EC e alla versione firmware BMC 4.74.07.

- Gli apparecchi SGF6112, SG6160, SG110 e SG1100 vengono automaticamente aggiornati alla versione firmware BMC 3.16.07.

Le politiche ILM vengono gestite in modo diverso a seconda del loro stato

- La policy attiva rimarrà la stessa dopo l'aggiornamento.
- Durante l'aggiornamento vengono conservate solo le ultime 10 policy storiche.
- Se è stata proposta una policy, questa verrà eliminata durante l'aggiornamento.

Potrebbero essere attivati degli avvisi

Gli avvisi potrebbero essere attivati quando i servizi vengono avviati e arrestati e quando il sistema StorageGRID funziona come ambiente a versione mista (alcuni nodi della griglia eseguono una versione precedente, mentre altri sono stati aggiornati a una versione successiva). Al termine dell'aggiornamento potrebbero essere attivati altri avvisi.

Ad esempio, potresti visualizzare l'avviso **Impossibile comunicare con il nodo** quando i servizi sono arrestati oppure l'avviso **Errore di comunicazione Cassandra** quando alcuni nodi sono stati aggiornati a StorageGRID 11.9 ma altri nodi eseguono ancora StorageGRID 11.8. In genere, questi avvisi scompariranno al termine dell'aggiornamento.

L'avviso **Posizionamento ILM non realizzabile** potrebbe essere attivato quando i nodi di archiviazione vengono arrestati durante l'aggiornamento a StorageGRID 11.9. Questo avviso potrebbe persistere per 1 giorno dopo il completamento dell'aggiornamento.

Una volta completato l'aggiornamento, puoi rivedere tutti 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 potrebbe essere generato un numero elevato di notifiche SNMP quando i nodi della griglia vengono arrestati e riavviati durante l'aggiornamento. Per evitare notifiche eccessive, deselezionare la casella di controllo **Abilita notifiche agente SNMP (CONFIGURAZIONE > Monitoraggio > Agente SNMP)** per disabilitare le notifiche SNMP prima di avviare l'aggiornamento. Quindi, riattivare le notifiche una volta completato l'aggiornamento.

Le modifiche alla configurazione sono limitate



Questo elenco si applica specificamente agli aggiornamenti da StorageGRID 11.8 a StorageGRID 11.9. Se si esegue l'aggiornamento a un'altra versione StorageGRID, fare riferimento all'elenco delle modifiche limitate nelle istruzioni di aggiornamento per quella versione.

Fino al completamento dell'attività **Abilita nuova funzionalità**:

- Non apportare modifiche alla configurazione della griglia.
- Non abilitare o disabilitare nuove funzionalità.
- Non aggiornare la configurazione ILM. In caso contrario, potresti riscontrare un comportamento ILM incoerente e inaspettato.
- Non applicare un hotfix o ripristinare un nodo della griglia.



Se è necessario ripristinare un nodo durante l'aggiornamento, contattare l'assistenza tecnica.

- Non dovresti gestire gruppi HA, interfacce VLAN o endpoint del bilanciatore del carico durante l'aggiornamento a StorageGRID 11.9.
- Non eliminare alcun gruppo HA finché non sarà completato l'aggiornamento a StorageGRID 11.9. Gli indirizzi IP virtuali in altri gruppi HA potrebbero diventare inaccessibili.

Fino al completamento dell'attività **Passaggi finali di aggiornamento**:

- Non eseguire una procedura di espansione.
- Non eseguire una procedura di disattivazione.

Non è possibile visualizzare i dettagli del bucket o gestirli dal Tenant Manager

Durante l'aggiornamento a StorageGRID 11.9 (ovvero mentre il sistema funziona come ambiente a versione mista), non è possibile visualizzare i dettagli dei bucket o gestirli tramite Tenant Manager. Uno dei seguenti errori viene visualizzato nella pagina Bucket in Tenant Manager:

- Non puoi utilizzare questa API durante l'aggiornamento alla versione 11.9.
- Non è possibile visualizzare i dettagli del controllo delle versioni dei bucket in Tenant Manager durante l'aggiornamento alla versione 11.9.

Questo errore verrà risolto una volta completato l'aggiornamento alla versione 11.9.

Soluzione alternativa

Mentre è in corso l'aggiornamento alla versione 11.9, utilizzare i seguenti strumenti per visualizzare i dettagli dei bucket o gestirli, anziché utilizzare Tenant Manager:

- Per eseguire operazioni S3 standard su un bucket, utilizzare ["API REST S3"](#) o il ["API di gestione degli inquilini"](#).
- Per eseguire operazioni personalizzate StorageGRID su un bucket (ad esempio, visualizzare e modificare la coerenza del bucket, abilitare o disabilitare gli aggiornamenti dell'ora dell'ultimo accesso o configurare l'integrazione della ricerca), utilizzare l'API Tenant Management.

Verificare la versione installata di StorageGRID

Prima di avviare l'aggiornamento, verificare che sia installata la versione precedente di StorageGRID con l'ultimo hotfix disponibile applicato.

Informazioni su questo compito

Prima di eseguire l'aggiornamento a StorageGRID 11.9, è necessario che nella griglia sia installato StorageGRID 11.8. Se stai utilizzando una versione precedente di StorageGRID, devi installare tutti i file di aggiornamento precedenti insieme ai relativi hotfix più recenti (fortemente consigliato) finché la versione corrente della tua griglia non sarà StorageGRID 11.8.x.y.

Un possibile percorso di aggiornamento è mostrato in [esempio](#).



NetApp consiglia vivamente di applicare l'hotfix più recente per ogni versione StorageGRID prima di eseguire l'aggiornamento alla versione successiva e di applicare l'hotfix più recente per ogni nuova versione installata. In alcuni casi è necessario applicare un hotfix per evitare il rischio di perdita di dati. Vedere ["Download NetApp : StorageGRID"](#) e le note di rilascio per ogni hotfix per saperne di più.

Passi

1. Sign in a Grid Manager utilizzando un ["browser web supportato"](#) .
2. Nella parte superiore di Grid Manager, seleziona **Guida > Informazioni**.
3. Verificare che **Versione** sia 11.8.x.y.

Nel numero di versione StorageGRID 11.8.x.y:

- La **versione principale** ha un valore x pari a 0 (11.8.0).
 - Un **hotfix**, se applicato, ha un valore y (ad esempio, 11.8.0.1).
4. Se **Versione** non è 11.8.x.y, vai a ["Download NetApp : StorageGRID"](#) per scaricare i file di ogni versione precedente, incluso l'ultimo hotfix per ogni versione.
 5. Ottieni le istruzioni di aggiornamento per ogni versione scaricata. Quindi, eseguire la procedura di aggiornamento del software per quella versione e applicare l'hotfix più recente per quella versione (fortemente consigliato).

Vedi il ["Procedura di hotfix di StorageGRID"](#) .

Esempio: aggiornamento a StorageGRID 11.9 dalla versione 11.6

L'esempio seguente mostra i passaggi per eseguire l'aggiornamento dalla versione 11.6 StorageGRID alla versione 11.8 in preparazione per un aggiornamento a StorageGRID 11.9.

Scarica e installa il software nella seguente sequenza per preparare il tuo sistema all'aggiornamento:

1. Aggiorna alla versione principale StorageGRID 11.6.0.
2. Applicare l'ultimo hotfix StorageGRID 11.6.0.y.
3. Aggiorna alla versione principale StorageGRID 11.7.0.
4. Applicare l'ultimo hotfix StorageGRID 11.7.0.y.
5. Aggiorna alla versione principale StorageGRID 11.8.0.
6. Applicare l'ultimo hotfix StorageGRID 11.8.0.y.

Ottenere i materiali necessari per un aggiornamento del software

Prima di iniziare l'aggiornamento del software, procuratevi tutto il materiale necessario.

Articolo	Note
Computer portatile di servizio	Il portatile di servizio deve avere: • Porta di rete • Client SSH (ad esempio, PuTTY)

Articolo	Note
"Browser web supportato"	In genere, il supporto del browser cambia per ogni versione StorageGRID . Assicurati che il tuo browser sia compatibile con la nuova versione StorageGRID .
Frase segreta di provisioning	La passphrase viene creata e documentata quando il sistema StorageGRID viene installato per la prima volta. La passphrase di provisioning non è elencata in <code>Passwords.txt</code> file.
Archivio RPM o DEB di Linux	Se i nodi sono distribuiti su host Linux, è necessario "scaricare e installare il pacchetto RPM o DEB su tutti gli host" prima di iniziare l'aggiornamento. Assicurati che il tuo sistema operativo soddisfi i requisiti minimi della versione del kernel di StorageGRID: • "Installa StorageGRID sugli host Red Hat Enterprise Linux" • "Installa StorageGRID su host Ubuntu o Debian"
Documentazione StorageGRID	• "Note di rilascio" per StorageGRID 11.9 (è richiesto l'accesso). Assicuratevi di leggerli attentamente prima di iniziare l'aggiornamento. • "Guida alla risoluzione dell'aggiornamento del software StorageGRID" per la versione principale a cui stai effettuando l'aggiornamento (è richiesto l'accesso) • Altro "Documentazione StorageGRID" , come richiesto.

Controllare le condizioni del sistema

Prima di aggiornare un sistema StorageGRID , verificare che il sistema sia pronto ad accogliere l'aggiornamento. Assicurarsi che il sistema funzioni normalmente e che tutti i nodi della griglia siano operativi.

Passi

1. Sign in a Grid Manager utilizzando un ["browser web supportato"](#) .
2. Controllare e risolvere eventuali avvisi attivi.
3. Verificare che non vi siano attività di griglia in conflitto attive o in sospenso.
 - a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - b. Selezionare **site > primary Admin Node > CMN > Grid Tasks > Configurazione**.

Le attività di valutazione della gestione del ciclo di vita delle informazioni (ILME) sono le uniche attività della griglia che possono essere eseguite contemporaneamente all'aggiornamento del software.

- c. Se sono attive o in sospenso altre attività della griglia, attendere che vengano completate o che il blocco venga rilasciato.



Contattare l'assistenza tecnica se un'attività non viene completata o se il blocco non viene sbloccato.

4. Fare riferimento a "[Comunicazioni interne al nodo della griglia](#)" E "[Comunicazioni esterne](#)" per garantire che tutte le porte richieste per StorageGRID 11.9 siano aperte prima dell'aggiornamento.



Non sono necessarie porte aggiuntive durante l'aggiornamento a StorageGRID 11.9.

La seguente porta obbligatoria è stata aggiunta in StorageGRID 11.7. Assicurati che sia disponibile prima di eseguire l'aggiornamento a StorageGRID 11.9.

Porta	Descrizione
18086	Porta TCP utilizzata per le richieste S3 dal bilanciatore del carico StorageGRID a LDR e al nuovo servizio LDR. Prima di effettuare l'aggiornamento, verificare che questa porta sia aperta da tutti i nodi della griglia a tutti i nodi di archiviazione. Il blocco di questa porta causerà interruzioni del servizio S3 dopo l'aggiornamento a StorageGRID 11.9.



Se hai aperto porte firewall personalizzate, verrai avvisato durante il pre-controllo dell'aggiornamento. Prima di procedere con l'aggiornamento è necessario contattare l'assistenza tecnica.

Aggiorna il software

Avvio rapido dell'aggiornamento

Prima di iniziare l'aggiornamento, rivedere il flusso di lavoro generale. La pagina Aggiornamento StorageGRID ti guida attraverso ogni fase dell'aggiornamento.

1

Preparare gli host Linux

Se i nodi StorageGRID sono distribuiti su host Linux, "[installare il pacchetto RPM o DEB su ciascun host](#)" prima di iniziare l'aggiornamento.

2

Carica i file di aggiornamento e hotfix

Dal nodo di amministrazione principale, accedi alla pagina di aggiornamento StorageGRID e carica il file di aggiornamento e il file hotfix, se necessario.

3

Scarica il pacchetto di ripristino

Scaricare il pacchetto di ripristino corrente prima di avviare l'aggiornamento.

4

Eseguire i controlli preliminari dell'aggiornamento

I controlli preliminari all'aggiornamento ti aiutano a individuare i problemi, in modo da poterli risolvere prima di avviare l'aggiornamento vero e proprio.

5

Avvia l'aggiornamento

Quando si avvia l'aggiornamento, i controlli preliminari vengono eseguiti nuovamente e il nodo di amministrazione primario viene aggiornato automaticamente. Non è possibile accedere a Grid Manager mentre è in corso 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 il pacchetto di ripristino

Dopo aver aggiornato il nodo di amministrazione primario, scaricare un nuovo pacchetto di ripristino.

7

Approva i nodi

È possibile approvare singoli nodi della griglia, gruppi di nodi della griglia o tutti i nodi della griglia.



Non approvare l'aggiornamento di un nodo della griglia a meno che tu non sia sicuro che il nodo sia pronto per essere arrestato e riavviato.

8

Riprendere le operazioni

Una volta aggiornati tutti i nodi della griglia, vengono abilitate nuove funzionalità e sarà possibile riprendere le operazioni. Per eseguire una procedura di dismissione o espansione, è necessario attendere il completamento dell'attività in background **Aggiorna database** e dell'attività **Passaggi finali di aggiornamento**.

Informazioni correlate

["Stimare il tempo necessario per completare un aggiornamento"](#)

Linux: Scarica e installa il pacchetto RPM o DEB su tutti gli host

Se i nodi StorageGRID sono distribuiti 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 di StorageGRID da Grid Manager, come primo passaggio viene richiesto di scaricare l'archivio di aggiornamento e qualsiasi hotfix necessario. Tuttavia, se è necessario scaricare file per aggiornare gli host Linux, è possibile risparmiare tempo scaricando in anticipo tutti i file necessari.

Passi

1. Vai a ["Download NetApp : StorageGRID"](#) .
2. Seleziona il pulsante per scaricare l'ultima versione oppure seleziona un'altra versione dal menu a discesa e seleziona **Vai**.

Le versioni del software StorageGRID hanno il seguente formato: 11.x.y. Gli hotfix StorageGRID hanno il seguente formato: 11.x.y.z.

3. Sign in con il nome utente e la password del tuo account NetApp .
4. Se viene visualizzato un avviso di attenzione/lettura obbligatoria, prendere nota del numero dell'hotfix e selezionare la casella di controllo.

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

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

6. Dalla seconda colonna (**Aggiorna StorageGRID**), scarica due file:
 - Archivio di aggiornamento per l'ultima versione (si tratta del file nella sezione denominata **VMware, SG1000 o SG100 Primary Admin Node**). Sebbene questo file non sia necessario finché non si esegue l'aggiornamento, scaricarlo ora farà risparmiare tempo.
 - Un archivio RPM o DEB in entrambi .tgz O .zip formato. Seleziona il .zip file se si utilizza Windows sul portatile di servizio.
 - 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 hai dovuto accettare un avviso di Attenzione/Lettura obbligatoria a causa di un hotfix richiesto, scarica l'hotfix:
 - a. Torna a ["Download NetApp : StorageGRID"](#) .
 - b. Selezionare il numero dell'hotfix dal menu a discesa.
 - c. Accettare nuovamente l'avviso di avvertenza e l'EULA.
 - d. Scarica e salva l'hotfix e il relativo file README.

All'avvio dell'aggiornamento, ti verrà richiesto di caricare il file hotfix nella pagina di aggiornamento StorageGRID .

Installa l'archivio su tutti gli host Linux

Eseguire questi passaggi prima di aggiornare il software StorageGRID .

Passi

1. Estrarre i pacchetti RPM o DEB dal file di installazione.
2. Installare i pacchetti RPM o DEB su tutti gli host Linux.

Consultare i passaggi per l'installazione dei servizi host StorageGRID nelle istruzioni di installazione:

- ["Red Hat Enterprise Linux: installa i servizi host StorageGRID"](#)
- ["Ubuntu o Debian: installa i servizi host StorageGRID"](#)

I nuovi pacchetti vengono installati come pacchetti aggiuntivi.

Rimuovere gli archivi di installazione per le versioni precedenti

Per liberare spazio sugli host Linux, puoi rimuovere gli archivi di installazione delle versioni precedenti di StorageGRID di cui non hai più bisogno.

Passi

1. Rimuovere i vecchi archivi di installazione StorageGRID .

Cappello rosso

1. Acquisisci l'elenco dei pacchetti StorageGRID installati: `dnf list | grep -i storagegrid`.

Esempio:

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. Rimuovere i pacchetti StorageGRID precedenti: `dnf remove images-package service-package`



Non rimuovere gli archivi di installazione per la versione di StorageGRID attualmente in esecuzione o per le versioni di StorageGRID a cui si prevede di eseguire l'aggiornamento.

Puoi tranquillamente ignorare gli avvisi che compaiono. Si riferiscono ai file che sono stati sostituiti quando si installano pacchetti StorageGRID più recenti.

Esempio:

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.

Dependencies resolved.
```

```

=====
=====
Package                Architecture      Version           Repository
Size
=====
=====
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
=====
=====
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__
.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:

```

```
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl
itter.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p
yc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:
remove failed: No such file or directory
```

```
Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 2/2
```

```
Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
```

```
Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-
```

```
20220210.0232.8d56cfe.x86_64 2/2
```

```
Installed products updated.
```

```
Removed:
```

```
StorageGRID-Webscale-Images-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64
```

```
StorageGRID-Webscale-Service-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64
```

```
Complete!
```

```
[root@rhel-example ~]#
```

Ubuntu e Debian

1. Acquisisci l'elenco dei pacchetti StorageGRID installati: `dpkg -l | grep storagegrid`

Esempio:

```
root@debian-example:~# dpkg -l | grep storagegrid  
ii storagegrid-webscale-images-11-6-0 11.6.0-20220210.0232.8d56cfe  
amd64 StorageGRID Webscale docker images for 11.6.0  
ii storagegrid-webscale-images-11-7-0 11.7.0-  
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker  
images for 11.7.0  
ii storagegrid-webscale-images-11-8-0 11.8.0-20240131.0139.e3e0c87  
amd64 StorageGRID Webscale docker images for 11.8.0  
ii storagegrid-webscale-images-11-9-0 11.9.0-20240826.1753.4aeeb70  
amd64 StorageGRID Webscale docker images for 11.9.0  
ii storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe  
amd64 StorageGRID Webscale host services for 11.6.0  
ii storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c  
amd64 StorageGRID Webscale host services for 11.7.0  
ii storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87  
amd64 StorageGRID Webscale host services for 11.8.0  
ii storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70  
amd64 StorageGRID Webscale host services for 11.9.0  
root@debian-example:~#
```

2. Rimuovere i pacchetti StorageGRID precedenti: `dpkg -r images-package service-package`



Non rimuovere gli archivi di installazione per la versione di StorageGRID attualmente in esecuzione o per le versioni di StorageGRID a cui si prevede di eseguire l'aggiornamento.

Esempio:


```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. Rimuovere le immagini del contenitore StorageGRID .

Docker

1. Acquisisci l'elenco delle immagini dei contenitori installate: `docker images`

Esempio:

```
[root@docker-example ~]# docker images
REPOSITORY          TAG                 IMAGE ID            CREATED
SIZE
storagegrid-11.9.0  Admin_Node         610f2595bcb4       2 days ago
2.77GB
storagegrid-11.9.0  Storage_Node       7f73d33eb880       2 days ago
2.65GB
storagegrid-11.9.0  API_Gateway        2f0bb79526e9       2 days ago
1.82GB
storagegrid-11.8.0  Storage_Node       7125480de71b       7 months ago
2.54GB
storagegrid-11.8.0  Admin_Node         404e9f1bd173       7 months ago
2.63GB
storagegrid-11.8.0  Archive_Node       c3294a29697c       7 months ago
2.39GB
storagegrid-11.8.0  API_Gateway        1f88f24b9098       7 months ago
1.74GB
storagegrid-11.7.0  Storage_Node       1655350eff6f       16 months ago
2.51GB
storagegrid-11.7.0  Admin_Node         872258dd0dc8       16 months ago
2.48GB
storagegrid-11.7.0  Archive_Node       121e7c8b6d3b       16 months ago
2.41GB
storagegrid-11.7.0  API_Gateway        5b7a26e382de       16 months ago
1.77GB
storagegrid-11.6.0  Admin_Node         ee39f71a73e1       2 years ago
2.38GB
storagegrid-11.6.0  Storage_Node       f5ef895dcad0       2 years ago
2.08GB
storagegrid-11.6.0  Archive_Node       5782de552db0       2 years ago
1.95GB
storagegrid-11.6.0  API_Gateway        cb480ed37eea       2 years ago
1.35GB
[root@docker-example ~]#
```

2. Rimuovere le immagini dei contenitori per le versioni precedenti StorageGRID : `docker rmi image id`



Non rimuovere le immagini del contenitore per la versione di StorageGRID attualmente in esecuzione o per le versioni di StorageGRID a cui si prevede di eseguire l'aggiornamento.

Esempio:

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051ddf02
Deleted:
sha256:5f269aabbf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8cccafa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66bde
[root@docker-example ~]#
```

Podman

1. Acquisisci l'elenco delle immagini dei contenitori installate: `podman images`

Esempio:

```
[root@podman-example ~]# podman images
```

REPOSITORY SIZE	TAG	IMAGE ID	CREATED
localhost/storagegrid-11.8.0 2.57 GB	Storage_Node	7125480de71b	7 months ago
localhost/storagegrid-11.8.0 2.67 GB	Admin_Node	404e9f1bd173	7 months ago
localhost/storagegrid-11.8.0 2.42 GB	Archive_Node	c3294a29697c	7 months ago
localhost/storagegrid-11.8.0 1.77 GB	API_Gateway	1f88f24b9098	7 months ago
localhost/storagegrid-11.7.0 2.54 GB	Storage_Node	1655350eff6f	16 months ago
localhost/storagegrid-11.7.0 2.51 GB	Admin_Node	872258dd0dc8	16 months ago
localhost/storagegrid-11.7.0 2.44 GB	Archive_Node	121e7c8b6d3b	16 months ago
localhost/storagegrid-11.7.0 1.8 GB	API_Gateway	5b7a26e382de	16 months ago
localhost/storagegrid-11.6.0 2.42 GB	Admin_Node	ee39f71a73e1	2 years ago
localhost/storagegrid-11.6.0 2.11 GB	Storage_Node	f5ef895dcad0	2 years ago
localhost/storagegrid-11.6.0 1.98 GB	Archive_Node	5782de552db0	2 years ago
localhost/storagegrid-11.6.0 1.38 GB	API_Gateway	cb480ed37eea	2 years ago

```
[root@podman-example ~]#
```

2. Rimuovere le immagini dei contenitori per le versioni precedenti StorageGRID : `podman rmi image id`



Non rimuovere le immagini del contenitore per la versione di StorageGRID attualmente in esecuzione o per le versioni di StorageGRID a cui si prevede di eseguire l'aggiornamento.

Esempio:

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

Eseguire l'aggiornamento

È possibile eseguire l'aggiornamento a StorageGRID 11.9 e applicare contemporaneamente l'hotfix più recente per quella versione. La pagina di aggiornamento StorageGRID fornisce il percorso di aggiornamento consigliato e link diretti alle pagine di download corrette.

Prima di iniziare

Hai esaminato tutte le considerazioni e completato tutti i passaggi di pianificazione e preparazione.

Accedi alla pagina di aggiornamento di StorageGRID

Come primo passo, accedi alla pagina StorageGRID Upgrade in Grid Manager.

Passi

1. Sign in a Grid Manager utilizzando un ["browser web supportato"](#) .
2. Selezionare **MANUTENZIONE** > **Sistema** > **Aggiornamento software**.
3. Dal riquadro di aggiornamento StorageGRID , seleziona **Aggiorna**.

Seleziona i file

Il percorso di aggiornamento nella pagina Aggiornamento StorageGRID indica quali versioni principali (ad esempio, 11.9.0) e hotfix (ad esempio, 11.9.0.1) è necessario installare per ottenere la versione più recente StorageGRID . Dovresti installare le versioni e gli hotfix consigliati 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 **Verifica aggiornamenti software** nella pagina AutoSupport (**SUPPORTO** > **Strumenti** > * AutoSupport* > **Impostazioni**) potrebbe essere disabilitata.

Passi

1. Per il passaggio **Seleziona file**, rivedere il percorso di aggiornamento.
2. Dalla sezione Scarica file, seleziona ciascun collegamento **Download** per scaricare i file richiesti dal sito di supporto NetApp .

Se non viene visualizzato alcun percorso di aggiornamento, andare a ["Download NetApp : StorageGRID"](#) per verificare se è disponibile una nuova versione o un hotfix e per scaricare i file necessari.



Se hai bisogno di scaricare e installare un pacchetto RPM o DEB su tutti gli host Linux, potresti già avere i file di aggiornamento e hotfix StorageGRID elencati nel percorso di aggiornamento.

3. Selezionare **Sfoglia** per caricare il file di aggiornamento della versione su StorageGRID:
`NetApp_StorageGRID_11.9.0_Software_uniqueID.upgrade`

Una volta completato il processo di caricamento e convalida, accanto al nome del file appare un segno di spunta verde.

4. Se hai scaricato un file hotfix, seleziona **Sfoglia** per caricare il file. L'hotfix verrà applicato automaticamente come parte dell'aggiornamento della versione.

5. Selezionare **Continua**.

Eseguire controlli preliminari

L'esecuzione di controlli preliminari consente di rilevare e risolvere eventuali problemi di aggiornamento prima di iniziare ad aggiornare la griglia.

Passi

1. Per il passaggio **Esegui controlli preliminari**, inizia immettendo la passphrase di provisioning per la tua griglia.
2. Seleziona **Scarica pacchetto di ripristino**.

Prima di aggiornare il nodo di amministrazione primario, è necessario scaricare la copia corrente del file del pacchetto di ripristino. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

3. Una volta scaricato il file, conferma di poter accedere al contenuto, incluso il `Passwords.txt` file.
4. Copia il file scaricato(`.zip`) in due luoghi sicuri, protetti e separati.



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 controlli preliminari** e attendere il completamento dei controlli preliminari.
6. Esaminare i dettagli per ogni pre-controllo segnalato e risolvere eventuali errori segnalati. Vedi il "[Guida alla risoluzione dell'aggiornamento del software StorageGRID](#)" per la versione StorageGRID 11.9.

È necessario risolvere tutti gli *errori* di pre-controllo prima di poter aggiornare il sistema. Tuttavia, non è necessario risolvere gli *avvertimenti* di pre-controllo prima di effettuare l'aggiornamento.



Se hai aperto porte firewall personalizzate, verrai avvisato durante la convalida del pre-controllo. Prima di procedere con l'aggiornamento è necessario contattare l'assistenza tecnica.

7. Se hai apportato modifiche alla configurazione per risolvere i problemi segnalati, seleziona nuovamente **Esegui controlli preliminari** per ottenere risultati aggiornati.

Se tutti gli errori sono stati risolti, verrà richiesto di avviare l'aggiornamento.

Avvia l'aggiornamento e aggiorna il nodo di amministrazione primario

Quando si avvia l'aggiornamento, vengono eseguiti nuovamente i controlli preliminari 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 mentre il nodo di amministrazione primario è in fase di aggiornamento. Anche i registri di controllo non saranno disponibili.

Passi

1. Selezionare **Avvia aggiornamento**.

Viene visualizzato un avviso per ricordarti che perderai temporaneamente l'accesso a Grid Manager.

2. Selezionare **OK** per confermare l'avviso e avviare l'aggiornamento.
3. Attendere che vengano eseguiti i controlli preliminari dell'aggiornamento e che il nodo di amministrazione primario venga aggiornato.



Se vengono segnalati errori di pre-controllo, risolverli e selezionare nuovamente **Avvia aggiornamento**.

Se la griglia ha un altro nodo di amministrazione online e pronto, è possibile utilizzarlo per monitorare lo stato del nodo di amministrazione 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 al passaggio **Aggiorna altri nodi**.

Aggiorna altri nodi

È necessario aggiornare tutti i nodi della griglia, ma è possibile eseguire più sessioni di aggiornamento e personalizzare la sequenza di aggiornamento. Ad esempio, potresti preferire aggiornare i nodi nel sito A in una sessione e poi aggiornare i nodi nel sito B in una sessione successiva. Se si sceglie di eseguire l'aggiornamento in più sessioni, tenere presente che non sarà possibile iniziare a utilizzare le nuove funzionalità finché tutti i nodi non saranno 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 della griglia, i servizi su quel nodo vengono arrestati. Successivamente, il nodo della griglia 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, programmare una finestra di manutenzione o avvisare i clienti.

Passi

1. Per il passaggio **Aggiorna altri nodi**, rivedere il Riepilogo, che fornisce l'ora di inizio dell'aggiornamento nel suo complesso e lo stato di ciascuna attività di aggiornamento principale.
 - **Avvia servizio di aggiornamento** è la prima attività di aggiornamento. Durante questa attività, il file software viene distribuito ai nodi della griglia e il servizio di aggiornamento viene avviato su ciascun nodo.
 - Una volta completata l'attività **Avvia servizio di 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, inserisci la passphrase di provisioning e scarica una nuova copia del Recovery Package.



Dopo aver aggiornato il nodo di amministrazione primario, è necessario scaricare una nuova copia del file del pacchetto di ripristino. 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 e i nodi di archiviazione.

Un nodo della griglia può trovarsi in una di queste fasi quando le tabelle vengono visualizzate per la prima volta:

- Disimballaggio dell'aggiornamento
- Scaricamento
- In attesa di approvazione

4. Quando sei pronto a selezionare i nodi della griglia per l'aggiornamento (o se devi annullare l'approvazione dei nodi selezionati), segui queste istruzioni:

Compito	Istruzioni
Cerca nodi specifici da approvare, ad esempio tutti i nodi in un sito particolare	Inserisci la stringa di ricerca nel campo Cerca
Seleziona tutti i nodi per l'aggiornamento	Seleziona Approva tutti i nodi
Seleziona tutti i nodi dello stesso tipo per l'aggiornamento (ad esempio, tutti i nodi di archiviazione)	Selezionare il pulsante Approva tutto per il tipo di nodo Se si approvano più nodi dello stesso tipo, i nodi verranno aggiornati uno alla volta.
Seleziona un singolo nodo per l'aggiornamento	Selezionare il pulsante Approva per il nodo
Posticipa l'aggiornamento su tutti i nodi selezionati	Seleziona Non approvare tutti i nodi
Posticipa l'aggiornamento su tutti i nodi selezionati dello stesso tipo	Selezionare il pulsante Non approvare tutto per il tipo di nodo
Posticipare l'aggiornamento su un singolo nodo	Selezionare il pulsante Non approvare per il nodo

5. Attendi che i nodi approvati procedano attraverso queste fasi di aggiornamento:

- Approvato e in attesa di essere aggiornato
- Interruzione dei servizi



Non è possibile rimuovere un nodo quando la sua fase raggiunge **Arresto dei servizi**. Il pulsante **Non approvare** è disabilitato.

- Contenitore di arresto
- Pulizia delle immagini Docker
- Aggiornamento dei pacchetti del sistema operativo di base



Quando un nodo dell'appliance raggiunge questa fase, il software StorageGRID Appliance Installer sull'appliance viene aggiornato. Questo processo automatizzato garantisce che la versione di StorageGRID Appliance Installer rimanga sincronizzata con la versione del software StorageGRID .

- Riavvio



Alcuni modelli di appliance potrebbero riavviarsi più volte per aggiornare il firmware e il BIOS.

- Esecuzione dei passaggi dopo il riavvio
- Servizi di avvio
- Fatto

6. Ripeti il **fase di approvazione** tutte le volte necessarie finché tutti i nodi della griglia non saranno stati aggiornati.

Aggiornamento completo

Quando tutti i nodi della griglia hanno completato le fasi di aggiornamento, l'attività **Aggiorna altri nodi della griglia** viene visualizzata come Completata. Le restanti attività di aggiornamento vengono eseguite automaticamente in background.

Passi

1. Non appena l'attività **Abilita funzionalità** è completata (operazione che avviene rapidamente), puoi iniziare a utilizzare "nuove funzionalità" nella versione aggiornata StorageGRID .
2. Durante l'attività **Aggiorna database**, il processo di aggiornamento controlla ogni nodo per verificare che il database Cassandra non debba essere aggiornato.



L'aggiornamento da StorageGRID 11.8 a 11.9 non richiede un aggiornamento del database Cassandra; tuttavia, il servizio Cassandra verrà arrestato e riavviato su ciascun nodo di archiviazione. Per le future versioni delle funzionalità StorageGRID , il completamento della fase di aggiornamento del database Cassandra potrebbe richiedere diversi giorni.

3. Una volta completata l'attività **Aggiorna database**, attendere qualche minuto affinché vengano completati i **Passaggi finali dell'aggiornamento**.
4. Una volta completati i **passaggi finali dell'aggiornamento**, l'aggiornamento è completato. Il primo passaggio, **Seleziona file**, viene visualizzato nuovamente con un banner verde di successo.
5. Verificare che il funzionamento della rete sia tornato alla normalità:
 - a. Verificare che i servizi funzionino normalmente e che non vi siano avvisi imprevisti.
 - b. Verificare che le connessioni client al sistema StorageGRID funzionino come previsto.

Risolvere i problemi di aggiornamento

Se durante l'aggiornamento si verifica un problema, potresti riuscire a risolverlo autonomamente. Se non riesci a risolvere un problema, raccogli quante più informazioni possibili e contatta l'assistenza tecnica.

L'aggiornamento non viene completato

Nelle sezioni seguenti viene descritto come ripristinare situazioni in cui l'aggiornamento è parzialmente fallito.

Errori di pre-controllo dell'aggiornamento

Per rilevare e risolvere i problemi, è possibile eseguire manualmente i controlli preliminari all'aggiornamento prima di avviare l'aggiornamento vero e proprio. 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 l'assistenza tecnica.

Il nodo della griglia si blocca o non riesce ad avviarsi

Se un nodo della griglia si blocca durante il processo di aggiornamento o non si avvia correttamente al termine dell'aggiornamento, contattare l'assistenza tecnica per indagare e correggere eventuali problemi sottostanti.

L'acquisizione o il recupero dei dati è interrotto

Se l'acquisizione o il recupero dei dati viene interrotto inaspettatamente quando non si sta aggiornando un nodo della griglia, contattare l'assistenza tecnica.

Errori di aggiornamento del database

Se l'aggiornamento del database fallisce e si verifica un errore, riprovare. Se il problema persiste, contattare l'assistenza tecnica.

Informazioni correlate

["Controllo delle condizioni del sistema prima di aggiornare il software"](#)

Problemi dell'interfaccia utente

Durante o dopo l'aggiornamento potrebbero verificarsi problemi con Grid Manager o Tenant Manager.

Grid Manager visualizza più messaggi di errore durante l'aggiornamento

Se aggiorni il browser o passi a un'altra pagina di Grid Manager mentre è in corso l'aggiornamento del nodo di amministrazione principale, potresti visualizzare più messaggi "503: Servizio non disponibile" e "Problema di connessione al server". Puoi tranquillamente ignorare questi messaggi: non appariranno più non appena il nodo sarà 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 l'assistenza tecnica.

L'interfaccia web non risponde come previsto

Dopo l'aggiornamento del software StorageGRID, Grid Manager o Tenant Manager potrebbero non rispondere come previsto.

Se riscontri problemi con l'interfaccia web:

- Assicurati di utilizzare un ["browser web supportato"](#).



In genere, il supporto del browser cambia per ogni versione StorageGRID.

- Svuota la cache del tuo browser web.

La cancellazione della cache rimuove le risorse obsolete utilizzate dalla versione precedente del software StorageGRID e consente all'interfaccia utente di funzionare di nuovo correttamente. Per le istruzioni, consultare la documentazione del browser web.

Messaggi di errore "Controllo della disponibilità dell'immagine Docker"

Quando si tenta di avviare il processo di aggiornamento, è possibile che venga visualizzato un messaggio di errore che indica "I seguenti problemi sono stati identificati dalla suite di convalida del controllo della disponibilità delle immagini Docker". Prima di poter completare l'aggiornamento, è necessario risolvere tutti i problemi.

Se non sei sicuro delle modifiche necessarie per risolvere i problemi identificati, contatta l'assistenza tecnica.

Messaggio	Causa	Soluzione
Impossibile determinare la versione dell'aggiornamento. File di informazioni sulla versione di aggiornamento {file_path} non corrispondeva al formato previsto.	Il pacchetto di aggiornamento è danneggiato.	Ricarica il pacchetto di aggiornamento e riprova. Se il problema persiste, contattare l'assistenza tecnica.
File di informazioni sulla versione di aggiornamento {file_path} non è stato trovato. Impossibile determinare la versione dell'aggiornamento.	Il pacchetto di aggiornamento è danneggiato.	Ricarica il pacchetto di aggiornamento e riprova. Se il problema persiste, contattare l'assistenza tecnica.
Impossibile determinare la versione di rilascio attualmente installata su {node_name} .	Un file critico sul nodo è danneggiato.	Contattare l'assistenza tecnica.
Errore di connessione durante il tentativo di elencare le versioni su {node_name}	Il nodo è offline oppure la connessione è stata interrotta.	Verificare che tutti i nodi siano online e raggiungibili dal nodo di amministrazione primario, quindi riprovare.
L'host per il nodo {node_name} non ha StorageGRID {upgrade_version} immagine caricata. Prima di poter 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 su 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.	Verificare 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 immagine. Attendi qualche minuto e riprova. Vedere "Linux: installa il pacchetto RPM o DEB su tutti gli host" .
Errore durante il controllo del nodo {node_name}	Si è verificato un errore imprevisto.	Attendi qualche minuto e riprova.
Errore non rilevato durante l'esecuzione dei controlli preliminari. {error_string}	Si è verificato un errore imprevisto.	Attendi qualche minuto e riprova.

Applica l'hotfix StorageGRID

Procedura di hotfix di StorageGRID

Potrebbe essere necessario applicare un hotfix al sistema StorageGRID se vengono rilevati e risolti problemi con il software tra un rilascio e l'altro delle funzionalità.

Gli hotfix StorageGRID contengono modifiche software rese disponibili al di fuori di una release di funzionalità o patch. Le stesse modifiche saranno incluse in una versione futura. Inoltre, ogni versione di hotfix contiene un riepilogo di tutti gli hotfix precedenti presenti nella versione di funzionalità o patch.

Considerazioni per l'applicazione di un hotfix

Non è possibile applicare un hotfix StorageGRID quando è in esecuzione un'altra procedura di manutenzione. Ad esempio, non è possibile applicare un hotfix mentre è in esecuzione una procedura di dismissione, espansione o ripristino.



Se una procedura di dismissione di un nodo o di un sito viene sospesa, è possibile applicare in tutta sicurezza un hotfix. Inoltre, potresti essere in grado di applicare un hotfix durante le fasi finali di una procedura di aggiornamento StorageGRID. Per maggiori dettagli, consultare le istruzioni per l'aggiornamento del software StorageGRID.

Dopo aver caricato l'hotfix in Grid Manager, l'hotfix viene applicato automaticamente al nodo di amministrazione primario. Successivamente, puoi approvare l'applicazione dell'hotfix al resto dei nodi nel tuo sistema StorageGRID.

Se un hotfix non riesce ad essere applicato a uno o più nodi, il motivo dell'errore viene visualizzato nella colonna Dettagli della tabella di avanzamento dell'hotfix. È necessario risolvere i problemi che hanno causato gli errori e quindi ripetere l'intero processo. I nodi su cui è stata precedentemente applicata correttamente la correzione rapida verranno ignorati nelle applicazioni successive. È possibile ripetere in tutta sicurezza il processo di hotfix tutte le volte che si desidera, finché tutti i nodi non saranno stati aggiornati. Affinché l'applicazione sia completa, è necessario che l'hotfix sia installato correttamente su tutti i nodi della griglia.

Sebbene i nodi della griglia vengano aggiornati con la nuova versione dell'hotfix, le modifiche effettive in un hotfix potrebbero interessare solo servizi specifici su tipi specifici di nodi. Ad esempio, un hotfix potrebbe interessare solo il servizio LDR sui nodi di archiviazione.

Come vengono applicati gli hotfix per il ripristino e l'espansione

Dopo che un hotfix è stato applicato alla griglia, il nodo di amministrazione primario installa automaticamente la stessa versione dell'hotfix su tutti i nodi ripristinati tramite operazioni di ripristino o aggiunti in un'espansione.

Tuttavia, se è necessario ripristinare il nodo di amministrazione primario, è necessario installare manualmente la versione corretta StorageGRID e quindi applicare l'hotfix. La versione finale StorageGRID del nodo di amministrazione primario deve corrispondere alla versione degli altri nodi nella griglia.

L'esempio seguente illustra come applicare un hotfix durante il ripristino del nodo di amministrazione primario:

1. Supponiamo che la griglia esegua una versione StorageGRID 11.A.B con l'ultimo hotfix. La "versione griglia" è 11.A.B.y.
2. Il nodo di amministrazione primario non funziona.
3. Si ridistribuisce il nodo di amministrazione primario utilizzando StorageGRID 11.A.B ed si esegue la

procedura di ripristino.



Se necessario, per adattare la versione della griglia, è possibile utilizzare una versione secondaria durante la distribuzione del nodo; non è necessario distribuire prima la versione principale.

4. Quindi si applica l'hotfix 11.A.B.y al nodo di amministrazione primario.

Per ulteriori informazioni, consultare ["Configura il nodo di amministrazione primario sostitutivo"](#).

Come viene influenzato il tuo sistema quando applichi un hotfix

È necessario comprendere in che modo l'applicazione di un hotfix inciderà sul sistema StorageGRID.

Gli hotfix StorageGRID non sono dirompenti

Il sistema StorageGRID può acquisire e recuperare dati dalle applicazioni client durante l'intero processo di hotfix. Se si approva l'aggiornamento rapido di tutti i nodi dello stesso tipo (ad esempio, nodi di archiviazione), i nodi vengono disattivati uno alla volta, quindi non c'è un momento in cui tutti i nodi della griglia o tutti i nodi della griglia di un certo tipo non sono disponibili.

Per garantire una disponibilità continua, assicurati che la policy ILM contenga regole che specifichino l'archiviazione di più copie di ciascun oggetto. È inoltre necessario assicurarsi che tutti i client S3 esterni siano configurati per inviare richieste a uno dei seguenti:

- Un indirizzo IP virtuale di gruppo ad alta disponibilità (HA)
- Un bilanciatore di carico di terze parti ad alta disponibilità
- Più nodi gateway per ogni client
- Più nodi di archiviazione per ogni client

Le applicazioni client potrebbero subire interruzioni a breve termine

Il sistema StorageGRID può acquisire e recuperare dati dalle applicazioni client durante l'intero processo di hotfix; tuttavia, le connessioni client ai singoli nodi gateway o nodi di archiviazione potrebbero essere temporaneamente interrotte se l'hotfix richiede il riavvio dei servizi su tali nodi. La connettività verrà ripristinata al termine del processo di hotfix e i servizi saranno ripresi sui singoli nodi.

Potrebbe essere necessario pianificare un periodo di inattività per applicare un hotfix se la perdita di connettività per un breve periodo non è accettabile. È possibile utilizzare l'approvazione selettiva per pianificare quando aggiornare determinati nodi.



È possibile utilizzare più gateway e gruppi ad alta disponibilità (HA) per garantire il failover automatico durante il processo di hotfix. Vedi 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 quando i servizi vengono riavviati e quando il sistema StorageGRID funziona come ambiente a versione mista (alcuni nodi della griglia eseguono una versione precedente, mentre altri sono stati aggiornati a una versione successiva). In genere, questi avvisi e notifiche scompariranno al termine dell'hotfix.

Le modifiche alla configurazione sono limitate

Quando si applica un hotfix a StorageGRID:

- Non apportare modifiche alla configurazione della griglia (ad esempio, specificando le subnet della rete della griglia o approvando i nodi della griglia in sospeso) finché l'hotfix non è stato applicato a tutti i nodi.
- Non aggiornare la configurazione ILM finché l'hotfix non è stato applicato a tutti i nodi.

Ottieni i materiali necessari per l'hotfix

Prima di applicare un hotfix, è necessario procurarsi tutti i materiali necessari.

Articolo	Note
File di hotfix StorageGRID	È necessario scaricare il file hotfix StorageGRID .
• Porta di rete • "Browser web supportato" • Client SSH (ad esempio, PuTTY)	
Pacchetto di recupero(.zip) file	Prima di applicare un hotfix, "scarica il file del pacchetto di ripristino più recente" nel caso in cui si verifichino problemi durante l'hotfix. Quindi, dopo aver applicato l'hotfix, scaricare una nuova copia del file Recovery Package e salvarla 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 un hotfix manualmente tramite il client SSH. IL Passwords.txt il file fa parte del pacchetto di ripristino .zip file.
Frase segreta di provisioning	La passphrase viene creata e documentata quando il sistema StorageGRID viene installato per la prima volta. La passphrase di provisioning non è elencata in Passwords.txt file.
Documentazione correlata	readme.txt`file per l'hotfix. Questo file è incluso nella pagina di download dell'hotfix. Assicurati di rivedere il `readme limare con cura prima di applicare l'hotfix.

Scarica il file hotfix

È necessario scaricare il file hotfix prima di poterlo applicare.

Passi

1. Vai a ["Download NetApp : StorageGRID"](#) .
2. Selezionare la freccia rivolta verso il basso sotto **Software disponibile** per visualizzare un elenco degli 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 appena ["recuperato il nodo di amministrazione primario"](#) e devi applicare un hotfix, seleziona la stessa versione dell'hotfix installata sugli altri nodi della griglia.

- Seleziona la versione hotfix che desideri scaricare e seleziona **Vai**.
- Sign in utilizzando il nome utente e la password del tuo account NetApp .
- Leggere e accettare il Contratto di licenza con l'utente finale.

Viene visualizzata la pagina di download della versione selezionata.

- Scarica l'hotfix `readme.txt` file per visualizzare un riepilogo delle modifiche incluse nell'hotfix.

4. Selezionare il pulsante di download per l'hotfix e salvare il file.



Non modificare il nome di questo 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` estensione.

5. Seleziona una posizione per il download e seleziona **Salva**.

Controllare le condizioni del sistema prima di applicare l'hotfix

È necessario verificare che il sistema sia pronto ad accogliere l'hotfix.

- Sign in a Grid Manager utilizzando un ["browser web supportato"](#) .
- Se possibile, assicurarsi che il sistema funzioni normalmente e che tutti i nodi della rete siano collegati alla rete.

I nodi connessi hanno segni di spunta verdi  nella pagina Nodi.

- Se possibile, verificare la presenza di eventuali avvisi in corso e risolverli.
- Assicurarsi che non siano in corso altre procedure di manutenzione, come ad esempio aggiornamenti, ripristini, espansioni o dismissioni.

Prima di applicare un hotfix, è opportuno attendere il completamento di eventuali procedure di manutenzione attive.

Non è possibile applicare un hotfix StorageGRID quando è in esecuzione un'altra procedura di manutenzione. Ad esempio, non è possibile applicare un hotfix mentre è in esecuzione una procedura di dismissione, espansione o ripristino.



Se un nodo o un sito ["la procedura di dismissione è sospesa"](#) , puoi applicare in tutta sicurezza un hotfix. Inoltre, potresti essere in grado di applicare un hotfix durante le fasi finali di una procedura di aggiornamento StorageGRID . Vedi le istruzioni per ["aggiornamento del software StorageGRID"](#) .

Applica hotfix

L'hotfix viene applicato automaticamente al nodo di amministrazione primario. Quindi, è necessario approvare l'applicazione dell'hotfix ad altri nodi della griglia finché tutti i nodi non eseguono la stessa versione del software. È possibile personalizzare la sequenza di approvazione scegliendo di 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 un hotfix"](#).
- Hai la passphrase di provisioning.
- Hai accesso Root o autorizzazione di Manutenzione.

Informazioni su questo compito

- È possibile ritardare l'applicazione di un hotfix a un nodo, ma il processo di hotfix non sarà completo finché non si applica l'hotfix a tutti i nodi.
- Non è possibile eseguire un aggiornamento del software StorageGRID o un aggiornamento del sistema operativo SANtricity finché non è stato completato il processo di hotfix.

Passi

1. Sign in a Grid Manager utilizzando un ["browser web supportato"](#).
2. Selezionare **MANUTENZIONE > Sistema > Aggiornamento software**.

Viene visualizzata la pagina Aggiornamento software.

Software update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances. NetApp recommends you apply the latest hotfix before and after each software upgrade. Some hotfixes are required to prevent data loss.

StorageGRID upgrade

Upgrade to the next StorageGRID version and apply the latest hotfix for that version.

Upgrade →

StorageGRID hotfix

Apply a hotfix to your current StorageGRID software version.

Apply hotfix →

SANtricity OS update

Update the SANtricity OS software on your StorageGRID storage appliances.

Update →

3. Selezionare **Applica hotfix**.

Viene visualizzata la pagina StorageGRID Hotfix.

StorageGRID Hotfix

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

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

Hotfix file

Hotfix file ?

Browse

Passphrase

Provisioning Passphrase ?

Start

4. Seleziona il file hotfix scaricato dal sito di supporto NetApp .

- a. Selezionare **Sfoglia**.
- b. Individua e seleziona il file.

`hotfix-install-version`

- c. Selezionare **Apri**.

Il file è caricato. Una volta completato il caricamento, il nome del file viene visualizzato nel campo Dettagli.



Non modificare il nome del file perché fa parte del processo di verifica.

5. Immettere la passphrase di provisioning nella casella di testo.

Il pulsante **Avvia** diventa attivo.

6. Selezionare **Avvia**.

Viene visualizzato un avviso che informa che la connessione del browser potrebbe interrompersi temporaneamente quando i servizi sul nodo di amministrazione primario vengono riavviati.

7. Selezionare **OK** per iniziare ad applicare l'hotfix al nodo di amministrazione primario.

Quando inizia l'hotfix:

- a. Vengono eseguite le convalide degli hotfix.



Se vengono segnalati errori, risolvetele, ricaricate il file hotfix e selezionate nuovamente **Avvia**.

- b. Viene visualizzata la tabella di avanzamento dell'installazione dell'hotfix.

Questa tabella mostra tutti i nodi nella griglia e la fase attuale dell'installazione dell'hotfix per ciascun nodo. I nodi nella tabella sono raggruppati per tipo (nodi amministrativi, nodi gateway e nodi di archiviazione).

- c. La barra di avanzamento raggiunge il completamento e il nodo di amministrazione primario viene visualizzato come "Completato".

Hotfix Installation Progress

[Approve All](#)
[Remove All](#)

Admin Nodes - 1 out of 1 completed

Search

Site	Name	Progress	Stage	Details	Action
Vancouver	VTC-ADM1-101-191		Complete		

8. Facoltativamente, ordina gli elenchi dei nodi in ciascun raggruppamento in ordine crescente o decrescente per **Sito**, **Nome**, **Avanzamento**, **Fase** o **Dettagli**. Oppure inserisci un termine nella casella **Cerca** per cercare nodi specifici.
9. Approva i nodi della griglia pronti per essere aggiornati. I nodi approvati dello stesso tipo vengono aggiornati uno alla volta.



Non approvare l'hotfix per un nodo a meno che tu non sia sicuro che il nodo sia pronto per essere aggiornato. Quando l'hotfix viene applicato a un nodo della griglia, alcuni servizi su quel 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 nodi individuali alla coda degli hotfix.
- Selezionare il pulsante **Approva tutto** all'interno di ciascun raggruppamento per aggiungere tutti i nodi dello stesso tipo alla coda degli hotfix. Se hai inserito 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 in 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 il/i nodo/i successivo/i.

- Selezionare il pulsante di primo livello **Approva tutto** nella parte superiore della pagina per aggiungere tutti i nodi nella griglia alla coda degli hotfix.



È necessario completare l'hotfix StorageGRID prima di poter avviare un aggiornamento software diverso. Se non riesci a completare l'hotfix, contatta l'assistenza tecnica.

- Selezionare **Rimuovi** o **Rimuovi tutto** per rimuovere un nodo o tutti i nodi dalla coda degli hotfix.

Quando la fase supera "In coda", il pulsante **Rimuovi** viene nascosto e non è più possibile rimuovere il nodo dal processo di hotfix.

Storage Nodes - 1 out of 9 completed
Approve All
Remove All

Site	Name	Progress	Stage	Details	Action
Raleigh	RAL-S1-101-196		Queued		Remove
Raleigh	RAL-S2-101-197		Complete		
Raleigh	RAL-S3-101-198		Queued		Remove
Sunnyvale	SVL-S1-101-199		Queued		Remove
Sunnyvale	SVL-S2-101-93		Waiting for you to approve		Approve
Sunnyvale	SVL-S3-101-94		Waiting for you to approve		Approve
Vancouver	VTC-S1-101-193		Waiting for you to approve		Approve
Vancouver	VTC-S2-101-194		Waiting for you to approve		Approve
Vancouver	VTC-S3-101-195		Waiting for you to approve		Approve

10. Attendi che l'hotfix venga applicato a ciascun nodo della griglia approvato.

Una volta installata correttamente la correzione su tutti i nodi, la tabella Avanzamento installazione correzione si chiude. Un banner verde mostra la data e l'ora in cui è stato completato l'hotfix.

11. Se non è stato possibile applicare l'hotfix a nessun nodo, rivedere l'errore per ciascun nodo, risolvere il problema e ripetere questi passaggi.

La procedura non sarà completa finché l'hotfix non sarà applicato correttamente a tutti i nodi. È possibile ripetere in tutta sicurezza il processo di hotfix tutte le volte che si desidera, fino al suo completamento.

Configurare e gestire un sistema StorageGRID

Amministra StorageGRID

Amministra StorageGRID

Utilizzare queste istruzioni per configurare e amministrare un sistema StorageGRID .

Informazioni su queste istruzioni

Le attività principali per la configurazione e l'amministrazione StorageGRID consentono di:

- Utilizzare Grid Manager per impostare gruppi e utenti
- Creare account tenant per consentire alle applicazioni client S3 di archiviare e recuperare oggetti
- Configurare e gestire le reti StorageGRID
- Configura AutoSupport
- Gestisci le impostazioni del nodo

Prima di iniziare

- Hai una conoscenza generale del sistema StorageGRID .
- Hai una conoscenza abbastanza approfondita delle shell dei comandi Linux, delle reti e della configurazione e installazione dell'hardware del server.

Inizia 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

Dovresti impostare la larghezza consigliata per la finestra del browser.

Larghezza del browser	Pixel
Minimo	1024
Ottimale	1280

Sign in a Grid Manager

Per accedere alla pagina di accesso di Grid Manager, è necessario immettere il nome di dominio completo (FQDN) o l'indirizzo IP di un nodo di amministrazione nella barra degli indirizzi di un browser Web supportato.

Ogni sistema StorageGRID include un nodo amministrativo primario e un numero qualsiasi di nodi amministrativi non primari. È possibile accedere a Grid Manager su qualsiasi nodo di amministrazione per gestire il sistema StorageGRID. Tuttavia, alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

Connettiti al gruppo HA

Se i nodi amministrativi sono inclusi in un gruppo ad alta disponibilità (HA), la connessione avviene tramite l'indirizzo IP virtuale del gruppo HA o un nome di dominio completo mappato all'indirizzo IP virtuale. Il nodo di amministrazione primario dovrebbe essere selezionato come interfaccia primaria del gruppo, in modo che quando si accede a Grid Manager, si acceda al nodo di amministrazione primario, a meno che il nodo di amministrazione primario non sia disponibile. Vedere ["Gestire gruppi ad alta disponibilità"](#).

Utilizzare SSO

I passaggi di accesso sono leggermente diversi se ["è stato configurato l'accesso singolo \(SSO\)"](#).

Sign in a Grid Manager sul primo nodo di amministrazione

Prima di iniziare

- Hai le tue credenziali di accesso.
- Stai utilizzando un ["browser web supportato"](#).
- I cookie sono abilitati nel tuo browser web.
- Appartieni a un gruppo di utenti che ha 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 di amministrazione o l'indirizzo IP virtuale di un gruppo HA di nodi di amministrazione.

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 riservata di Grid Manager. È necessario utilizzare la porta 443.

Passi

1. Avviare un browser web supportato.
2. Nella barra degli indirizzi del browser, inserisci l'URL di Grid Manager.
3. Se viene visualizzato un avviso di sicurezza, installare il certificato utilizzando la procedura guidata di installazione del browser. Vedere ["Gestire i certificati di sicurezza"](#).

4. Sign in a Grid Manager.

La schermata di accesso visualizzata dipende dalla configurazione dell'accesso singolo (SSO) per StorageGRID.

Non si utilizza SSO

- a. Inserisci il tuo nome utente e la password per Grid Manager.
- b. Seleziona **Accedi**.



The screenshot shows the NetApp StorageGRID Grid Manager login interface. At the top, the NetApp logo is followed by 'StorageGRID®' and 'Grid Manager' in a large font. Below this, there are two input fields: 'Username' and 'Password'. The 'Username' field has a blue border and a cursor. Below the 'Password' field is a blue 'Sign in' button. At the bottom, there are three links: 'Tenant sign in', 'NetApp support', and 'NetApp.com'.

Utilizzo di SSO

- Se StorageGRID utilizza SSO e questa è la prima volta che accedi all'URL su questo browser:
 - i. Seleziona * Sign in*. Puoi lasciare lo 0 nel campo Account.



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Inserisci le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione. Per esempio:

Sign in with your organizational account

Sign in

- Se StorageGRID utilizza SSO e in precedenza hai effettuato l'accesso a Grid Manager o a un account tenant:
 - i. Inserisci **0** (ID account per Grid Manager) oppure seleziona **Grid Manager** se compare nell'elenco degli account recenti.

The image shows a web interface for NetApp StorageGRID. At the top, there is a logo consisting of a square icon followed by the text "NetApp StorageGRID®". Below the logo, the heading "Sign in" is displayed in a large, bold font. Underneath the heading, there is a section labeled "Recent" with a dropdown menu showing "Grid Manager". Below this, there is a section labeled "Account" with a text input field containing the character "0". A blue button with the text "Sign in" is positioned below the input field. At the bottom of the form, there is a link that reads "NetApp support | NetApp.com".

NetApp StorageGRID®

Sign in

Recent

Grid Manager ▼

Account

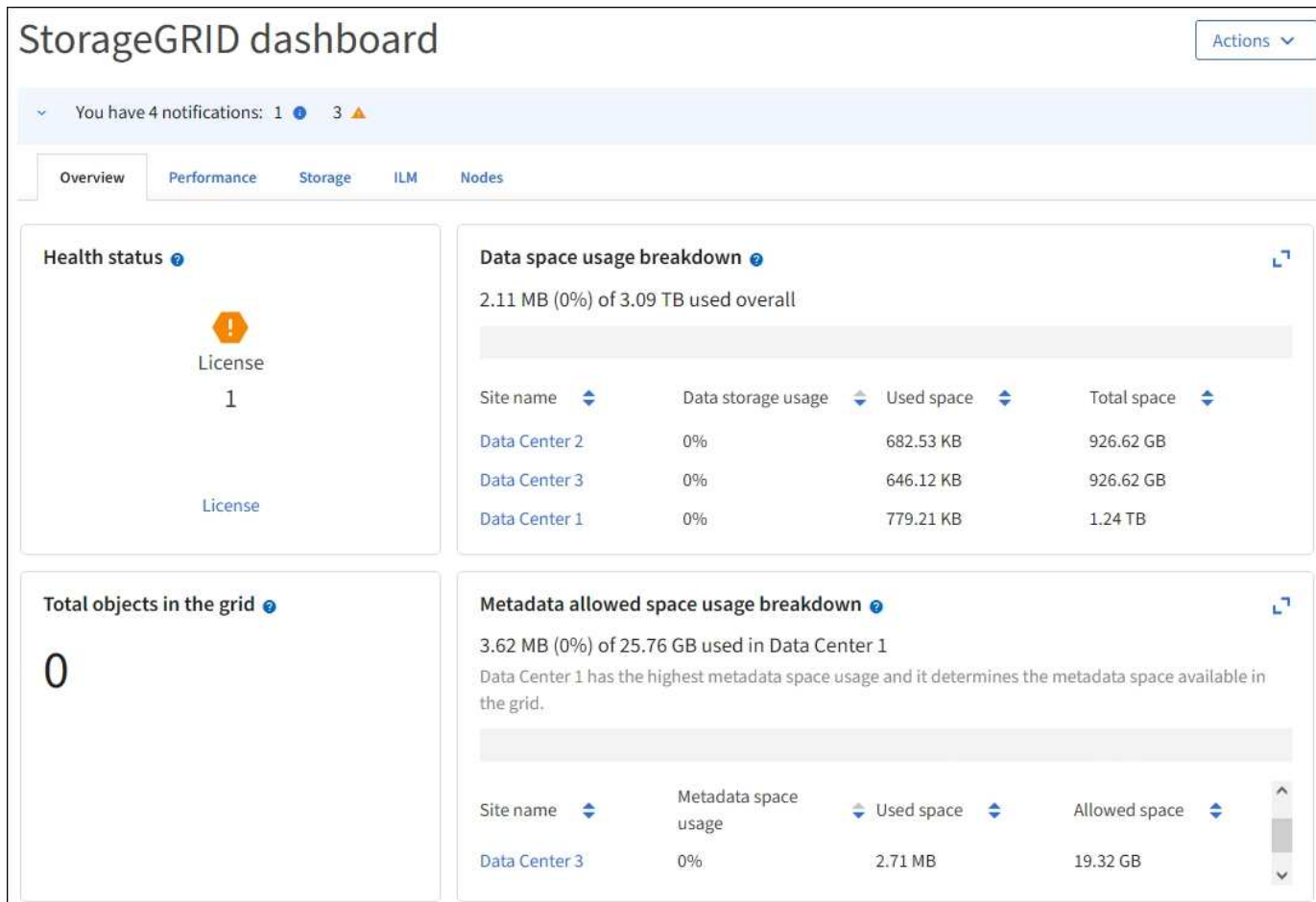
0

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Seleziona * Sign in*.
- iii. Sign in con le tue credenziali SSO standard alla pagina di accesso SSO della tua organizzazione.

Dopo aver effettuato l'accesso, viene visualizzata la home page di Grid Manager, che include la dashboard. Per sapere quali informazioni sono fornite, vedere "[Visualizza e gestisci la dashboard](#)".



Accedi a un altro nodo di amministrazione

Per accedere a un altro nodo di amministrazione, seguire questi passaggi.

Non si utilizza SSO

Passi

1. Nella barra degli indirizzi del browser, inserisci il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Includere il numero di porta, se necessario.
2. Inserisci il tuo nome utente e la password per Grid Manager.
3. Seleziona **Accedi**.

Utilizzo di SSO

Se StorageGRID utilizza SSO e hai effettuato l'accesso a un nodo amministrativo, puoi accedere ad altri nodi amministrativi senza dover effettuare nuovamente l'accesso.

Passi

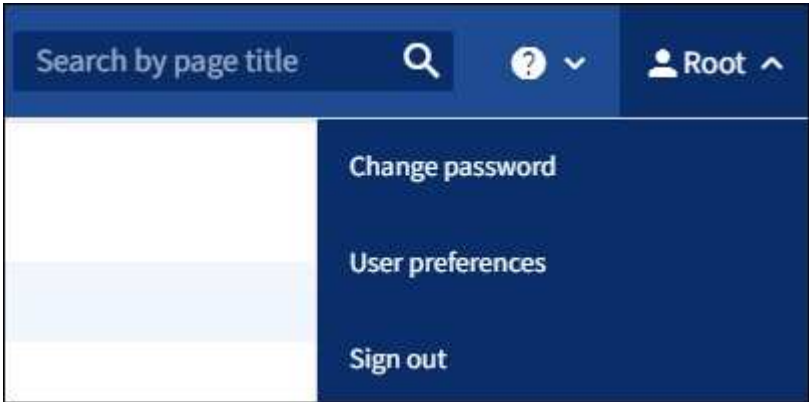
1. Inserisci il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione nella barra degli indirizzi del browser.
2. Se la sessione SSO è scaduta, inserisci nuovamente le tue credenziali.

Esci da Grid Manager

Una volta terminato di lavorare con Grid Manager, è necessario disconnettersi per impedire agli utenti non autorizzati di accedere al sistema StorageGRID . In base alle impostazioni dei cookie del browser, la chiusura del browser potrebbe non comportare la disconnessione dal sistema.

Passi

- 1. Seleziona il tuo nome utente nell'angolo in alto a destra.



- 2. Seleziona **Esci**.

Opzione	Descrizione
SSO non in uso	Hai effettuato la disconnessione dal nodo di amministrazione. Viene visualizzata la pagina di accesso di Grid Manager. Nota: se hai effettuato l'accesso a più di un nodo di amministrazione, devi disconnetterti da ciascun nodo.
SSO abilitato	Hai effettuato l'uscita da tutti i nodi amministrativi a cui stavi accedendo. Viene visualizzata la pagina di accesso a StorageGRID . Grid Manager è elencato come predefinito nel menu a discesa Account recenti e il campo ID account mostra 0. Nota: se l'SSO è abilitato e hai effettuato l'accesso anche a Tenant Manager, devi anche "uscire dall'account dell'inquilino" A "uscire da SSO" .

Cambia la tua password

Se sei un utente locale di Grid Manager, puoi modificare la tua password.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

Informazioni su questo compito

Se accedi a StorageGRID come utente federato o se è abilitato l'accesso singolo (SSO), non puoi modificare

la password in Grid Manager. In alternativa, è necessario modificare la password nella fonte di identità esterna, ad esempio Active Directory o OpenLDAP.

Passi

1. Dall'interfaccia Grid Manager, seleziona **il tuo nome** > **Cambia password**.
2. Inserisci la tua password attuale.
3. Digita una nuova password.

La password deve contenere almeno 8 e non più di 32 caratteri. Le password sono sensibili alle maiuscole e alle minuscole.

4. Reinserisci la nuova password.
5. Seleziona **Salva**.

Visualizza le informazioni sulla licenza StorageGRID

Ogni volta che è necessario, è possibile visualizzare le informazioni sulla licenza del sistema StorageGRID , ad esempio la capacità di archiviazione massima della griglia.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

Informazioni su questo compito

Se si verifica un problema con la licenza software per questo sistema StorageGRID , la scheda Stato di integrità nella dashboard include un'icona Stato licenza e un collegamento **Licenza**. Il numero indica il numero di problemi relativi alla licenza.



Passi

1. Accedi alla pagina Licenza eseguendo una delle seguenti operazioni:
 - Selezionare **MANUTENZIONE** > **Sistema** > **Licenza**.
 - Dalla scheda Stato di integrità nella dashboard, seleziona l'icona Stato licenza o il collegamento **Licenza**.

Questo collegamento appare solo se c'è un problema con la licenza.

2. Visualizza i dettagli di sola lettura per la licenza corrente:

- ID di sistema StorageGRID , ovvero il numero di identificazione univoco per questa installazione StorageGRID
- Numero di serie della licenza
- Tipo di licenza, **Perpetua** o **Abbonamento**
- Capacità di stoccaggio autorizzata della rete
- Capacità di archiviazione supportata
- Data di scadenza della licenza. **N/D** appare per una licenza perpetua.
- Data di fine del supporto

Questa data viene letta dal file di licenza corrente e potrebbe non essere aggiornata se hai esteso o rinnovato il contratto di assistenza dopo aver ottenuto il file di licenza. Per aggiornare questo valore, vedere ["Aggiorna le informazioni sulla licenza StorageGRID"](#) . È anche possibile visualizzare la data di fine effettiva del contratto utilizzando Active IQ.

- Contenuto del file di testo della licenza

Aggiorna le informazioni sulla licenza StorageGRID

È necessario aggiornare le informazioni sulla licenza del sistema StorageGRID ogni volta che cambiano i termini della licenza. Ad esempio, è necessario aggiornare le informazioni sulla licenza se si acquista capacità di archiviazione aggiuntiva per la propria rete.

Prima di iniziare

- Hai un nuovo file di licenza da applicare al tuo sistema StorageGRID .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Hai la passphrase di provisioning.

Passi

1. Selezionare **MANUTENZIONE > Sistema > Licenza**.
2. Nella sezione Aggiorna licenza, seleziona **Sfoglia**.
3. Individuare e selezionare il nuovo file di licenza(.txt).

Il nuovo file di licenza viene convalidato e visualizzato.

4. Immettere la passphrase di provisioning.
5. Seleziona **Salva**.

Utilizzare la API

Utilizzare l'API di gestione della griglia

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Grid Management anziché l'interfaccia utente di Grid Manager. Ad esempio, potresti voler utilizzare l'API per automatizzare le operazioni o per creare più entità, come gli utenti, più rapidamente.

Risorse di alto livello

L'API di gestione della griglia 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 maggiori dettagli, 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. Anche gli endpoint privati StorageGRID ignorano la versione API della richiesta.

Inviare richieste API

L'API Grid Management utilizza la piattaforma API open source Swagger. Swagger fornisce un'interfaccia utente intuitiva che consente agli sviluppatori e ai non sviluppatori di eseguire operazioni in tempo reale in StorageGRID tramite l'API.

L'interfaccia utente di Swagger fornisce dettagli e documentazione completi per ogni operazione API.

Prima di iniziare

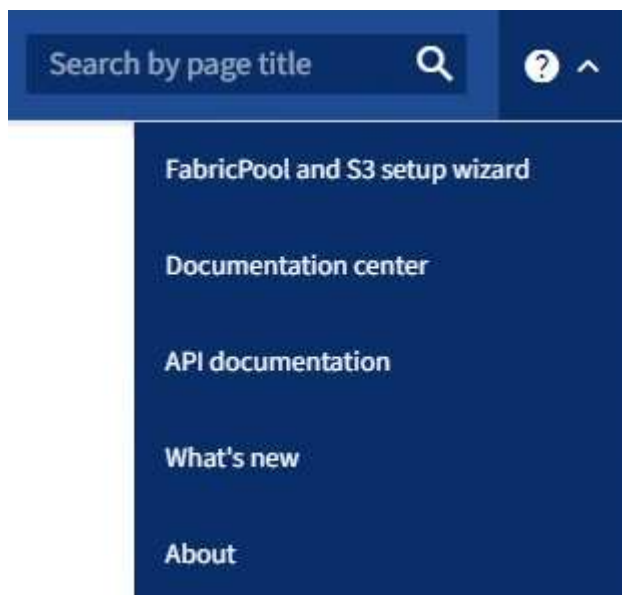
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).



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

Passi

1. Dall'interfaccia di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API**.



2. Per eseguire un'operazione con l'API privata, seleziona **Vai alla documentazione dell'API privata** nella pagina dell'API di gestione StorageGRID.

Le API private sono soggette a modifiche senza preavviso. Anche gli endpoint privati StorageGRID

ignorano la versione API della richiesta.

3. Selezionare l'operazione desiderata.

Quando si espande un'operazione API, è possibile visualizzare le azioni HTTP disponibili, come GET, PUT, UPDATE e 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.

groups Operations on groups

GET /grid/groups Lists Grid Administrator Groups

Parameters Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated --
limit integer (query)	maximum number of results Default value : 25 25
marker string (query)	marker-style pagination offset (value is Group's URN) marker - marker-style pagination offset (value
includeMarker boolean (query)	If set, the marker element is also returned --
order string (query)	pagination order (desc requires marker) Available values : asc, desc --

Responses Response content type application/json

Code	Description
200	successfully retrieved Example Value Model <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers",</pre>

5. Determina se la richiesta richiede parametri aggiuntivi, come un gruppo o un ID utente. Quindi, ottieni questi valori. Potrebbe essere necessario inviare prima una richiesta API diversa per ottenere le

informazioni necessarie.

6. Determina se è necessario modificare il corpo della richiesta di esempio. In tal caso, puoi selezionare **Modello** per conoscere i requisiti per ciascun campo.
7. Seleziona **Provalo**.
8. Fornire tutti i parametri richiesti o modificare il corpo della richiesta come richiesto.
9. Selezionare **Esegui**.
10. Esaminare il codice di risposta per determinare se la richiesta è andata a buon fine.

Operazioni dell'API di gestione della griglia

L'API di gestione della griglia organizza le operazioni disponibili nelle seguenti sezioni.



Questo elenco include solo le operazioni disponibili nell'API pubblica.

- **account**: operazioni per gestire gli account dei tenant di archiviazione, tra cui la creazione di nuovi account e il recupero dell'utilizzo dello spazio di archiviazione per un determinato account.
- **alert-history**: Operazioni sugli avvisi risolti.
- **alert-receivers**: Operazioni sui destinatari delle notifiche di avviso (e-mail).
- **alert-rules**: Operazioni sulle regole di avviso.
- **alert-silences**: Operazioni sui silenzi degli avvisi.
- **avvisi**: Operazioni sugli avvisi.
- **audit**: Operazioni per elencare e aggiornare la configurazione di audit.
- **auth**: Operazioni per eseguire l'autenticazione della sessione utente.

L'API di gestione della griglia supporta lo schema di autenticazione Bearer Token. Per effettuare l'accesso, è necessario fornire 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 successive richieste API ("`Authorization: Bearer token`"). Il token scade dopo 16 ore.



Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On, è necessario eseguire diversi passaggi per l'autenticazione. Vedere "Autenticazione all'API se è abilitato l'accesso singolo".

Per informazioni su come migliorare la sicurezza dell'autenticazione, vedere "Protezione contro la falsificazione delle richieste tra siti".

- **client-certificates**: Operazioni per configurare i certificati client in modo che StorageGRID sia accessibile in modo sicuro tramite strumenti di monitoraggio esterni.
- **config**: Operazioni relative alla versione del prodotto e alle versioni dell'API di gestione della griglia. È possibile elencare la versione di rilascio del prodotto e le versioni principali dell'API Grid Management supportate da tale versione, nonché disabilitare le versioni obsolete dell'API.
- **deactivated-features**: Operazioni per visualizzare le funzionalità che potrebbero essere state disattivate.
- **dns-servers**: Operazioni per elencare e modificare i server DNS esterni configurati.
- **drive-details**: Operazioni sulle unità per modelli specifici di dispositivi di archiviazione.

- **endpoint-domain-names**: Operazioni per elencare e modificare i nomi di dominio degli endpoint S3.
- **erasure-coding**: Operazioni sui profili di codifica di cancellazione.
- **espansione**: Operazioni di espansione (a livello di procedura).
- **expansion-nodes**: 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 delle reti di griglia.
- **grid-passwords**: Operazioni per la gestione delle password della griglia.
- **gruppi**: operazioni per gestire i gruppi di amministratori di griglia locali e per recuperare i gruppi di amministratori di griglia federati da un server LDAP esterno.
- **identity-source**: Operazioni per configurare una fonte di identità esterna e per sincronizzare manualmente le informazioni sui gruppi federati e sugli utenti.
- **ilm**: Operazioni sulla gestione del ciclo di vita delle informazioni (ILM).
- **in-progress-procedures**: 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 registro.
- **metriche**: operazioni sulle metriche StorageGRID , tra cui query di metriche istantanee in un singolo punto nel tempo e query di metriche di intervallo in un intervallo di tempo. L'API di gestione della griglia utilizza lo strumento di monitoraggio dei sistemi Prometheus come fonte di dati backend. Per informazioni sulla creazione di query Prometheus, consultare il sito web di Prometheus.



Metriche che includono *private* nei loro nomi sono destinati esclusivamente all'uso interno. Queste metriche sono soggette a modifiche tra le versioni StorageGRID senza preavviso.

- **node-details**: Operazioni sui dettagli del nodo.
- **node-health**: Operazioni sullo stato di integrità del nodo.
- **node-storage-state**: Operazioni sullo stato di archiviazione del nodo.
- **nntp-servers**: operazioni per elencare o aggiornare i server NTP (Network Time Protocol) esterni.
- **oggetti**: Operazioni sugli oggetti e sui metadati degli oggetti.
- **recovery**: Operazioni per la procedura di recupero.
- **recovery-package**: Operazioni per scaricare il pacchetto di ripristino.
- **regioni**: Operazioni per visualizzare e creare regioni.
- **s3-object-lock**: Operazioni sulle impostazioni globali di S3 Object Lock.
- **server-certificate**: Operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp**: Operazioni sulla configurazione SNMP corrente.
- **storage-watermarks**: Filigrane del nodo di archiviazione.
- **traffic-classes**: Operazioni per le policy di classificazione del traffico.
- **untrusted-client-network**: Operazioni sulla configurazione della rete client non attendibile.
- **utenti**: operazioni per visualizzare e gestire gli utenti di Grid Manager.

Controllo delle versioni dell'API di gestione della griglia

L'API di gestione della griglia 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 aggiornata quando vengono apportate modifiche che non sono compatibili con le versioni precedenti. La versione secondaria dell'API viene aggiornata quando vengono apportate modifiche *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o nuove proprietà.

L'esempio seguente illustra come la versione dell'API viene aumentata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Vecchia versione	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con le versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene abilitata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova versione delle funzionalità di StorageGRID, si continua ad avere accesso alla versione API precedente per almeno una versione delle funzionalità StorageGRID.



È possibile configurare le versioni supportate. Consultare la sezione **config** della documentazione dell'API Swagger per "[API di gestione della griglia](#)" per maggiori informazioni. Dopo aver aggiornato tutti i client API per utilizzare la versione più recente, è necessario disattivare il supporto per la versione precedente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Obsoleto: vero"
- Il corpo della risposta JSON include "deprecated": true
- Un avviso obsoleto è stato aggiunto a nms.log. Per esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determina quali versioni API sono supportate nella versione corrente

Utilizzare il GET `/versions` Richiesta API per restituire un elenco delle principali versioni 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 API utilizzando un parametro di percorso(/api/v4) o un'intestazione(Api-Version: 4). Se si specificano 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 falsificazione delle richieste tra siti (CSRF)

È possibile contribuire a proteggersi dagli attacchi CSRF (Cross-Site Request Forgery) 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 abilitarla o meno al momento dell'accesso.

Un aggressore in grado di attivare una richiesta a un sito diverso (ad esempio con un modulo HTTP POST) può far sì che determinate richieste vengano effettuate utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggersi dagli attacchi CSRF utilizzando i token CSRF. Se abilitato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro del corpo POST specifico.

Per abilitare 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 è impostato con un valore casuale per gli accessi a Grid Manager e `AccountCsrfToken` il cookie viene impostato con un valore casuale per gli accessi al Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere uno dei seguenti elementi:

- IL `X-Csrf-Token` intestazione, con il valore dell'intestazione impostato sul valore del cookie token CSRF.
- Per gli endpoint che accettano un corpo codificato in formato: A `csrfToken` parametro del corpo della richiesta codificato nel modulo.

Per ulteriori esempi e dettagli, consultare la documentazione API online.



Le richieste che hanno impostato un 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 abilitato l'accesso singolo

Utilizzare l'API se è abilitato l'accesso singolo (Active Directory)

Se hai ["configurato e abilitato l'accesso singolo \(SSO\)"](#) e si utilizza Active Directory come provider SSO, è necessario inviare una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso singolo

Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO.

Prima di iniziare

- Conosci il nome utente e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

Per ottenere un token di autenticazione, puoi utilizzare uno dei seguenti esempi:

- IL `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione StorageGRID(`./rpms` per Red Hat Enterprise Linux, `./debs` per Ubuntu o Debian, e `./vsphere` per VMware).

- Un esempio di flusso di lavoro delle richieste curl.

Il flusso di lavoro curl potrebbe interrompersi se eseguito troppo lentamente. Potresti visualizzare l'errore: `A valid SubjectConfirmation was not found on this Response`.



Il flusso di lavoro curl di esempio non protegge la password dalla visualizzazione da parte di altri utenti.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version`.

Passi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare il `storagegrid-ssoauth.py` Script Python. Vai al passaggio 2.
 - Utilizzare le richieste curl. Vai al passaggio 3.
2. Se vuoi usare il `storagegrid-ssoauth.py` script, passa lo script all'interprete Python ed esegui lo script.

Quando richiesto, immettere i valori per i seguenti argomenti:

- Il metodo SSO. Inserisci ADFS o adfs.
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID
- L'indirizzo per StorageGRID
- ID dell'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. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

3. Se si desidera utilizzare le richieste curl, attenersi alla seguente procedura.
 - a. Dichiarare le variabili necessarie per effettuare 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 di gestione della griglia, utilizzare 0 come TENANTACCOUNTID.

- b. Per ricevere un URL di autenticazione firmato, inviare una richiesta 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 saranno trasmessi 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 codificato in URL, ma non include il livello 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. Salva il SAMLRequest dalla risposta per utilizzarla nei comandi successivi.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

- d. Ottieni un URL completo che includa l'ID della richiesta client da AD FS.

Un'opzione è quella di 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&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salva l'ID della richiesta del client dalla risposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Invia le tue credenziali all'azione del modulo dalla risposta precedente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS restituisce un reindirizzamento 302, con informazioni aggiuntive nelle intestazioni.



Se l'autenticazione a più fattori (MFA) è abilitata per il tuo 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...UJikvo77sXPw%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. Salva il MSISAuth cookie dalla risposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Invia una richiesta GET alla posizione specificata con i cookie dal POST di autenticazione.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Le intestazioni della risposta conterranno informazioni sulla sessione AD FS per un successivo utilizzo in caso di disconnessione, mentre il corpo della risposta conterrà SAMLResponse in un campo modulo 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
XFXvWw3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDk0Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj01OVpcMQ==;
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="PHNhbwXwOlJlc3Bvb3N...1scDpsZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Salva il SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```


- j. Utilizzando il salvato `SAMLResponse`, crea uno `StorageGRID/api/saml-response` richiesta di generazione di un token di autenticazione `StorageGRID`.

Per `RelayState`, utilizzare l'ID dell'account tenant oppure utilizzare 0 se si desidera accedere all'API di gestione della griglia.

```
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. Salva il token di autenticazione nella risposta come `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi usare `MYTOKEN` per altre richieste, in modo simile a come utilizzeresti l'API se non si utilizzasse l'SSO.

Disconnettersi dall'API se è abilitato l'accesso singolo

Se è stato abilitato l'accesso singolo (SSO), è necessario inviare una serie di richieste API per disconnettersi dall'API di gestione della griglia o dall'API di gestione dei tenant. Queste istruzioni si applicano se si utilizza Active Directory come provider di identità SSO

Informazioni su questo compito

Se necessario, puoi disconnetterti dall'API `StorageGRID` effettuando il logout dalla pagina di disconnessione singola della tua organizzazione. In alternativa, è possibile attivare il single logout (SLO) da `StorageGRID`, che richiede un token portatore `StorageGRID` valido.

Passi

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%3D",
  "responseTime": "2018-11-20T22:20:30.839Z",
  "status": "success"
}
```

2. Salva 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 solo tramite API.

```
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 portatore StorageGRID .

L'eliminazione del token portatore StorageGRID funziona allo stesso modo dell'eliminazione senza SSO. Se non viene specificato `cookie "sso=true", l'utente viene disconnesso da StorageGRID senza che ciò influisca sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

UN 204 No Content la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```

Utilizzare l'API se è abilitato l'accesso Single Sign-On (Azure)

Se hai [configurato e abilitato l'accesso singolo \(SSO\)](#) e si utilizza Azure come provider SSO, è possibile utilizzare due script di esempio per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso Single Sign-On di Azure

Queste istruzioni si applicano se si utilizza Azure come provider di identità SSO

Prima di iniziare

- Conosci l'indirizzo email e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

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 StorageGRID(`./rpms` per Red Hat Enterprise Linux, `./debs` per Ubuntu o Debian, e `./vsphere` per VMware).

Per scrivere la tua integrazione API con Azure, consulta `storagegrid-ssoauth-azure.py` sceneggiatura. Lo script Python invia direttamente due richieste a StorageGRID (prima per ottenere SAMLRequest e poi per ottenere il token di autorizzazione) e chiama anche lo script Node.js per interagire con Azure ed eseguire le operazioni SSO.

Le operazioni SSO possono essere eseguite utilizzando una serie di richieste API, ma non è un'operazione semplice. Il modulo Puppeteer Node.js viene utilizzato per eseguire lo scraping dell'interfaccia Azure SSO.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version`.

Passi

1. Installare le dipendenze richieste, come segue:
 - a. Installa Node.js (vedi ["https://nodejs.org/en/download/"](https://nodejs.org/en/download/)).

b. Installa 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):

- L'indirizzo e-mail SSO utilizzato per accedere ad Azure
- L'indirizzo per StorageGRID
- ID dell'account tenant, se si desidera accedere all'API di gestione tenant

4. Quando richiesto, immettere la password e prepararsi a fornire un'autorizzazione MFA ad Azure, se richiesto.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*****

Watch for and approve a 2FA authorization request
*****
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



Lo script presuppone che l'autenticazione MFA venga eseguita tramite Microsoft Authenticator. Potrebbe essere necessario modificare lo script per supportare altre forme di MFA (ad esempio l'inserimento di un codice ricevuto in un messaggio di testo).

Il token di autorizzazione StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

Utilizzare l'API se è abilitato l'accesso singolo (PingFederate)

Se hai [configurato e abilitato l'accesso singolo \(SSO\)](#) e utilizzi PingFederate come provider SSO, devi inviare una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso singolo

Queste istruzioni si applicano se si utilizza PingFederate come provider di identità SSO

Prima di iniziare

- Conosci il nome utente e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

Per ottenere un token di autenticazione, puoi utilizzare uno dei seguenti esempi:

- IL `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione StorageGRID(`./rpms` per Red Hat Enterprise Linux, `./debs` per Ubuntu o Debian, e `./vsphere` per

VMware).

- Un esempio di flusso di lavoro delle richieste curl.

Il flusso di lavoro curl potrebbe interrompersi se eseguito troppo lentamente. Potresti visualizzare l'errore: `A valid SubjectConfirmation was not found on this Response.`



Il flusso di lavoro curl di esempio non protegge la password dalla visualizzazione da parte di altri utenti.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version.`

Passi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare il `storagegrid-ssoauth.py` Script Python. Vai al passaggio 2.
 - Utilizzare le richieste curl. Vai al passaggio 3.
2. Se vuoi usare il `storagegrid-ssoauth.py` script, passa lo script all'interprete Python ed esegui lo script.

Quando richiesto, immettere i valori per i seguenti argomenti:

- Il metodo SSO. È possibile immettere qualsiasi variante di "pingfederate" (PINGFEDERATE, pingfederate e così via).
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID . Questo campo non è utilizzato per PingFederate. Puoi lasciarlo vuoto o inserire qualsiasi valore.
- L'indirizzo per StorageGRID
- ID dell'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. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

3. Se si desidera utilizzare le richieste curl, attenersi alla seguente procedura.
 - a. Dichiarare le variabili necessarie per effettuare l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```



Per accedere all'API di gestione della griglia, utilizzare 0 come TENANTACCOUNTID.

- b. Per ricevere un URL di autenticazione firmato, inviare una richiesta 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 codificato in URL, ma non include il livello 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. Salva il SAMLRequest dalla risposta per utilizzarla nei comandi successivi.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Esporta la risposta e il cookie e ripeti la risposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Esporta il valore 'pf.adapterId' e riproduci la risposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Esporta il valore 'href' (rimuovi la barra finale /) e riproduci la risposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Esporta il valore 'azione':

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Invia i cookie insieme alle credenziali:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Salva il SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbwXwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizzando il salvato SAMLResponse , crea uno StorageGRID/api/saml-response richiesta di generazione di un token di autenticazione StorageGRID .

Per RelayState , utilizzare l'ID dell'account tenant oppure utilizzare 0 se si desidera accedere all'API di gestione della griglia.

```
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. Salva il token di autenticazione nella risposta come MYTOKEN .

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi usare MYTOKEN per altre richieste, in modo simile a come utilizzeresti l'API se non si utilizzasse l'SSO.

Disconnettersi dall'API se è abilitato l'accesso singolo

Se è stato abilitato l'accesso singolo (SSO), è necessario inviare una serie di richieste API per disconnettersi dall'API di gestione della griglia o dall'API di gestione dei tenant. Queste istruzioni si applicano se si utilizza PingFederate come provider di identità SSO

Informazioni su questo compito

Se necessario, puoi disconnetterti dall'API StorageGRID effettuando il logout dalla pagina di disconnessione singola della tua organizzazione. In alternativa, è possibile attivare il single logout (SLO) da StorageGRID, che richiede un token portatore StorageGRID valido.

Passi

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. Salva 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 solo tramite API.

```
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 portatore StorageGRID .

L'eliminazione del token portatore StorageGRID funziona allo stesso modo dell'eliminazione senza SSO. Se non viene specificato `cookie "sso=true", l'utente viene disconnesso da StorageGRID senza che ciò influisca sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

UN 204 No Content la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```

Disattivare le funzionalità con l'API

È possibile utilizzare l'API Grid Management per disattivare completamente determinate funzionalità nel sistema StorageGRID . Quando una funzionalità viene disattivata, a nessuno può essere assegnata l'autorizzazione per eseguire le attività correlate a tale funzionalità.

Informazioni su questo compito

Il sistema Funzionalità disattivate consente di impedire l'accesso a determinate funzionalità del sistema StorageGRID . La disattivazione di una funzionalità è l'unico modo per impedire all'utente root o agli utenti che appartengono a gruppi di amministratori con autorizzazione di **accesso root** di utilizzare tale funzionalità.

Per capire come questa funzionalità potrebbe essere utile, consideriamo il seguente scenario:

_La società A è un fornitore di servizi che affitta la capacità di archiviazione del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei propri locatari, la Società A desidera garantire che i propri dipendenti non possano mai accedere all'account di un locatario dopo che l'account è stato distribuito.

_L'azienda A può raggiungere questo obiettivo utilizzando il sistema Disattiva funzionalità nell'API di gestione della griglia. Disattivando completamente la funzionalità **Modifica password root del tenant** in Grid Manager (sia nell'interfaccia utente che nell'API), la Società A garantisce che gli utenti amministratori, inclusi l'utente root e gli utenti appartenenti a gruppi con autorizzazione di **Accesso root**, non possano modificare la password per l'utente root di alcun account tenant.

Passi

1. Accedi alla documentazione Swagger per l'API Grid Management. Vedere ["Utilizzare l'API di gestione della griglia"](#) .
2. Individuare l'endpoint Disattiva funzionalità.
3. Per disattivare una funzionalità, ad esempio Modifica password root del tenant, invia un corpo all'API in questo modo:

```
{ "grid": { "changeTenantRootPassword": true } }
```

Una volta completata la richiesta, la funzionalità Modifica password root del tenant viene disabilitata. L'autorizzazione di gestione **Modifica password root del tenant** non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password root per un tenant fallirà con "403 Forbidden".

Riattiva le funzionalità disattivate

Per impostazione predefinita, è possibile utilizzare l'API Grid Management per riattivare una funzionalità che è stata disattivata. Tuttavia, se si desidera impedire che le funzionalità disattivate vengano riattivate, è possibile disattivare la funzionalità **activateFeatures** stessa.



La funzione **activateFeatures** non può essere riattivata. Se decidi di disattivare questa funzione, tieni presente che perderai definitivamente la possibilità di riattivare qualsiasi altra funzione disattivata. Per ripristinare eventuali funzionalità perse è necessario contattare l'assistenza tecnica.

Passi

1. Accedi alla documentazione Swagger per l'API Grid Management.
2. Individuare l'endpoint Disattiva funzionalità.
3. Per riattivare tutte le funzionalità, invia un corpo all'API in questo modo:

```
{ "grid": null }
```

Una volta completata questa richiesta, tutte le funzionalità, inclusa la funzionalità Modifica password root del tenant, vengono riattivate. L'autorizzazione di gestione **Modifica password root del tenant** ora viene visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password root per un tenant avrà esito positivo, a condizione che l'utente disponga dell'autorizzazione di gestione **Accesso root** o **Modifica password root del tenant**.



L'esempio precedente fa sì che tutte le funzionalità disattivate vengano riattivate. Se sono state disattivate altre funzionalità che devono rimanere disattivate, è necessario specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzionalità Modifica password root del tenant e continuare a disattivare l'autorizzazione di gestione storageAdmin, inviare questa richiesta PUT:

```
{ "grid": {"storageAdmin": true} }
```

Controlla l'accesso a StorageGRID

Controllo dell'accesso a StorageGRID

È possibile controllare chi può accedere a StorageGRID e quali attività gli utenti possono eseguire creando o importando gruppi e utenti e assegnando autorizzazioni a ciascun gruppo. Facoltativamente, è possibile abilitare l'accesso singolo (SSO), creare certificati client e modificare le password della griglia.

Controlla l'accesso al 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 e utenti locali.

Utilizzando ["federazione di identità"](#) rende l'impostazione ["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 l'assistenza tecnica.

Si determinano le attività che ciascun utente può svolgere assegnando diverse ["permessi"](#) a ciascun gruppo. Ad esempio, potresti voler consentire agli utenti di un gruppo di gestire le regole ILM e agli utenti di un altro gruppo di eseguire attività di manutenzione. Per accedere al sistema, un utente deve appartenere ad almeno un gruppo.

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

Abilita l'accesso singolo

Il sistema StorageGRID supporta l'accesso Single Sign-On (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0). Dopo di te ["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.

Cambia la passphrase di provisioning

La passphrase di provisioning è necessaria per numerose 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 le chiavi di crittografia per il sistema StorageGRID. Puoi ["cambiare la passphrase"](#) come richiesto.

Cambiare le password della console del nodo

Ogni nodo nella griglia ha una password univoca per la console del nodo, che è necessaria per accedere al nodo come "admin" tramite SSH oppure come utente root su una connessione alla console fisica/VM. Se necessario, puoi ["cambiare la password della console del nodo"](#) per ogni nodo.

Cambia la passphrase di provisioning

Utilizzare questa procedura per modificare la passphrase di provisioning StorageGRID. La passphrase è necessaria per le procedure di recupero, 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"](#).
- Hai i permessi di accesso di Manutenzione o Root.
- Hai la passphrase di provisioning corrente.

Informazioni su questo compito

La passphrase di provisioning è richiesta per molte procedure di installazione e manutenzione e per ["scaricando il pacchetto di ripristino"](#). La passphrase di provisioning non è elencata in `Passwords.txt` file. Assicuratevi di documentare la passphrase di provisioning e di conservarla in un luogo sicuro e protetto.

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.
2. In **Modifica passphrase di provisioning**, seleziona **Apporta una modifica**
3. Inserisci la tua passphrase di provisioning attuale.
4. Inserisci la nuova passphrase. La passphrase deve contenere almeno 8 e non più di 32 caratteri. Le passphrase sono sensibili alle maiuscole e alle minuscole.
5. Conservare la nuova passphrase di provisioning in un luogo sicuro. È necessario per le procedure di installazione, ampliamento e manutenzione.
6. Reinserisci la nuova passphrase e seleziona **Salva**.

Una volta completata la modifica della passphrase di provisioning, il sistema visualizza un banner verde di successo.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

7. Selezionare **Pacchetto di ripristino**.

8. Immettere la nuova passphrase di provisioning per scaricare il nuovo pacchetto di ripristino.



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.

Cambiare le password della console del nodo

Ogni nodo della griglia ha una password univoca per la console del nodo, necessaria per accedere al nodo. Segui questi passaggi per modificare ogni password univoca della console del nodo per ogni nodo nella tua griglia.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).
- Hai la passphrase di provisioning corrente.

Informazioni su questo compito

Utilizzare la password della console del nodo per accedere a un nodo come "admin" tramite SSH oppure come utente root su una connessione VM/console fisica. Il processo di modifica della password della console del nodo crea nuove password per ogni nodo nella griglia e memorizza le password in un file aggiornato `Passwords.txt` file 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.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.
2. In **Modifica password console nodo**, seleziona **Apporta una modifica**.

Inserisci la passphrase di provisioning

Passi

1. Inserisci la passphrase di provisioning per la tua griglia.
2. Selezionare **Continua**.

Scarica il pacchetto di ripristino corrente

Prima di modificare le password della console del nodo, scaricare il pacchetto di ripristino corrente. È possibile utilizzare le password contenute in questo file se il processo di modifica della password non riesce per un nodo.

Passi

1. Seleziona **Scarica pacchetto di ripristino**.
2. Copia il file del pacchetto di ripristino(.zip) in due luoghi sicuri, protetti e separati.



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, seleziona **Sì** se sei pronto a iniziare a modificare le password della console del nodo.

Non è possibile annullare questo processo una volta avviato.

Cambiare le password della console del nodo

Quando si avvia il processo di inserimento della password della console del nodo, viene generato un nuovo pacchetto di ripristino che include le nuove password. Quindi, le password vengono aggiornate su ciascun nodo.

Passi

1. Attendi che venga generato il nuovo pacchetto di ripristino, operazione che potrebbe richiedere alcuni minuti.
2. Seleziona **Scarica nuovo pacchetto di ripristino**.
3. Al termine del download:
 - a. Apri il .zip file.
 - b. Conferma di poter accedere ai contenuti, incluso il `Passwords.txt` file, che contiene le nuove password della console del nodo.
 - c. Copia il nuovo file del pacchetto di ripristino(.zip) in due luoghi sicuri, protetti e separati.



Non sovrascrivere il vecchio Recovery Package.

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. Seleziona la casella di controllo per indicare che hai scaricato il nuovo pacchetto di ripristino e ne hai verificato il contenuto.
5. Selezionare **Modifica password console nodo** e attendere che tutti i nodi vengano aggiornati con le nuove password. Potrebbero volerci alcuni minuti.

Se le password vengono modificate per tutti i nodi, viene visualizzato un banner verde di operazione riuscita. Vai al passaggio successivo.

Se si verifica un errore durante il processo di aggiornamento, un messaggio banner elenca il numero di nodi le cui password non sono state modificate. Il sistema riproverà automaticamente il processo su qualsiasi nodo la cui password non è riuscita a cambiare. Se il processo termina con alcuni nodi che non hanno ancora modificato la password, 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. Seleziona **Riprova**.



Il nuovo tentativo modifica solo le password della console dei nodi che non sono riusciti nei precedenti tentativi di modifica della password.

6. Dopo aver modificato le password della console del nodo per tutti i nodi, eliminare il [primo pacchetto di ripristino scaricato](#).
7. Facoltativamente, utilizzare il collegamento **Pacchetto di ripristino** per scaricare una copia aggiuntiva del nuovo Pacchetto di ripristino.

Modificare le password di accesso SSH per i nodi amministrativi

La modifica delle password di accesso SSH per i nodi amministrativi aggiorna anche i set univoci di chiavi SSH interne per ciascun nodo nella griglia. Il nodo di amministrazione primario utilizza queste chiavi SSH per accedere ai nodi tramite autenticazione sicura e senza password.

Utilizzare una chiave SSH per accedere a un nodo come `admin` o all'utente `root` su una macchina virtuale o su una connessione alla console fisica.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).
- Hai la passphrase di provisioning corrente.

Informazioni su questo compito

Le nuove password di accesso per i nodi di amministrazione e le nuove chiavi interne per ciascun nodo sono memorizzate nel `Passwords.txt` file nel pacchetto di ripristino. Le chiavi sono elencate nella colonna Password di quel file.

Esistono password di accesso SSH separate per le chiavi SSH utilizzate per la comunicazione tra i nodi. Questa procedura non li modifica.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.
2. In **Modifica chiavi SSH**, seleziona **Apporta una modifica**.

Scarica il pacchetto di ripristino corrente

Prima di modificare le chiavi di accesso SSH, scaricare il pacchetto di ripristino corrente. È possibile utilizzare le chiavi contenute in questo file se il processo di modifica delle chiavi non riesce per un nodo.

Passi

1. Inserisci la passphrase di provisioning per la tua griglia.
2. Seleziona **Scarica pacchetto di ripristino**.

3. Copia il file del pacchetto di ripristino(.zip) in due luoghi sicuri, protetti e separati.



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 **Continua**.
5. Quando viene visualizzata la finestra di dialogo di conferma, seleziona **Sì** se sei pronto a iniziare a modificare le chiavi di accesso SSH.



Non è possibile annullare questo processo una volta avviato.

Cambia le chiavi di accesso SSH

Quando viene avviato il processo di modifica delle chiavi di accesso SSH, viene generato un nuovo pacchetto di ripristino che include le nuove chiavi. Quindi, le chiavi vengono aggiornate su ciascun nodo.

Passi

1. Attendi che venga generato il nuovo pacchetto di ripristino, operazione che potrebbe richiedere alcuni minuti.
2. Quando il pulsante Scarica nuovo pacchetto di ripristino è abilitato, seleziona **Scarica nuovo pacchetto di ripristino** e salva il nuovo file del pacchetto di ripristino(.zip) in due luoghi sicuri, protetti e separati.
3. Al termine del download:
 - a. Apri il .zip file.
 - b. Conferma di poter accedere ai contenuti, incluso il Passwords.txt file, che contiene le nuove chiavi di accesso SSH.
 - c. Copia il nuovo file del pacchetto di ripristino(.zip) in due luoghi sicuri, protetti e separati.



Non sovrascrivere il vecchio Recovery Package.

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. Attendi che le chiavi vengano aggiornate su ciascun nodo, operazione che potrebbe richiedere alcuni minuti.

Se le chiavi vengono modificate per tutti i nodi, viene visualizzato un banner verde di successo.

Se si verifica un errore durante il processo di aggiornamento, un messaggio banner elenca il numero di nodi le cui chiavi non sono state modificate. Il sistema riproverà automaticamente il processo su qualsiasi nodo la cui chiave non è riuscita a cambiare. Se il processo termina con alcuni nodi che non hanno ancora una chiave modificata, viene visualizzato il pulsante **Riprova**.

Se l'aggiornamento della chiave non è riuscito per uno o più nodi:

- a. Esaminare i messaggi di errore elencati nella tabella.
- b. Risolvere i problemi.
- c. Seleziona **Riprova**.

Il nuovo tentativo modifica solo le chiavi di accesso SSH sui nodi che non sono riusciti durante i precedenti tentativi di modifica delle chiavi.

5. Dopo aver modificato le chiavi di accesso SSH per tutti i nodi, eliminare [primo pacchetto di ripristino scaricato](#) .
6. Facoltativamente, selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino** per scaricare una copia aggiuntiva del nuovo Pacchetto di ripristino.

Utilizzare la federazione delle identità

L'utilizzo della federazione delle identità velocizza 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 di amministratori 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"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Stai utilizzando Active Directory, Azure AD, OpenLDAP o Oracle Directory Server come provider di identità.



Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare l'assistenza tecnica.

- Se si prevede di utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere [Linee guida per la configurazione di un server OpenLDAP](#) .
- Se si prevede di abilitare l'accesso singolo (SSO), è necessario aver esaminato il ["requisiti e considerazioni per l'accesso unico"](#) .
- Se si prevede di utilizzare Transport Layer Security (TLS) per le comunicazioni con il server LDAP, il provider di identità utilizza TLS 1.2 o 1.3. Vedere ["Cifature supportate per le connessioni TLS in uscita"](#) .

Informazioni su questo compito

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 amministrazione. Gli utenti nei 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 una propria fonte di identità. Gli utenti nei gruppi di tenant possono accedere a Tenant Manager ed eseguire attività in base alle autorizzazioni assegnate al gruppo in Tenant Manager. Vedere ["Crea un account inquilino"](#) E ["Utilizzare un account tenant"](#) per i dettagli.

Inserisci la configurazione

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Federazione identità**.
2. Selezionare **Abilita federazione delle identità**.

3. Nella sezione Tipo di servizio LDAP, seleziona il tipo di servizio LDAP che desideri configurare.

Ldap service type

Select the type of LDAP service you want to configure.

Active Directory

Azure

OpenLDAP

Other

Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se hai selezionato **Altro**, compila i campi nella sezione Attributi LDAP. procedere al passaggio successivo.

- **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`. Il valore di ciascun utente per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
- **Nome univoco del 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 di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.

5. Per tutti i tipi di servizio LDAP, immettere le informazioni richieste sul server LDAP e sulla connessione di rete nella sezione Configura server LDAP.

- **Nome host:** nome di dominio completo (FQDN) o indirizzo IP del server LDAP.
- **Porta:** la porta utilizzata per connettersi al server LDAP.



La porta predefinita per STARTTLS è 389, mentre la porta predefinita per LDAPS è 636. Tuttavia, puoi utilizzare qualsiasi porta, a patto che il firewall sia configurato correttamente.

- **Nome utente:** percorso completo del nome distinto (DN) dell'utente che si conatterà al server LDAP.

Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome dell'entità utente.

L'utente specificato deve avere l'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

- `sAMAccountName`O`uid`

- objectGUID, entryUUID, O nsuniqueid
 - cn
 - memberOf`O `isMemberOf
 - **Directory attiva:** objectSid, primaryGroupID, userAccountControl, E userPrincipalName
 - **Azzurro:** accountEnabled E userPrincipalName
- **Password:** la password associata al nome utente.



Se in futuro dovessi cambiare la password, dovrai aggiornarla in questa pagina.

- **DN base gruppo:** percorso completo del nome distinto (DN) per un sottoalbero LDAP in cui si desidera cercare i gruppi. Nell'esempio di Active Directory (sotto), 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 **Nome univoco del gruppo** devono essere univoci all'interno del **DN di base del gruppo** a cui appartengono.

- **DN base utente:** percorso completo del nome distinto (DN) di un sottoalbero LDAP in cui si desidera cercare gli utenti.



I valori **Nome univoco utente** devono essere univoci all'interno del **Nome base utente** a cui appartengono.

- **Formato nome utente associato** (facoltativo): il modello di nome utente predefinito che StorageGRID dovrebbe utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il **formato nome utente di associazione** perché può consentire agli utenti di accedere se StorageGRID non è in grado di associarsi all'account di servizio.

Inserisci 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 di nome distinto:** CN=[USERNAME], CN=Users, DC=example, DC=com

Includi [USERNAME] esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), seleziona un'impostazione di sicurezza.

- **Usa STARTTLS:** usa STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma non è supportata per Azure.
- **Usa LDAPS:** l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario 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 impone la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

7. Se hai selezionato STARTTLS o LDAPS, scegli il certificato utilizzato per proteggere la connessione.
 - **Utilizza il certificato CA del sistema operativo:** utilizza il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni.
 - **Utilizza certificato CA personalizzato:** utilizza un certificato di sicurezza personalizzato.

Se selezioni questa impostazione, copia e incolla il certificato di sicurezza personalizzato nella casella di testo Certificato CA.

Testare la connessione e salvare la configurazione

Dopo aver immesso tutti i valori, è necessario testare la connessione prima di poter salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente associato, se ne è stato fornito uno.

Passi

1. Selezionare **Test connessione**.
2. Se non hai fornito un formato di nome utente di associazione:
 - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di 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, risolvi eventuali problemi e verifica nuovamente la connessione.
3. Se hai fornito un formato di nome utente vincolato, inserisci il nome utente e la password di un utente federato valido.

Ad esempio, inserisci il tuo nome utente e la tua password. Non includere caratteri speciali nel nome utente, come @ o /.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

[Cancel](#) [Test Connection](#)

- Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di connessione riuscito". Selezionare **Salva** per salvare la configurazione.

- Se le impostazioni di connessione, il formato del nome utente associato o il nome utente e la password di prova non sono validi, viene visualizzato un messaggio di errore. Risolvi eventuali problemi e verifica nuovamente la connessione.

Forza la sincronizzazione con la fonte dell'identità

Il sistema StorageGRID sincronizza periodicamente i gruppi federati e gli utenti dalla fonte di identità. È possibile forzare l'avvio della sincronizzazione se si desidera abilitare o limitare le autorizzazioni utente il più rapidamente possibile.

Passi

1. Vai alla pagina Federazione delle identità.
2. Seleziona **Sincronizza server** nella parte superiore della pagina.

Il processo di sincronizzazione potrebbe richiedere del tempo, a seconda dell'ambiente.



L'avviso **Errore di sincronizzazione della federazione delle identità** viene attivato se si verifica un problema durante la sincronizzazione di gruppi e utenti federati dall'origine dell'identità.

Disabilitare la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione delle identità per gruppi e utenti. Quando la federazione delle identità è disabilitata, non c'è comunicazione tra StorageGRID e l'origine dell'identità. Tuttavia, tutte le impostazioni configurate vengono mantenute, consentendoti di riattivare facilmente la federazione delle identità in futuro.

Informazioni su questo compito

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno effettuare l'accesso.
- Gli utenti federati attualmente connessi manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno effettuare l'accesso dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non verrà eseguita e non verranno generati avvisi per gli account che non sono stati sincronizzati.
- La casella di controllo **Abilita federazione delle identità** è disabilitata se l'accesso Single Sign-On (SSO) è impostato su **Abilitato** o **Modalità Sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere "[Disabilitare l'accesso singolo](#)".

Passi

1. Vai alla pagina Federazione delle identità.
2. Deseleziona la casella di controllo **Abilita federazione delle 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 origini identità diverse da ActiveDirectory o Azure, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare tutte le chiavi S3 dell'utente o rimuovere l'utente da tutti i gruppi.

Sovrapposizioni di membri e raffinazione

Le sovrapposizioni memberof e refint dovrebbero essere abilitate. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo in <http://www.openldap.org/doc/admin24/index.html> ["Documentazione OpenLDAP: Guida dell'amministratore 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, assicurati che i campi menzionati nella guida per Nome utente siano indicizzati per prestazioni ottimali.

Consultare le informazioni sul mantenimento dell'appartenenza al gruppo inverso in <http://www.openldap.org/doc/admin24/index.html> ["Documentazione OpenLDAP: Guida dell'amministratore versione 2.4"] .

Gestisci gruppi di amministratori

È possibile creare gruppi di amministratori per gestire le autorizzazioni di sicurezza per uno o più utenti amministratori. Per poter accedere al sistema StorageGRID , gli utenti devono appartenere a un gruppo.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .
- Se si prevede di importare un gruppo federato, è necessario aver configurato la federazione delle identità e il gruppo federato esiste già nell'origine identità configurata.

Crea un gruppo di amministratori

I gruppi di amministratori consentono di stabilire quali utenti possono accedere a quali funzionalità e operazioni in Grid Manager e nell'API Grid Management.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Gruppi amministratori**.
2. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federato.

- Crea un gruppo locale se vuoi assegnare autorizzazioni agli utenti locali.
- Crea un gruppo federato per importare gli utenti dall'origine dell'identità.

Gruppo locale

Passi

1. Seleziona **Gruppo locale**.
2. Inserisci un nome visualizzato per il gruppo, che potrai aggiornare in seguito se necessario. Ad esempio, "Utenti addetti alla manutenzione" o "Amministratori ILM".
3. Inserisci un nome univoco per il gruppo, che non potrai aggiornare in seguito.
4. Selezionare **Continua**.

Gruppo federato

Passi

1. Seleziona **Gruppo federato**.
2. Inserisci il nome del gruppo che desideri importare, esattamente come appare nell'origine identità configurata.
 - Per Active Directory e Azure, utilizzare sAMAccountName.
 - Per OpenLDAP, utilizzare il CN (nome comune).
 - Per un altro LDAP, utilizzare il nome univoco appropriato per il server LDAP.
3. Selezionare **Continua**.

Gestisci i permessi del gruppo

Passi

1. Per la **Modalità di accesso**, seleziona se gli utenti del gruppo possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nell'API di gestione della griglia oppure se possono solo visualizzare impostazioni e funzionalità.
 - **Lettura-scrittura** (predefinito): gli utenti possono modificare le impostazioni ed eseguire le operazioni consentite dalle loro autorizzazioni di gestione.
 - **Sola lettura**: gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Grid Manager o nell'API Grid Management. Gli utenti locali con privilegi di sola lettura possono modificare le proprie password.



Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su **Sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Seleziona uno o più ["autorizzazioni del gruppo amministratore"](#).

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti al gruppo non potranno accedere a StorageGRID.

3. Se stai creando un gruppo locale, seleziona **Continua**. Se stai creando un gruppo federato, seleziona

Crea gruppo e Fine.

Aggiungi utenti (solo gruppi locali)

Passi

1. Facoltativamente, seleziona uno o più utenti locali per questo gruppo.

Se non hai ancora creato utenti locali, puoi salvare il gruppo senza aggiungere utenti. Puoi aggiungere questo gruppo all'utente nella pagina Utenti. Vedere "[Gestisci utenti](#)" per i dettagli.

2. Seleziona **Crea gruppo e Fine**.

Visualizza e modifica i gruppi di amministrazione

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 modificare un gruppo, utilizzare il menu **Azioni** o la pagina dei dettagli.

Compito	Menu Azioni	Pagina dei dettagli
Visualizza i dettagli del gruppo	a. Selezionare la casella di controllo per il gruppo. b. Seleziona Azioni > Visualizza dettagli gruppo.	Selezionare il nome del gruppo nella tabella.
Modifica il nome visualizzato (solo gruppi locali)	a. Selezionare la casella di controllo per il gruppo. b. Seleziona Azioni > Modifica nome gruppo. c. Inserisci il nuovo nome. d. Seleziona Salva modifiche.	a. Selezionare il nome del gruppo per visualizzarne i dettagli. b. Seleziona l'icona di modifica . c. Inserisci il nuovo nome. d. Seleziona Salva modifiche.
Modifica la modalità di accesso o le autorizzazioni	a. Selezionare la casella di controllo per il gruppo. b. Seleziona Azioni > Visualizza dettagli gruppo. c. Facoltativamente, modifica la modalità di accesso del gruppo. d. Facoltativamente, seleziona o deseleziona "autorizzazioni del gruppo amministratore". e. Seleziona Salva modifiche.	a. Selezionare il nome del gruppo per visualizzarne i dettagli. b. Facoltativamente, modifica la modalità di accesso del gruppo. c. Facoltativamente, seleziona o deseleziona "autorizzazioni del gruppo amministratore". d. Seleziona Salva modifiche.

Duplica un gruppo

Passi

1. Selezionare la casella di controllo per il gruppo.
2. Selezionare **Azioni > Duplica gruppo**.
3. Completa la procedura guidata Duplica gruppo.

Elimina un gruppo

È possibile eliminare un gruppo di amministratori quando si desidera rimuovere il gruppo dal sistema e rimuovere tutte le autorizzazioni ad esso associate. L'eliminazione di un gruppo di amministratori rimuove tutti gli utenti dal gruppo, ma non elimina gli utenti stessi.

Passi

1. Nella pagina Gruppi, seleziona la casella di controllo per ogni gruppo che desideri rimuovere.
2. Selezionare **Azioni > Elimina gruppo**.
3. Seleziona **Elimina gruppi**.

Autorizzazioni del gruppo amministratore

Quando si creano gruppi di utenti amministratori, 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 può eseguire quell'utente.

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti a quel 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:

- Sign in a Grid Manager
- Visualizza la dashboard
- Visualizza le pagine dei nodi
- Visualizza gli avvisi correnti e risolti
- Cambiare la 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 oppure se possono solo visualizzare le impostazioni e le funzionalità correlate. Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su **Sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

Nelle sezioni seguenti vengono descritte le autorizzazioni che è possibile assegnare durante la creazione o la modifica di un gruppo di amministratori. Per qualsiasi funzionalità non esplicitamente menzionata è necessario il permesso di **accesso root**.

Accesso root

Questa autorizzazione fornisce l'accesso a tutte le funzionalità di amministrazione della griglia.

Cambia la password di root del tenant

Questa autorizzazione fornisce l'accesso all'opzione **Cambia password di 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 abilitata la funzionalità di importazione delle chiavi S3. Gli utenti che non dispongono di questa autorizzazione non possono visualizzare l'opzione **Cambia password di root**.



Per concedere l'accesso alla pagina Tenant, che contiene l'opzione **Cambia password di root**, assegnare anche l'autorizzazione **Account tenant**.

Configurazione della pagina della topologia della griglia

Questa autorizzazione consente di accedere alle schede Configurazione nella pagina **SUPPORTO > Strumenti > Topologia griglia**.



La pagina Topologia griglia è stata deprecata e verrà rimossa in una versione futura.

ILM

Questa autorizzazione fornisce l'accesso alle seguenti opzioni del menu **ILM**:

- Regole
- Politiche
- Tag di policy
- Pool di stoccaggio
- Gradi di stoccaggio
- Regioni
- Ricerca metadati oggetto



Per gestire i gradi di archiviazione, gli utenti devono disporre delle autorizzazioni **Altra configurazione della griglia** e **Configurazione della pagina della topologia della griglia**.

Manutenzione

Per utilizzare queste opzioni, gli utenti devono disporre dell'autorizzazione di manutenzione:

- **CONFIGURAZIONE > Controllo accessi:**
 - Password di griglia
- **CONFIGURAZIONE > Rete:**
 - Nomi di dominio endpoint S3
- **MANUTENZIONE > Attività:**
 - Dismissione
 - Espansione
 - Controllo dell'esistenza dell'oggetto
 - Recupero

- **MANUTENZIONE > Sistema:**

- Pacchetto di recupero
- Aggiornamento software

- **SUPPORTO > Strumenti:**

- Registri

Gli utenti che non dispongono dell'autorizzazione di manutenzione possono visualizzare, ma non modificare, queste pagine:

- **MANUTENZIONE > Rete:**

- server DNS
- Rete a griglia
- server NTP

- **MANUTENZIONE > Sistema:**

- Licenza

- **CONFIGURAZIONE > Rete:**

- Nomi di dominio endpoint S3

- **CONFIGURAZIONE > Sicurezza:**

- Certificati

- **CONFIGURAZIONE > Monitoraggio:**

- Server di audit e syslog

Gestisci gli avvisi

Questa autorizzazione fornisce l'accesso 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 fornisce l'accesso a:

- Pagina **SUPPORTO > Strumenti > Metriche**
- Query personalizzate sulle metriche Prometheus utilizzando la sezione **Metriche** dell'API di gestione della griglia
- Schede della dashboard di Grid Manager che contengono metriche

Ricerca metadati oggetto

Questa autorizzazione fornisce l'accesso alla pagina **ILM > Ricerca metadati oggetto**.

Altra configurazione della griglia

Questa autorizzazione fornisce l'accesso ad ulteriori opzioni di configurazione della griglia.



Per visualizzare queste opzioni aggiuntive, gli utenti devono disporre anche dell'autorizzazione **Configurazione della pagina topologia griglia**.

- **ILM:**
 - Gradi di stoccaggio
- **CONFIGURAZIONE > Sistema:**
- **SUPPORTO > Altro:**
 - Costo del collegamento

Amministratore dell'appliance di archiviazione

Questa autorizzazione prevede:

- Accesso a E-Series SANtricity System Manager su dispositivi di storage tramite Grid Manager.
- Possibilità di eseguire attività di risoluzione dei problemi e manutenzione nella scheda Gestisci unità per gli apparecchi che supportano queste operazioni.

Conti degli inquilini

Questa autorizzazione fornisce la possibilità di:

- Accedi alla pagina Inquilini, dove puoi creare, modificare e rimuovere gli account degli inquilini
- Visualizza le policy di classificazione del traffico esistenti
- Visualizza le schede della dashboard di Grid Manager che contengono i dettagli del tenant

Gestisci utenti

È possibile visualizzare gli utenti locali e federati. È anche possibile creare utenti locali e assegnarli a gruppi di amministratori locali per determinare a quali funzionalità di Grid Manager possono accedere questi utenti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Crea 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 funzionalità di Grid Manager e Grid Management API l'utente può accedere.

È possibile creare solo utenti locali. Utilizzare la fonte di identità esterna per gestire utenti e gruppi federati.

Grid Manager include un utente locale predefinito, denominato "root". Non è possibile rimuovere l'utente root.



Se è abilitato l'accesso Single Sign-On (SSO), gli utenti locali non possono accedere a StorageGRID.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Utenti amministratori**.
2. Seleziona **Crea utente**.

Inserisci le credenziali utente

Passi

1. Inserisci il nome completo dell'utente, un nome utente univoco e una password.
2. Facoltativamente, seleziona **Sì** se questo utente non deve avere accesso a Grid Manager o all'API Grid Management.
3. Selezionare **Continua**.

Assegna ai gruppi

Passi

1. Facoltativamente, assegnare l'utente a uno o più gruppi per determinare le autorizzazioni dell'utente.

Se non hai ancora creato gruppi, puoi salvare l'utente senza selezionare i gruppi. Puoi aggiungere questo utente a un gruppo nella pagina Gruppi.

Se un utente appartiene a più gruppi, le autorizzazioni sono cumulative. Vedere ["Gestisci gruppi di amministratori"](#) per i dettagli.

2. Selezionare **Crea utente** e poi **Fine**.

Visualizza e modifica gli utenti locali

È possibile visualizzare i dettagli degli utenti locali e federati esistenti. È possibile modificare un utente locale per cambiarne il nome completo, la password o l'appartenenza al gruppo. È anche possibile impedire temporaneamente a un utente di accedere a Grid Manager e all'API Grid Management.

È possibile modificare solo gli utenti locali. Utilizzare la fonte di 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 cambiare la password di un utente locale, utilizzare il menu **Azioni** o la pagina dei dettagli.

Tutte le modifiche verranno applicate la volta successiva che l'utente si disconnette e accede nuovamente a Grid Manager.



Gli utenti locali possono modificare le proprie password utilizzando l'opzione **Cambia password** nel banner di Grid Manager.

Compito	Menu Azioni	Pagina dei dettagli
Visualizza i dettagli dell'utente	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Visualizza dettagli utente .	Selezionare il nome dell'utente nella tabella.

Compito	Menu Azioni	Pagina dei dettagli
Modifica il nome completo (solo utenti locali)	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Modifica nome completo. c. Inserisci il nuovo nome. d. Seleziona Salva modifiche.	a. Selezionare il nome dell'utente per visualizzarne i dettagli. b. Seleziona l'icona di modifica  . c. Inserisci il nuovo nome. d. Seleziona Salva modifiche.
Nega o consenti l'accesso a StorageGRID	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Visualizza dettagli utente. c. Selezionare la scheda Accesso. d. Selezionare Sì per impedire all'utente di accedere a Grid Manager o all'API di gestione della griglia, oppure selezionare No per consentire all'utente di accedere. e. Seleziona Salva modifiche.	a. Selezionare il nome dell'utente per visualizzarne i dettagli. b. Selezionare la scheda Accesso. c. Selezionare Sì per impedire all'utente di accedere a Grid Manager o all'API di gestione della griglia, oppure selezionare No per consentire all'utente di accedere. d. Seleziona Salva modifiche.
Cambia password (solo utenti locali)	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Visualizza dettagli utente. c. Selezionare la scheda Password. d. Inserisci una nuova password. e. Seleziona Cambia password.	a. Selezionare il nome dell'utente per visualizzarne i dettagli. b. Selezionare la scheda Password. c. Inserisci una nuova password. d. Seleziona Cambia password.
Cambia gruppi (solo utenti locali)	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Visualizza dettagli utente. c. Selezionare la scheda Gruppi. d. Facoltativamente, seleziona il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. e. Selezionare Modifica gruppi per selezionare gruppi diversi. f. Seleziona Salva modifiche.	a. Selezionare il nome dell'utente per visualizzarne i dettagli. b. Selezionare la scheda Gruppi. c. Facoltativamente, seleziona il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. d. Selezionare Modifica gruppi per selezionare gruppi diversi. e. Seleziona Salva modifiche.

Duplica un utente

È possibile duplicare un utente esistente per crearne uno nuovo con le stesse autorizzazioni.

Passi

1. Selezionare la casella di controllo per l'utente.
2. Selezionare **Azioni > Duplica utente**.
3. Completa la procedura guidata Duplica utente.

Elimina un utente

È possibile eliminare un utente locale per rimuoverlo definitivamente dal sistema.



Non è possibile eliminare l'utente root.

Passi

1. Nella pagina Utenti, seleziona la casella di controllo per ogni utente che desideri rimuovere.
2. Selezionare **Azioni > Elimina utente**.
3. Seleziona **Elimina utente**.

Utilizzare l'accesso singolo (SSO)

Configurare l'accesso singolo

Quando è abilitato l'accesso 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 tramite il processo di accesso SSO implementato dalla tua organizzazione. Gli utenti locali non possono accedere a StorageGRID.

Come funziona l'accesso singolo

Il sistema StorageGRID supporta l'accesso Single Sign-On (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0).

Prima di abilitare l'accesso Single Sign-On (SSO), esaminare in che modo i processi di accesso e disconnessione StorageGRID vengono influenzati dall'abilitazione dell'SSO.

Sign in quando SSO è abilitato

Quando l'SSO è abilitato e accedi a StorageGRID, verrai reindirizzato alla pagina SSO della tua organizzazione per convalidare le tue credenziali.

Passi

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 Sign in a StorageGRID .

- Se è la prima volta che accedi all'URL su questo browser, ti verrà richiesto un ID account:



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- Se hai già effettuato l'accesso a Grid Manager o Tenant Manager, ti verrà chiesto di selezionare un account recente o di immettere un ID account:



Tenant Manager

Recent

Account

Sign in

[NetApp support](#) | [NetApp.com](#)



La pagina Sign in StorageGRID non viene visualizzata quando si immette l'URL completo per un account tenant (ovvero un nome di dominio completo o un indirizzo IP seguito da `/?accountId=20-digit-account-id`). Invece, verrai immediatamente reindirizzato alla pagina di accesso SSO della tua organizzazione, dove potrai [accedi con le tue credenziali SSO](#).

2. Indica se desideri accedere al Grid Manager o al Tenant Manager:

- Per accedere a Grid Manager, lasciare vuoto il campo **ID account**, immettere **0** come ID account oppure selezionare **Grid Manager** se compare nell'elenco degli account recenti.
- Per accedere a Tenant Manager, immettere l'ID account del tenant a 20 cifre oppure selezionare un tenant per nome se compare nell'elenco degli account recenti.

3. Seleziona * Sign in*

StorageGRID ti reindirizza alla pagina di accesso SSO della tua organizzazione. Per esempio:

Sign in with your organizational account

someone@example.com

Password

Sign in

4. Sign in con le tue credenziali SSO.

Se le tue 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 si appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID, si accede a Grid Manager o Tenant Manager, a seconda dell'account selezionato.



Se l'account di servizio non è accessibile, puoi comunque effettuare l'accesso, a patto che tu sia un utente esistente appartenente a un gruppo federato con autorizzazioni di accesso StorageGRID.

5. Facoltativamente, accedi ad altri nodi amministrativi oppure a Grid Manager o Tenant Manager, se disponi delle autorizzazioni adeguate.

Non è necessario reinserire le credenziali SSO.

Disconnettersi quando SSO è abilitato

Quando SSO è abilitato per StorageGRID, ciò che accade quando ci si disconnette dipende dall'account a cui si è effettuato l'accesso e da dove ci si disconnette.

Passi

1. Individua il link **Esci** nell'angolo in alto a destra dell'interfaccia utente.
2. Seleziona **Esci**.

Viene visualizzata la pagina Sign in a StorageGRID . Il menu a discesa **Account recenti** è stato aggiornato per includere **Grid Manager** o il nome del tenant, in modo da poter accedere più rapidamente a queste interfacce utente in futuro.

Se hai effettuato l'accesso a...	E ti disconnetti da...	Hai effettuato la disconnessione da...
Grid Manager su uno o più nodi amministrativi	Grid Manager su qualsiasi nodo di amministrazione	Grid Manager su tutti i nodi amministrativi Nota: se si utilizza Azure per SSO, potrebbero essere necessari alcuni minuti per uscire da tutti i nodi amministrativi.
Tenant Manager su uno o più nodi amministrativi	Tenant Manager su qualsiasi nodo amministrativo	Tenant Manager su tutti i nodi amministrativi
Sia Grid Manager che Tenant Manager	Responsabile della griglia	Solo il Grid Manager. Per uscire dall'SSO è necessario anche disconnettersi da Tenant Manager.



La tabella riassume cosa succede quando ci si disconnette se si utilizza una singola sessione del browser. Se hai effettuato l'accesso a StorageGRID in più sessioni del browser, devi disconnetterti da tutte le sessioni del browser separatamente.

Requisiti e considerazioni per l'accesso singolo

Prima di abilitare l'accesso Single Sign-On (SSO) per un sistema StorageGRID , esaminare i requisiti e le considerazioni.

Requisiti del fornitore di identità

StorageGRID supporta i seguenti provider di identità SSO (IdP):

- Servizio federativo di Active Directory (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 la federazione delle identità determina il tipo di SSO che è possibile implementare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Directory attiva	• Directory attiva • Azzurro • PingFederate
Azzurro	Azzurro

Requisiti AD FS

È possibile utilizzare una qualsiasi delle seguenti versioni di AD FS:

- Windows Server 2022 ADFS
- Windows Server 2019 ADFS
- Windows Server 2016 ADFS



Windows Server 2016 dovrebbe utilizzare ["Aggiornamento KB3201845"](#) , o superiore.

Requisiti aggiuntivi

- Sicurezza del livello di trasporto (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versione 3.5.1 o successiva

Considerazioni per Azure

Se si utilizza Azure come tipo di SSO e gli utenti hanno nomi di entità utente che non utilizzano sAMAccountName come prefisso, potrebbero 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 del certificato del server

Per impostazione predefinita, StorageGRID utilizza un certificato di interfaccia di gestione su ciascun nodo di amministrazione per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Quando si configurano trust di relying party (AD FS), applicazioni aziendali (Azure) o connessioni del provider di servizi (PingFederate) per StorageGRID, si utilizza il certificato del server come certificato di firma per le richieste StorageGRID .

Se non l'hai già fatto ["configurato un certificato personalizzato per l'interfaccia di gestione"](#) , dovresti farlo ora. Quando si installa un certificato server personalizzato, questo viene utilizzato per tutti i nodi amministrativi e può essere utilizzato in tutti i trust relying party StorageGRID , nelle applicazioni aziendali o nelle connessioni SP .



Non è consigliabile utilizzare il certificato server predefinito di un nodo di amministrazione in un trust di relying party, in un'applicazione aziendale o in una connessione SP . Se il nodo fallisce e lo si ripristina, viene generato un nuovo certificato server predefinito. Prima di poter accedere al nodo recuperato, è necessario aggiornare il trust della relying party, l'applicazione aziendale o la connessione SP con il nuovo certificato.

È possibile accedere al certificato del server di un nodo di amministrazione effettuando l'accesso alla shell dei

comandi del nodo e andando su `/var/local/mgmt-api` elenco. Un certificato server personalizzato è denominato `custom-server.crt`. Il certificato del server predefinito del nodo è denominato `server.crt`.

Requisiti portuali

L'accesso Single Sign-On (SSO) non è disponibile sulle porte riservate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione tramite Single Sign-On, è necessario utilizzare la porta HTTPS predefinita (443). Vedere ["Controllare l'accesso al firewall esterno"](#).

Conferma che gli utenti federati possono accedere

Prima di abilitare l'accesso Single Sign-On (SSO), è necessario confermare che almeno un utente federato possa accedere a Grid Manager e a Tenant Manager per tutti gli account tenant esistenti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).
- Hai già configurato la federazione delle identità.

Passi

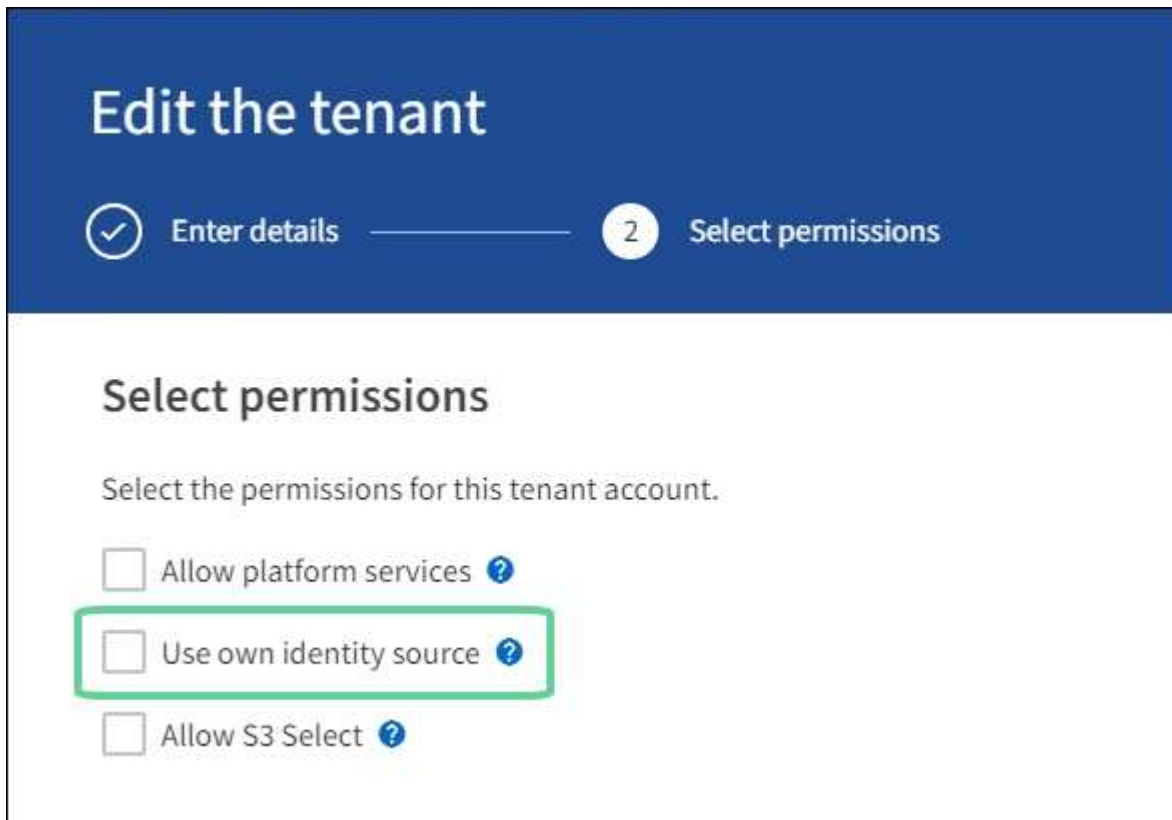
1. Se sono già presenti account tenant, verificare che nessuno dei tenant utilizzi la propria fonte di identità.



Quando si abilita SSO, un'origine identità configurata in Tenant Manager viene sostituita dall'origine identità configurata in Grid Manager. Gli utenti appartenenti all'origine identità del tenant non potranno più effettuare l'accesso a meno che non dispongano di un account con l'origine identità di Grid Manager.

- a. Sign in al Tenant Manager per ogni account tenant.
 - b. Selezionare **GESTIONE ACCESSI > Federazione identità**.
 - c. Verificare che la casella di controllo **Abilita federazione delle identità** non sia selezionata.
 - d. In tal caso, verificare che tutti i gruppi federati eventualmente utilizzati per questo account tenant non siano più necessari, deselezionare la casella di controllo e selezionare **Salva**.
2. Verificare che un utente federato possa accedere a Grid Manager:
 - a. Da Grid Manager, seleziona **CONFIGURAZIONE > Controllo accessi > Gruppi amministratori**.
 - b. Assicurarsi che almeno un gruppo federato sia stato importato dall'origine identità di Active Directory e che gli sia stata assegnata l'autorizzazione di accesso Root.
 - c. Disconnessione.
 - d. Conferma di poter accedere nuovamente a Grid Manager come utente del gruppo federato.
 3. Se sono presenti account tenant, verificare che un utente federato con autorizzazione di accesso Root possa accedere:
 - a. Da Grid Manager, seleziona **TENANTS**.
 - b. Selezionare l'account tenant e selezionare **Azioni > Modifica**.
 - c. Nella scheda Inserisci dettagli, seleziona **Continua**.
 - d. Se è selezionata la casella di controllo **Usa la propria fonte di identità**, deselezionarla e selezionare

Salva.



Viene visualizzata la pagina Inquilino.

- Selezionare l'account tenant, selezionare * Sign in* e accedere all'account tenant come utente root locale.
- Da Tenant Manager, seleziona **GESTIONE ACCESSI > Gruppi**.
- Assicurarsi che almeno a un gruppo federato di Grid Manager sia stata assegnata l'autorizzazione di accesso Root per questo tenant.
- Disconnessione.
- Conferma di poter accedere nuovamente al tenant come utente nel gruppo federato.

Informazioni correlate

- ["Requisiti e considerazioni per l'accesso singolo"](#)
- ["Gestisci gruppi di amministratori"](#)
- ["Utilizzare un account tenant"](#)

Utilizza la modalità sandbox

È possibile utilizzare la modalità sandbox per configurare e testare l'accesso singolo (SSO) prima di abilitarlo per tutti gli utenti StorageGRID . Dopo aver abilitato l'SSO, puoi tornare alla modalità sandbox ogni volta che hai bisogno di modificare o testare nuovamente la configurazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

- Tu hai il "[Permesso di accesso root](#)".
- Hai configurato la federazione delle identità per il tuo sistema StorageGRID.
- Per il tipo di servizio LDAP di federazione delle identità, hai selezionato Active Directory o Azure, in base al provider di identità SSO che intendi utilizzare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Directory attiva	• Directory attiva • Azzurro • PingFederate
Azzurro	Azzurro

Informazioni su questo compito

Quando l'SSO è abilitato e un utente tenta di accedere a un nodo di amministrazione, 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 è andata a buon fine. Per richieste andate a buon fine:

- La risposta da Active Directory o PingFederate include un identificatore univoco universale (UUID) per l'utente.
- La risposta di Azure include un nome dell'entità utente (UPN).

Per consentire a StorageGRID (il fornitore del servizio) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione degli utenti, è necessario configurare determinate impostazioni in StorageGRID. Successivamente, è necessario utilizzare il software del provider di identità SSO per creare un trust della relying party (AD FS), un'applicazione aziendale (Azure) o un provider di servizi (PingFederate) per ciascun nodo di amministrazione. Infine, è necessario tornare a StorageGRID per abilitare SSO.

La modalità sandbox semplifica l'esecuzione di questa configurazione avanti e indietro e il test di tutte le impostazioni prima di abilitare l'SSO. Quando si utilizza la modalità sandbox, gli utenti non possono accedere tramite SSO.

Accedi alla modalità sandbox

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.

Viene visualizzata la pagina Single Sign-on, con l'opzione **Disabilitato** selezionata.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO status ⓘ ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



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 l'accesso singolo"](#).

2. Selezionare **Modalità Sandbox**.

Viene visualizzata la sezione Provider di identità.

Inserisci i dettagli del provider di identità

Passi

1. Selezionare il **tipo SSO** dall'elenco a discesa.
2. Compila i campi nella sezione Identity Provider in base al tipo di SSO selezionato.

Directory attiva

- a. Immettere il **Nome del servizio federativo** per il provider di identità, esattamente come appare in Active Directory Federation Service (AD FS).



Per individuare il nome del servizio federativo, accedere a Windows Server Manager. Selezionare **Strumenti > Gestione AD FS**. Dal menu Azione, seleziona **Modifica proprietà del servizio federativo**. Nel secondo campo viene visualizzato il nome del servizio federativo.

- b. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .

- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Utilizza certificato CA personalizzato:** utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

- **Non utilizzare TLS:** non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, immediatamente ["riavviare il servizio mgmt-api sui nodi amministrativi"](#) e testare un SSO riuscito nel Grid Manager.

- c. Nella sezione Relying Party, specificare l'**identificatore del relying party** per StorageGRID. Questo valore controlla il nome utilizzato per ogni trust della relying party in AD FS.

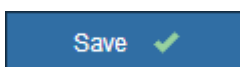
- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci `SG O StorageGRID` .
- Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG- [HOSTNAME]` . Viene generata una tabella che mostra l'identificatore della parte affidabile per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



È necessario creare un trust della relying party per ciascun nodo amministrativo nel sistema StorageGRID . La presenza di un trust di parte affidabile per ogni nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- d. Seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.



Azzurro

- a. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .

- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Utilizza certificato CA personalizzato:** utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

- **Non utilizzare TLS:** non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, immediatamente ["riavviare il servizio mgmt-api sui nodi amministrativi"](#) e testare un SSO riuscito nel Grid Manager.

- b. Nella sezione Applicazione aziendale, specificare il **Nome dell'applicazione aziendale** per StorageGRID. Questo valore controlla il nome utilizzato per ogni applicazione aziendale in Azure AD.

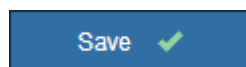
- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci `SG O StorageGRID`.
- Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG- [HOSTNAME]`. Viene generata una tabella che mostra il nome dell'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 amministrativo nel sistema StorageGRID. Disporre di un'applicazione aziendale per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

- c. Segui i passaggi in ["Crea applicazioni aziendali in Azure AD"](#) per creare un'applicazione aziendale per ogni nodo amministrativo elencato nella tabella.
- d. Da Azure AD, copiare l'URL dei metadati della federazione per ogni applicazione aziendale. Quindi, incolla questo URL nel campo **URL metadati federazione** corrispondente in StorageGRID.
- e. Dopo aver copiato e incollato un URL dei metadati di federazione per tutti i nodi amministrativi, seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.



PingFederate

- a. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID.
- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
 - **Utilizza certificato CA personalizzato:** utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

- **Non utilizzare TLS:** non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, immediatamente **riavviare il servizio mgmt-api sui nodi amministrativi** e testare un SSO riuscito nel Grid Manager.

- b. Nella sezione Fornitore di servizi (SP), specificare l'ID di connessione SP per StorageGRID. Questo valore controlla il nome utilizzato per ogni connessione SP in PingFederate.

- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci `SG O StorageGRID`.
- Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. Viene generata una tabella che mostra l'ID di connessione SP per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



È necessario creare una connessione SP per ciascun nodo amministrativo nel sistema StorageGRID. Disporre di una connessione SP per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

- c. Specificare l'URL dei metadati della federazione per ciascun nodo di amministrazione nel campo **URL dei metadati della federazione**.

Utilizzare il seguente formato:

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP  
Connection ID>
```

- d. Seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.

Save ✓

Configurare trust di relying party, applicazioni aziendali o connessioni SP

Una volta salvata la configurazione, viene visualizzato l'avviso di conferma della modalità Sandbox. Questa nota conferma che la modalità sandbox è ora abilitata e fornisce istruzioni generali.

StorageGRID può rimanere in modalità sandbox per tutto il tempo necessario. Tuttavia, quando nella pagina Single Sign-on è selezionata la **Modalità Sandbox**, l'SSO è disabilitato per tutti gli utenti StorageGRID. Possono effettuare l'accesso solo gli utenti locali.

Seguire questi passaggi per configurare trust di relying party (Active Directory), completare applicazioni

aziendali (Azure) o configurare connessioni SP (PingFederate).

Directory attiva

Passi

1. Vai ad Active Directory Federation Services (AD FS).
2. Creare uno o più trust di relying party per StorageGRID, utilizzando ciascun identificatore di relying party mostrato nella tabella nella pagina Single Sign-on StorageGRID .

È necessario creare un trust per ogni nodo amministrativo mostrato nella tabella.

Per le istruzioni, vai a ["Creare trust di relying party in AD FS"](#) .

Azzurro

Passi

1. Dalla pagina Single Sign-On per il nodo di amministrazione a cui hai effettuato l'accesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministrativi nella griglia, ripeti questi passaggi:
 - a. Sign in al nodo.
 - b. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
 - c. Scarica e salva i metadati SAML per quel nodo.
3. Vai al portale di Azure.
4. Segui i passaggi in ["Crea applicazioni aziendali in Azure AD"](#) per caricare il file di metadati SAML per ciascun nodo di amministrazione nella corrispondente applicazione aziendale di Azure.

PingFederate

Passi

1. Dalla pagina Single Sign-On per il nodo di amministrazione a cui hai effettuato l'accesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministrativi nella griglia, ripeti questi passaggi:
 - a. Sign in al nodo.
 - b. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
 - c. Scarica e salva i metadati SAML per quel nodo.
3. Vai su PingFederate.
4. ["Creare una o più connessioni al fornitore di servizi \(SP\) per StorageGRID"](#) . Utilizzare l'ID di connessione SP per ciascun nodo amministrativo (mostrato nella tabella nella pagina StorageGRID Single Sign-on) e i metadati SAML scaricati per tale nodo amministrativo.

È necessario creare una connessione SP per ogni nodo amministrativo mostrato nella tabella.

Test delle connessioni SSO

Prima di imporre l'uso dell'accesso singolo per l'intero sistema StorageGRID , è necessario verificare che l'accesso singolo e la disconnessione singola siano configurati correttamente per ciascun nodo di amministrazione.

Directory attiva

Passi

1. Nella pagina StorageGRID Single Sign-on, individuare il collegamento nel messaggio della modalità Sandbox.

L'URL deriva dal valore immesso nel campo **Nome del servizio federativo**.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

2. Seleziona il collegamento oppure copia e incolla l'URL in un browser per accedere alla pagina di accesso del tuo provider di identità.
3. Per confermare di poter utilizzare SSO per accedere a StorageGRID, seleziona * Sign in a uno dei seguenti siti*, seleziona l'identificativo della parte affidabile per il tuo nodo di amministrazione primario e seleziona * Sign in*.

You are not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

4. Inserisci il tuo nome utente e la tua password federati.
 - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

✓ Single sign-on authentication and logout test completed successfully.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
5. Ripetere questi passaggi per verificare la connessione SSO per ciascun nodo amministrativo nella

griglia.

Azzurro

Passi

1. Vai alla pagina Single Sign-On nel portale di Azure.
2. Seleziona **Prova questa applicazione**.
3. Inserisci le credenziali di un utente federato.
 - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

✓ Single sign-on authentication and logout test completed successfully.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
4. Ripetere questi passaggi per verificare la connessione SSO per ciascun nodo amministrativo nella griglia.

PingFederate

Passi

1. Dalla pagina StorageGRID Single Sign-on, selezionare il primo collegamento nel messaggio della modalità Sandbox.

Seleziona e testa un collegamento alla volta.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. Inserisci le credenziali di un utente federato.
 - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

✓ Single sign-on authentication and logout test completed successfully.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
3. Seleziona il collegamento successivo per verificare la connessione SSO per ciascun nodo di amministrazione nella tua griglia.

Se vedi un messaggio di pagina scaduta, seleziona il pulsante **Indietro** nel tuo browser e invia nuovamente le tue credenziali.

Abilita l'accesso singolo

Dopo aver confermato di poter utilizzare SSO per accedere a ciascun nodo di amministrazione, puoi abilitare SSO per l'intero sistema StorageGRID .



Quando SSO è abilitato, 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.

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
2. Modificare lo stato SSO in **Abilitato**.
3. Seleziona **Salva**.
4. Rivedere il messaggio di avviso e selezionare **OK**.

Ora è abilitato l'accesso singolo.



Se si utilizza il portale di Azure e si accede a StorageGRID dallo stesso computer utilizzato per accedere ad Azure, assicurarsi che l'utente del portale di Azure sia anche un utente StorageGRID autorizzato (un utente in un gruppo federato importato in StorageGRID) oppure disconnettersi dal portale di Azure prima di tentare di accedere a StorageGRID.

Creare trust di relying party in AD FS

È necessario utilizzare Active Directory Federation Services (AD FS) per creare un trust della relying party per ogni nodo amministrativo nel sistema. È possibile creare trust di relying party utilizzando i comandi di PowerShell, importando metadati SAML da StorageGRID o immettendo i dati manualmente.

Prima di iniziare

- Hai configurato l'accesso Single Sign-On per StorageGRID e hai selezionato **AD FS** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere ["Utilizza la modalità sandbox"](#).
- Conosci il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte affidabile per ciascun nodo di amministrazione nel tuo sistema. È possibile trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina StorageGRID Single Sign-on.



È necessario creare un trust della relying party per ciascun nodo amministrativo nel sistema StorageGRID . La presenza di un trust di parte affidabile per ogni nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Hai esperienza nella creazione di trust relying party in AD FS oppure hai accesso alla documentazione di Microsoft AD FS.

- Stai utilizzando lo snap-in Gestione AD FS e appartieni al gruppo Amministratori.
- Se si crea manualmente il trust della relying party, si dispone del certificato personalizzato caricato per l'interfaccia di gestione StorageGRID oppure si sa come accedere a un nodo di amministrazione dalla shell dei comandi.

Informazioni su questo compito

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. Per qualsiasi domanda, consultare la documentazione di Microsoft AD FS.

Creare un trust della relying party utilizzando Windows PowerShell

È possibile utilizzare Windows PowerShell per creare rapidamente uno o più trust relying party.

Passi

1. Dal menu Start di Windows, seleziona con il pulsante destro del mouse l'icona di PowerShell e seleziona **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'identificatore della parte affidabile 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, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

3. Da Windows Server Manager, selezionare **Strumenti > Gestione AD FS**.

Viene visualizzato lo strumento di gestione AD FS.

4. Selezionare **AD FS > Trust delle parti affidabili**.

Viene visualizzato l'elenco dei trust delle parti affidanti.

5. Aggiungere una policy di controllo degli accessi al trust della relying party appena creato:
 - a. Individua il trust della parte affidabile che hai appena creato.
 - b. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica criterio di controllo degli accessi**.
 - c. Selezionare una politica di controllo degli accessi.
 - d. Selezionare **Applica** e selezionare **OK**
6. Aggiungere una politica di emissione dei reclami al trust della parte affidabile appena creato:
 - a. Individua il trust della parte affidabile che hai appena creato.
 - b. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.
 - c. Seleziona **Aggiungi regola**.
 - d. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e

seleziona **Avanti**.

e. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

Ad esempio, **ObjectGUID in Name ID** o **UPN in Name ID**.

f. Per l'Attribute Store, selezionare **Active Directory**.

g. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.

h. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.

i. Selezionare **Fine** e quindi **OK**.

7. Verificare che i metadati siano stati importati correttamente.

a. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.

b. Verificare che i campi nelle schede **Endpoint**, **Identificatori** e **Firma** siano compilati.

Se i metadati sono mancanti, verificare che l'indirizzo dei metadati della Federazione sia corretto oppure immettere i valori manualmente.

8. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .

9. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere "[Utilizzare la modalità Sandbox](#)" per istruzioni.

Creare un trust della parte affidabile importando i metadati della federazione

È possibile importare i valori per ciascun trust della relying party accedendo ai metadati SAML per ciascun nodo di amministrazione.

Passi

1. In Windows Server Manager, seleziona **Strumenti**, quindi seleziona **Gestione AD FS**.

2. In Azioni, seleziona **Aggiungi trust della parte affidabile**.

3. Nella pagina di benvenuto, seleziona **Richiedi informazioni** e seleziona **Avvia**.

4. Selezionare **Importa dati sulla parte affidabile pubblicati online o su una rete locale**.

5. In **Indirizzo metadati federazione (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, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

6. Completare la procedura guidata Trust della parte affidabile, salvare il trust della parte affidabile e chiudere la procedura guidata.



Quando si immette il nome visualizzato, utilizzare l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, SG-DC1-ADM1 .

7. Aggiungi una regola di rivendicazione:

- a. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.
- b. Seleziona **Aggiungi regola**:
- c. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e seleziona **Avanti**.
- d. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

Ad esempio, **ObjectGUID in Name ID** o **UPN in Name ID**.

- e. Per l'Attribute Store, selezionare **Active Directory**.
- f. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.
- g. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.
- h. Selezionare **Fine** e quindi **OK**.

8. Verificare che i metadati siano stati importati correttamente.

- a. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.
- b. Verificare che i campi nelle schede **Endpoint**, **Identificatori** e **Firma** siano compilati.

Se i metadati sono mancanti, verificare che l'indirizzo dei metadati della Federazione sia corretto oppure immettere i valori manualmente.

9. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .

10. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere ["Utilizzare la modalità Sandbox"](#) per istruzioni.

Creare manualmente un trust della parte affidabile

Se si sceglie di non importare i dati per i trust delle parti affidabili, è possibile immettere i valori manualmente.

Passi

1. In Windows Server Manager, seleziona **Strumenti**, quindi seleziona **Gestione AD FS**.
2. In Azioni, seleziona **Aggiungi trust della parte affidabile**.
3. Nella pagina di benvenuto, seleziona **Richiedi informazioni** e seleziona **Avvia**.
4. Selezionare **Inserisci manualmente i dati sulla parte affidabile** e selezionare **Avanti**.
5. Completare la procedura guidata Trust della parte affidabile:

- a. Inserisci un nome visualizzato per questo nodo di amministrazione.

Per coerenza, utilizzare l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, SG-DC1-ADM1 .

- b. Salta il passaggio per configurare un certificato di crittografia token facoltativo.
- c. Nella pagina Configura URL, seleziona la casella di controllo **Abilita supporto per il protocollo SAML 2.0 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, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

- e. Nella pagina Configura identificatori, specificare l'identificatore della parte affidabile per lo stesso nodo di amministrazione:

Admin_Node_Identifier

Per *Admin_Node_Identifier*, immettere l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, SG-DC1-ADM1.

- f. Rivedere le impostazioni, salvare il trust della relying party e chiudere la procedura guidata.

Viene visualizzata la finestra di dialogo Modifica policy di emissione reclami.



Se la finestra di dialogo non viene visualizzata, fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.

- 6. Per avviare la procedura guidata Claim Rules, seleziona **Aggiungi regola**:
 - a. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e seleziona **Avanti**.
 - b. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

Ad esempio, **ObjectGUID in Name ID** o **UPN in Name ID**.
 - c. Per l'Attribute Store, selezionare **Active Directory**.
 - d. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.
 - e. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.
 - f. Selezionare **Fine** e quindi **OK**.
- 7. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.
- 8. Nella scheda **Endpoint**, configurare l'endpoint per la disconnessione singola (SLO):
 - a. Selezionare **Aggiungi SAML**.
 - b. Selezionare **Tipo di endpoint > Disconnessione SAML**.
 - c. Selezionare **Associa > Reindirizza**.
 - d. Nel campo **URL attendibile**, 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, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

a. Selezionare **OK**.

9. Nella scheda **Firma**, specificare il certificato di firma per questo trust della parte affidabile:

a. Aggiungi il certificato personalizzato:

- Se disponi del certificato di gestione personalizzato caricato su StorageGRID, seleziona tale certificato.
- Se non si dispone del certificato personalizzato, accedere al nodo di amministrazione, andare su `/var/local/mgmt-api` directory del nodo di amministrazione e aggiungere il `custom-server.crt` file del certificato.



Utilizzo del certificato predefinito del nodo di amministrazione(`server.crt`) non è raccomandato. Se il nodo di amministrazione non funziona, il certificato predefinito verrà rigenerato quando si ripristina il nodo e sarà necessario aggiornare il trust della parte affidabile.

b. Selezionare **Applica** e quindi **OK**.

Le proprietà del relying party vengono salvate e chiuse.

10. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .

11. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere "[Utilizza la modalità sandbox](#)" per istruzioni.

Crea applicazioni aziendali in Azure AD

Puoi utilizzare Azure AD per creare un'applicazione aziendale per ogni nodo di amministrazione del tuo sistema.

Prima di iniziare

- Hai iniziato a configurare l'accesso Single Sign-On per StorageGRID e hai selezionato **Azure** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "[Utilizza la modalità sandbox](#)".
- Per ogni nodo amministrativo del sistema è disponibile il **nome dell'applicazione aziendale**. È possibile copiare questi valori dalla tabella dei dettagli del nodo di amministrazione nella pagina Single Sign-on StorageGRID .



È necessario creare un'applicazione aziendale per ciascun nodo amministrativo nel sistema StorageGRID . Disporre di un'applicazione aziendale per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

- Hai esperienza nella creazione di applicazioni aziendali in Azure Active Directory.
- Hai un account Azure con una sottoscrizione attiva.
- Nell'account Azure ricopri uno dei seguenti ruoli: amministratore globale, amministratore dell'applicazione cloud, amministratore dell'applicazione o proprietario dell'entità servizio.

Accedi ad Azure AD

Passi

1. Accedi al "[Portale di Azure](#)".
2. Vai a "[Azure Active Directory](#)".
3. Selezionare "[Applicazioni aziendali](#)".

Crea applicazioni aziendali e salva la configurazione StorageGRID SSO

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 campi **URL metadati della federazione** corrispondenti nella pagina Single Sign-on di StorageGRID.

Passi

1. Ripetere i seguenti passaggi per ciascun nodo di amministrazione.
 - a. Nel riquadro Applicazioni aziendali di Azure, seleziona **Nuova applicazione**.
 - b. Seleziona **Crea la tua applicazione**.
 - c. Per il nome, immettere il **Nome dell'applicazione aziendale** copiato dalla tabella dei dettagli del nodo di amministrazione nella pagina Single Sign-on StorageGRID.
 - d. Lascia selezionato il pulsante di opzione **Integra qualsiasi altra applicazione non presente nella galleria (Non nella galleria)**.
 - e. Seleziona **Crea**.
 - f. Selezionare il link **Inizia** nel **2. Impostare la casella Single Sign-On** oppure selezionare il collegamento **Single Sign-On** sul margine sinistro.
 - g. Selezionare la casella **SAML**.
 - h. Copia l'**URL dei metadati della federazione app**, che puoi trovare in **Certificato di firma SAML del passaggio 3**.
 - i. Vai alla pagina StorageGRID Single Sign-on e incolla l'URL nel campo **URL metadati federazione** che corrisponde al **Nome applicazione aziendale** utilizzato.
2. Dopo aver incollato un URL dei metadati di federazione per ciascun nodo di amministrazione e aver apportato tutte le altre modifiche necessarie alla configurazione SSO, selezionare **Salva** nella pagina StorageGRID Single Sign-on.

Scarica i metadati SAML per ogni nodo amministrativo

Dopo aver salvato la configurazione SSO, puoi scaricare un file di metadati SAML per ogni nodo amministrativo nel tuo sistema StorageGRID.

Passi

1. Ripetere questi passaggi per ogni nodo di amministrazione.

- a. Sign in a StorageGRID dal nodo di amministrazione.
- b. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
- c. Selezionare il pulsante per scaricare i metadati SAML per quel nodo di amministrazione.
- d. Salva il file che caricherai in Azure AD.

Carica i metadati SAML in ogni applicazione aziendale

Dopo aver scaricato un file di metadati SAML per ogni nodo di amministrazione StorageGRID , eseguire i seguenti passaggi in Azure AD:

Passi

1. Torna al portale di Azure.
2. Ripetere questi passaggi per ogni applicazione aziendale:



Potrebbe essere necessario aggiornare la pagina Applicazioni aziendali per visualizzare le applicazioni aggiunte in precedenza all'elenco.

- a. Vai 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 metadati** e selezionare il file metadati SAML scaricato per il nodo di amministrazione corrispondente.
 - f. Dopo aver caricato il file, seleziona **Salva** e poi **X** per chiudere il riquadro. Verrai reindirizzato alla pagina Imposta Single Sign-On con SAML.
3. Segui i passaggi in "[Utilizza la modalità sandbox](#)" per testare ogni applicazione.

Crea connessioni al fornitore di servizi (SP) in PingFederate

Puoi utilizzare PingFederate per creare una connessione al provider di servizi (SP) per ogni nodo amministrativo del tuo sistema. Per velocizzare il processo, importerai i metadati SAML da StorageGRID.

Prima di iniziare

- Hai configurato l'accesso Single Sign-On per StorageGRID e hai selezionato **Ping Federate** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "[Utilizza la modalità sandbox](#)".
- Hai l'*ID di connessione SP * per ogni nodo amministrativo nel tuo sistema. È possibile trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina StorageGRID Single Sign-on.
- Hai scaricato i **metadati SAML** per ogni nodo amministrativo nel tuo sistema.
- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Tu hai
il https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html ["Guida di riferimento dell'amministratore"] per PingFederate Server. La documentazione

di PingFederate fornisce istruzioni e spiegazioni dettagliate passo dopo passo.

- Tu hai il "[Autorizzazione di amministratore](#)" per PingFederate Server.

Informazioni su questo compito

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 tua versione, consulta la documentazione di PingFederate Server.

Prerequisiti completi in PingFederate

Prima di poter creare le connessioni SP che utilizzerai per StorageGRID, devi completare le attività preliminari in PingFederate. Le informazioni ricavate da questi prerequisiti verranno utilizzate durante la configurazione delle connessioni SP .

Crea archivio dati

Se non lo hai già fatto, crea un archivio dati per connettere PingFederate al server LDAP di AD FS. Utilizza i valori che hai utilizzato quando "[configurazione della federazione delle identità](#)" in StorageGRID.

- **Tipo:** Directory (LDAP)
- **Tipo LDAP:** Active Directory
- **Nome attributo binario:** immettere **objectGUID** nella scheda Attributi binari LDAP esattamente come mostrato.

Crea un validatore di credenziali password

Se non l'hai già fatto, crea un validatore di credenziali password.

- **Tipo:** Nome utente LDAP Password Validatore credenziali
- **Archivio dati:** seleziona l'archivio dati che hai creato.
- **Base di ricerca:** immettere le informazioni da LDAP (ad esempio, DC=saml,DC=sgws).
- **Filtro di ricerca:** sAMAccountName=\${username}
- **Ambito:** Sottoalbero

Crea istanza dell'adattatore IdP

Se non l'hai già fatto, crea un'istanza dell'adattatore IdP.

Passi

1. Vai su **Autenticazione > Integrazione > Schede IdP**.
2. Selezionare **Crea nuova istanza**.
3. Nella scheda Tipo, seleziona **Adattatore IdP modulo HTML**.
4. Nella scheda IdP Adapter, seleziona **Aggiungi una nuova riga a 'Validatori di credenziali'**.
5. Seleziona il [validatore di credenziali password](#) che hai creato.
6. Nella scheda Attributi adattatore, selezionare l'attributo **username** per **Pseudonimo**.
7. Seleziona **Salva**.

Crea o importa il certificato di firma

Se non l'hai già fatto, crea o importa il certificato di firma.

Passi

1. Vai a **Sicurezza > Chiavi e certificati di firma e decrittazione**.
2. Creare o importare il certificato di firma.

Crea 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 di cui hai bisogno.



È necessario creare una connessione SP per ciascun nodo di amministrazione nel sistema StorageGRID, in modo che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo. Utilizzare queste istruzioni per creare la prima connessione SP. Poi vai a [Crea connessioni SP aggiuntive](#) per creare eventuali connessioni aggiuntive di cui hai bisogno.

Scegli il tipo di connessione SP

Passi

1. Vai su **Applicazioni > Integrazione > *Connessioni SP ***.
2. Seleziona **Crea connessione**.
3. Seleziona **Non utilizzare un modello per questa connessione**.
4. Selezionare **Profili SSO del browser** e **SAML 2.0** come protocollo.

Importa metadati SP

Passi

1. Nella scheda Importa metadati, seleziona **File**.
2. Seleziona il file di metadati SAML scaricato dalla pagina Single Sign-On StorageGRID per il nodo di amministrazione.
3. Esaminare il Riepilogo dei metadati e le informazioni fornite nella scheda Informazioni generali.

L'ID entità del partner e il nome della connessione sono impostati sull'ID di 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 l'SSO del browser IdP

Passi

1. Dalla scheda Browser SSO, seleziona **Configura Browser SSO**.
2. Nella scheda Profili SAML, seleziona le opzioni *** SP-initiated SSO***, *** SP-initial SLO***, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selezionare **Avanti**.
4. Nella scheda Durata asserzione, non apportare modifiche.

5. Nella scheda Creazione asserzione, selezionare **Configura creazione asserzione**.
 - a. Nella scheda Mappatura identità, selezionare **Standard**.
 - b. Nella scheda Contratto attributo, utilizzare **SAML_SUBJECT** come Contratto attributo e il formato del nome non specificato che è stato importato.
6. Per estendere il contratto, selezionare **Elimina** per rimuovere il `urn:oid`, che non viene utilizzato.

Istanza dell'adattatore della mappa

Passi

1. Nella scheda Mapping origine autenticazione, selezionare **Mappa nuova istanza adattatore**.
2. Nella scheda Istanza adattatore, selezionare **istanza dell'adattatore** che hai creato.
3. Nella scheda Metodo di mappatura, seleziona **Recupera attributi aggiuntivi da un archivio dati**.
4. Nella scheda Origine attributo e ricerca utente, seleziona **Aggiungi origine attributo**.
5. Nella scheda Archivio dati, fornire una descrizione e selezionare **archivio dati** hai aggiunto.
6. Nella scheda Ricerca directory LDAP:
 - Immettere il **DN di base**, che deve corrispondere esattamente al valore immesso in StorageGRID per il server LDAP.
 - Per l'ambito di ricerca, selezionare **Sottoalbero**.
 - Per la classe dell'oggetto radice, cercare e aggiungere uno di questi attributi: **objectGUID** o **userPrincipalName**.
7. Nella scheda Tipi di codifica degli attributi binari LDAP, selezionare **Base64** per l'attributo **objectGUID**.
8. Nella scheda Filtro LDAP, immettere **sAMAccountName=\${username}**.
9. Nella scheda Adempimento contratto attributi, seleziona **LDAP (attributo)** dal menu a discesa Origine e seleziona **objectGUID** o **userPrincipalName** dal menu a discesa Valore.
10. Rivedere e quindi salvare la fonte dell'attributo.
11. Nella scheda Failsave Attribute Source, seleziona **Abort the SSO Transaction**.
12. Rivedi il riepilogo e seleziona **Fine**.
13. Selezionare **Fatto**.

Configurare le impostazioni del protocollo

Passi

1. Nella scheda **Connessione SP * > *SSO browser > Impostazioni protocollo**, selezionare **Configura impostazioni protocollo**.
2. Nella scheda URL del servizio consumer di asserzione, accettare i valori predefiniti, che sono stati importati dai metadati SAML StorageGRID (**POST** per Binding e `/api/saml-response` per l'URL dell'endpoint).
3. Nella scheda URL del servizio SLO, accettare i valori predefiniti, che sono stati importati dai metadati SAML StorageGRID (**REDIRECT** per Binding e `/api/saml-logout` per l'URL dell'endpoint).
4. Nella scheda Binding SAML consentiti, deselezionare **ARTIFACT** e **SOAP**. Sono richiesti solo **POST** e **REDIRECT**.
5. Nella scheda Criterio di firma, lasciare selezionate le caselle di controllo **Richiedi la firma delle richieste di autorizzazione** e **Firma sempre l'asserzione**.

6. Nella scheda Criterio di crittografia, selezionare **Nessuno**.
7. Rivedi il riepilogo e seleziona **Fine** per salvare le impostazioni del protocollo.
8. Rivedi il riepilogo e seleziona **Fine** per salvare le impostazioni SSO del browser.

Configurare le credenziali

Passi

1. Dalla scheda Connessione SP , selezionare **Credenziali**.
2. Dalla scheda Credenziali, seleziona **Configura credenziali**.
3. Seleziona il [certificato di firma](#) che hai creato o importato.
4. Selezionare **Avanti** per andare a **Gestisci impostazioni di verifica della firma**.
 - a. Nella scheda Modello di fiducia, seleziona **Non ancorato**.
 - b. Nella scheda Certificato di verifica della firma, rivedere le informazioni sul certificato di firma, importate dai metadati SAML StorageGRID .
5. Rivedere le schermate di riepilogo e selezionare **Salva** per salvare la connessione SP .

Crea connessioni SP aggiuntive

Puoi copiare la prima connessione SP per creare le connessioni SP necessarie per ogni nodo amministrativo nella tua griglia. Carichi nuovi metadati per ogni copia.



Le connessioni SP per diversi nodi amministrativi utilizzano impostazioni identiche, ad eccezione dell'ID entità del partner, dell'URL di base, dell'ID connessione, del nome della connessione, della verifica della firma e dell'URL di risposta SLO.

Passi

1. Selezionare **Azione > Copia** per creare una copia della connessione SP iniziale per ogni nodo amministrativo aggiuntivo.
2. Inserisci l'ID connessione e il Nome connessione per la copia e seleziona **Salva**.
3. Selezionare il file di metadati corrispondente al nodo di amministrazione:
 - a. Selezionare **Azione > Aggiorna con metadati**.
 - b. Seleziona **Scegli file** e carica i metadati.
 - c. Selezionare **Avanti**.
 - d. Seleziona **Salva**.
4. Risolvi l'errore dovuto all'attributo non utilizzato:
 - a. Selezionare la nuova connessione.
 - b. Selezionare **Configura SSO browser > Configura creazione asserzione > Contratto attributo**.
 - c. Elimina la voce per **urn:oid**.
 - d. Seleziona **Salva**.

Disabilitare l'accesso singolo

Se non si desidera più utilizzare questa funzionalità, è possibile disattivare l'accesso Single Sign-On (SSO). È necessario disabilitare l'accesso singolo prima di poter

disabilitare la federazione delle identità.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Passi

1. Selezionare **CONFIGURAZIONE** > **Controllo accessi** > **Single sign-on**.

Viene visualizzata la pagina Single Sign-on.

2. Selezionare l'opzione **Disabilitato**.
3. Seleziona **Salva**.

Viene visualizzato un messaggio di avviso che indica che ora gli utenti locali potranno effettuare l'accesso.

4. Selezionare **OK**.

Al successivo accesso a StorageGRID , verrà visualizzata la pagina Sign in a StorageGRID e sarà necessario immettere il nome utente e la password di un utente StorageGRID locale o federato.

Disattivare e riattivare temporaneamente l'accesso singolo per un nodo di amministrazione

Potresti non essere in grado di accedere a Grid Manager se il sistema Single Sign-On (SSO) non funziona. In questo caso, puoi disattivare e riattivare temporaneamente l'SSO per un nodo di amministrazione. Per disattivare e riattivare l'SSO, è necessario accedere alla shell dei comandi del nodo.

Prima di iniziare

- Hai ["autorizzazioni di accesso specifiche"](#) .
- Tu hai il `Passwords.txt` file.
- Conosci la password dell'utente root locale.

Informazioni su questo compito

Dopo aver disabilitato l'SSO per un nodo di amministrazione, puoi accedere a Grid Manager come utente root locale. Per proteggere il sistema StorageGRID , è necessario utilizzare la shell dei comandi del nodo per riabilitare l'SSO sul nodo di amministrazione non appena si esegue la disconnessione.



La disabilitazione dell'SSO per un nodo amministrativo non influisce sulle impostazioni SSO per gli altri nodi amministrativi nella griglia. La casella di controllo **Abilita SSO** nella pagina Single Sign-on in Grid Manager rimane selezionata e tutte le impostazioni SSO esistenti vengono mantenute a meno che non vengano aggiornate.

Passi

1. Accedi a un nodo di amministrazione:
 - a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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. Conferma che vuoi disabilitare l'SSO.

Un messaggio indica che l'accesso singolo è disabilitato sul nodo.

4. Da un browser Web, accedi a Grid Manager sullo stesso nodo di amministrazione.

Ora viene visualizzata la pagina di accesso di Grid Manager perché l'SSO è stato disabilitato.

5. Sign in con il nome utente root e la password dell'utente root locale.

6. Se hai disabilitato temporaneamente l'SSO perché dovevi correggere la configurazione dell'SSO:

- Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
- Modifica le impostazioni SSO errate o obsolete.
- Seleziona **Salva**.

Selezionando **Salva** dalla pagina Single Sign-on, l'SSO viene automaticamente riattivato per l'intera griglia.

7. Se hai disabilitato temporaneamente l'SSO perché avevi bisogno di accedere a Grid Manager per qualche altro motivo:

- Esegui qualsiasi compito o compiti che devi svolgere.
- Selezionare **Esci** e chiudere Grid Manager.
- Riattivare SSO sul nodo di amministrazione. È possibile eseguire uno dei seguenti passaggi:

- Eseguire il seguente comando: `enable-saml`

Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

Conferma di voler abilitare l'SSO.

Un messaggio indica che l'accesso singolo è abilitato sul nodo.

- Riavviare il nodo della griglia: `reboot`

8. Da un browser Web, accedere a Grid Manager dallo stesso nodo di amministrazione.

9. Verificare che venga visualizzata la pagina Sign in a StorageGRID e che sia necessario immettere le credenziali SSO per accedere a Grid Manager.

Utilizzare la federazione di griglia

Che cos'è la federazione di rete?

È possibile utilizzare la federazione di griglia per clonare i tenant e replicare i loro oggetti

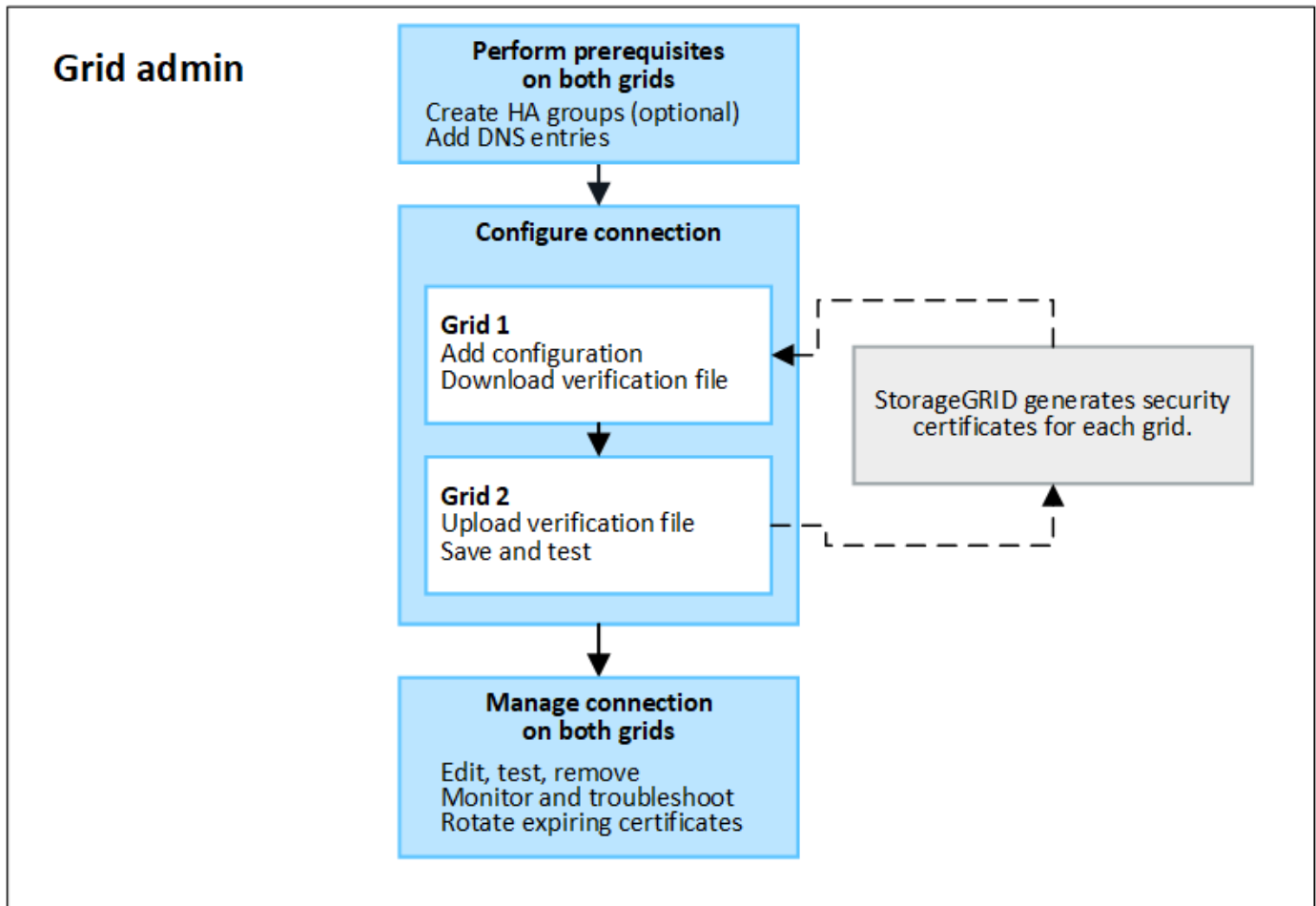
tra due sistemi StorageGRID per il ripristino di emergenza.

Che cos'è una connessione di federazione di rete?

Una connessione di federazione di griglia è una connessione bidirezionale, affidabile e sicura tra nodi di amministrazione e gateway in due sistemi StorageGRID .

Flusso di lavoro per la federazione della griglia

Il diagramma del flusso di lavoro riassume i passaggi per configurare una connessione di federazione di griglia tra due griglie.



Considerazioni e requisiti per le connessioni della federazione di rete

- Le griglie utilizzate per la federazione delle griglie devono eseguire versioni StorageGRID identiche o che non presentino più di una differenza di versione principale tra loro.

Per i dettagli sui requisiti di versione, fare riferimento a ["Note di rilascio"](#) .

- Una rete può avere una o più connessioni di federazione di rete ad altre reti. Ogni connessione della federazione di rete 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 vi è alcuna connessione implicita tra la Griglia 2 e la Griglia 3.
- Le connessioni della federazione di rete sono bidirezionali. Una volta stabilita la connessione, è possibile monitorarla e gestirla da entrambe le griglie.

- Deve esistere almeno una connessione di federazione di griglia prima di poter utilizzare ["clonazione dell'account"](#) O ["replicazione cross-grid"](#) .

Requisiti di rete e indirizzo IP

- Le connessioni di federazione della griglia possono verificarsi sulla rete della griglia, sulla rete di amministrazione o sulla rete client.
- Una connessione di federazione di rete collega una rete a un'altra rete. La configurazione per ciascuna griglia specifica un endpoint di federazione della griglia sull'altra griglia che è composta da nodi amministrativi, nodi gateway o entrambi.
- La pratica migliore è quella di connettersi ["gruppi ad alta disponibilità \(HA\)"](#) di nodi gateway e amministrativi su ciascuna griglia. L'utilizzo di gruppi HA aiuta a garantire che le connessioni della federazione di griglia rimangano online anche se i nodi non sono disponibili. Se l'interfaccia attiva in uno dei gruppi HA fallisce, la connessione può utilizzare un'interfaccia di backup.
- Non è consigliabile creare una connessione di federazione di griglia che utilizzi l'indirizzo IP di un singolo nodo di amministrazione o di un nodo gateway. Se il nodo non è più disponibile, anche la connessione alla federazione di rete non sarà più disponibile.
- ["Replicazione cross-grid"](#) degli oggetti richiede che i nodi di archiviazione su ciascuna griglia siano in grado di accedere ai nodi di amministrazione e gateway configurati sull'altra griglia. Per ogni griglia, verificare che tutti i nodi di archiviazione dispongano di un percorso ad alta larghezza di banda come i nodi di amministrazione o i nodi gateway utilizzati per la connessione.

Utilizzare i nomi di dominio completi (FQDN) per bilanciare il carico della connessione

Per un ambiente di produzione, utilizzare nomi di dominio completi (FQDN) per identificare ciascuna griglia nella connessione. Quindi, creare le voci DNS appropriate, come segue:

- FQDN per Grid 1 mappato a uno o più indirizzi IP virtuali (VIP) per gruppi HA in Grid 1 o all'indirizzo IP di uno o più nodi Admin o Gateway in Grid 1.
- FQDN per Grid 2 mappato a uno o più indirizzi VIP per Grid 2 o all'indirizzo IP di uno o più nodi Admin o Gateway in Grid 2.

Quando si utilizzano più voci DNS, le richieste di utilizzo della connessione vengono bilanciate nel modo seguente:

- Le voci DNS che mappano gli indirizzi VIP di più gruppi HA vengono bilanciate tra i nodi attivi nei gruppi HA.
- Le voci DNS che corrispondono agli indirizzi IP di più nodi amministrativi o nodi gateway vengono bilanciate tra i nodi mappati.

Requisiti portuali

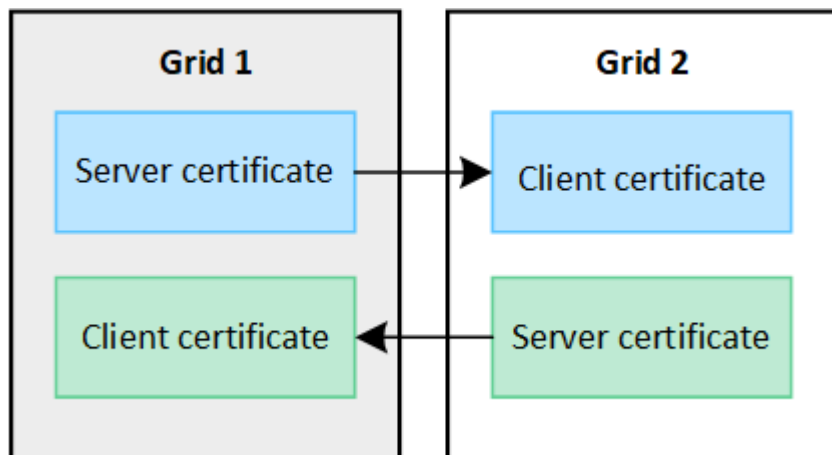
Quando si crea una connessione di federazione di griglia, è possibile specificare qualsiasi numero di porta non utilizzato compreso tra 23000 e 23999. Entrambe le griglie in questa connessione utilizzeranno la stessa porta.

È necessario assicurarsi che nessun nodo in entrambe le griglie utilizzi questa porta per altre connessioni.

Requisiti del certificato

Quando si configura una connessione di federazione di griglia, 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 si avvicinano alla data di scadenza, l'avviso **Scadenza del certificato di federazione della griglia** ti ricorda di ruotare i certificati, operazione che puoi effettuare tramite Grid Manager.



Se i certificati su una delle estremità della connessione scadono, la connessione smetterà di funzionare. La replica dei dati sarà sospesa finché i certificati non saranno aggiornati.

Saperne di più

- ["Creare connessioni di federazione di griglia"](#)
- ["Gestire le connessioni della federazione di rete"](#)
- ["Risolvere gli errori di federazione della griglia"](#)

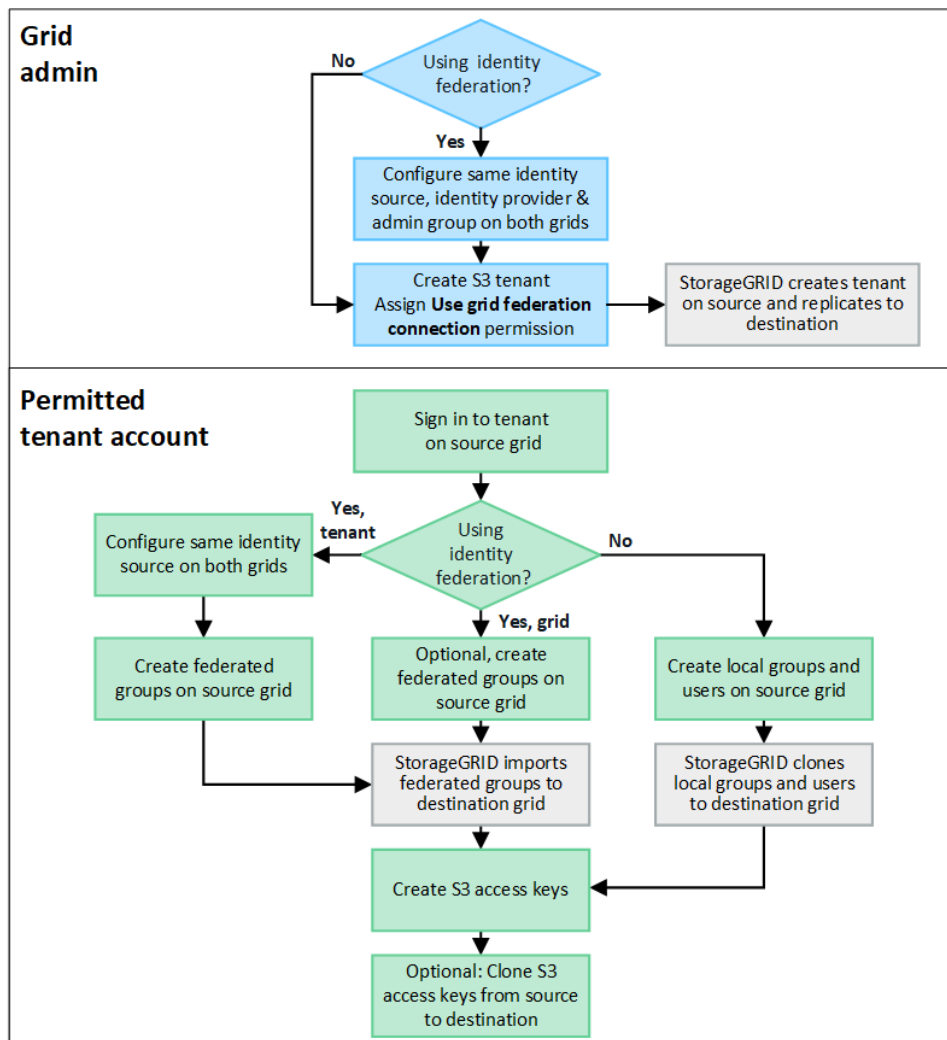
Che cos'è il clone dell'account?

Il clone dell'account è la replica automatica di un account tenant, gruppi tenant, utenti tenant e, facoltativamente, chiavi di accesso S3 tra i sistemi StorageGRID in un ["collegamento della federazione di rete"](#).

È richiesto il clone dell'account per ["replicazione cross-grid"](#). La clonazione delle informazioni dell'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.

Flusso di lavoro per la clonazione dell'account

Il diagramma del flusso di lavoro mostra i passaggi che gli amministratori della griglia e i tenant autorizzati eseguiranno per configurare il clone dell'account. Questi passaggi vengono eseguiti dopo l'["la connessione della federazione di griglia è configurata"](#).



Flusso di lavoro dell'amministratore della griglia

I passaggi eseguiti dagli amministratori della griglia dipendono dal fatto che i sistemi StorageGRID nel "[collegamento della federazione di rete](#)" utilizzare l'accesso singolo (SSO) o la federazione delle identità.

Configura SSO per il clone dell'account (facoltativo)

Se uno dei sistemi StorageGRID nella connessione di federazione della griglia utilizza SSO, entrambe le griglie devono utilizzare SSO. Prima di creare gli account tenant per la federazione della griglia, gli amministratori della griglia di origine e di destinazione del tenant devono eseguire questi passaggi.

Passi

1. Configurare la stessa origine identità per entrambe le griglie. Vedere "[Utilizzare la federazione delle identità](#)".
2. Configurare lo stesso provider di identità SSO (IdP) per entrambe le griglie. Vedere "[Configurare l'accesso singolo](#)".
3. "[Crea lo stesso gruppo di amministratori](#)" su entrambe le griglie importando lo stesso gruppo federato.

Quando si crea il tenant, si selezionerà questo gruppo per avere l'autorizzazione di accesso Root iniziale sia per l'account tenant di origine che per quello di destinazione.



Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non verrà replicato nella destinazione.

Configura la federazione delle identità a livello di griglia per il clone dell'account (facoltativo)

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 della griglia, gli amministratori della griglia di origine e di destinazione del tenant devono eseguire questi passaggi.

Passi

1. Configurare la stessa origine identità per entrambe le griglie. Vedere ["Utilizzare la federazione delle identità"](#).
2. Facoltativamente, se un gruppo federato avrà l'autorizzazione di accesso Root iniziale sia per gli account tenant di origine che di destinazione, ["creare lo stesso gruppo di amministratori"](#) su entrambe le griglie importando lo stesso gruppo federato.



Se si assegna l'autorizzazione di accesso Root a un gruppo federato che non esiste su entrambe le griglie, il tenant non viene replicato nella griglia di destinazione.

3. Se non si desidera che un gruppo federato disponga inizialmente dell'autorizzazione di accesso Root per entrambi gli account, specificare una password per l'utente root locale.

Crea un account tenant S3 consentito

Dopo aver configurato facoltativamente SSO o federazione delle identità, un amministratore della griglia esegue questi passaggi per determinare quali tenant possono replicare oggetti bucket su altri sistemi StorageGRID.

Passi

1. Determina quale griglia desideri che sia la griglia di origine del tenant per le operazioni di clonazione dell'account.

La griglia in cui il tenant viene creato originariamente è nota come *griglia sorgente* del tenant. La griglia in cui viene replicato il tenant è nota come *griglia di destinazione* del tenant.

2. Su quella griglia, crea un nuovo account tenant S3 o modifica un account esistente.
3. Assegnare l'autorizzazione **Usa connessione federazione griglia**.
4. Se l'account tenant gestirà i propri utenti federati, assegnare l'autorizzazione **Utilizza la propria origine identità**.

Se viene assegnata questa autorizzazione, sia l'account tenant di origine che quello 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 identità.

5. Selezionare una connessione federata di rete specifica.
6. Salva il tenant nuovo o modificato.

Quando viene salvato un nuovo tenant con l'autorizzazione **Usa connessione federazione griglia**, StorageGRID crea automaticamente una replica di tale tenant sull'altra griglia, come segue:

- Entrambi gli account tenant hanno lo stesso ID account, nome, quota di archiviazione e autorizzazioni assegnate.
- Se hai selezionato un gruppo federato con autorizzazione di accesso Root per il tenant, quel gruppo viene clonato nel tenant di destinazione.
- Se hai selezionato un utente locale con autorizzazione di accesso Root per il tenant, tale utente verrà clonato nel tenant di destinazione. Tuttavia, la password di quell'utente non viene clonata.

Per maggiori dettagli, vedere ["Gestire gli inquilini autorizzati per la federazione della rete"](#).

Flusso di lavoro dell'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 questi passaggi per clonare gruppi tenant, utenti e chiavi di accesso S3.

Passi

1. Sign in all'account del tenant nella griglia di origine del tenant.
2. Se consentito, configurare la federazione delle identità sia sugli account tenant di origine che di destinazione.
3. Creare gruppi e utenti sul tenant di origine.

Quando vengono creati nuovi gruppi o utenti sul tenant di origine, StorageGRID li clona automaticamente sul tenant di destinazione, ma non avviene alcuna clonazione 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.

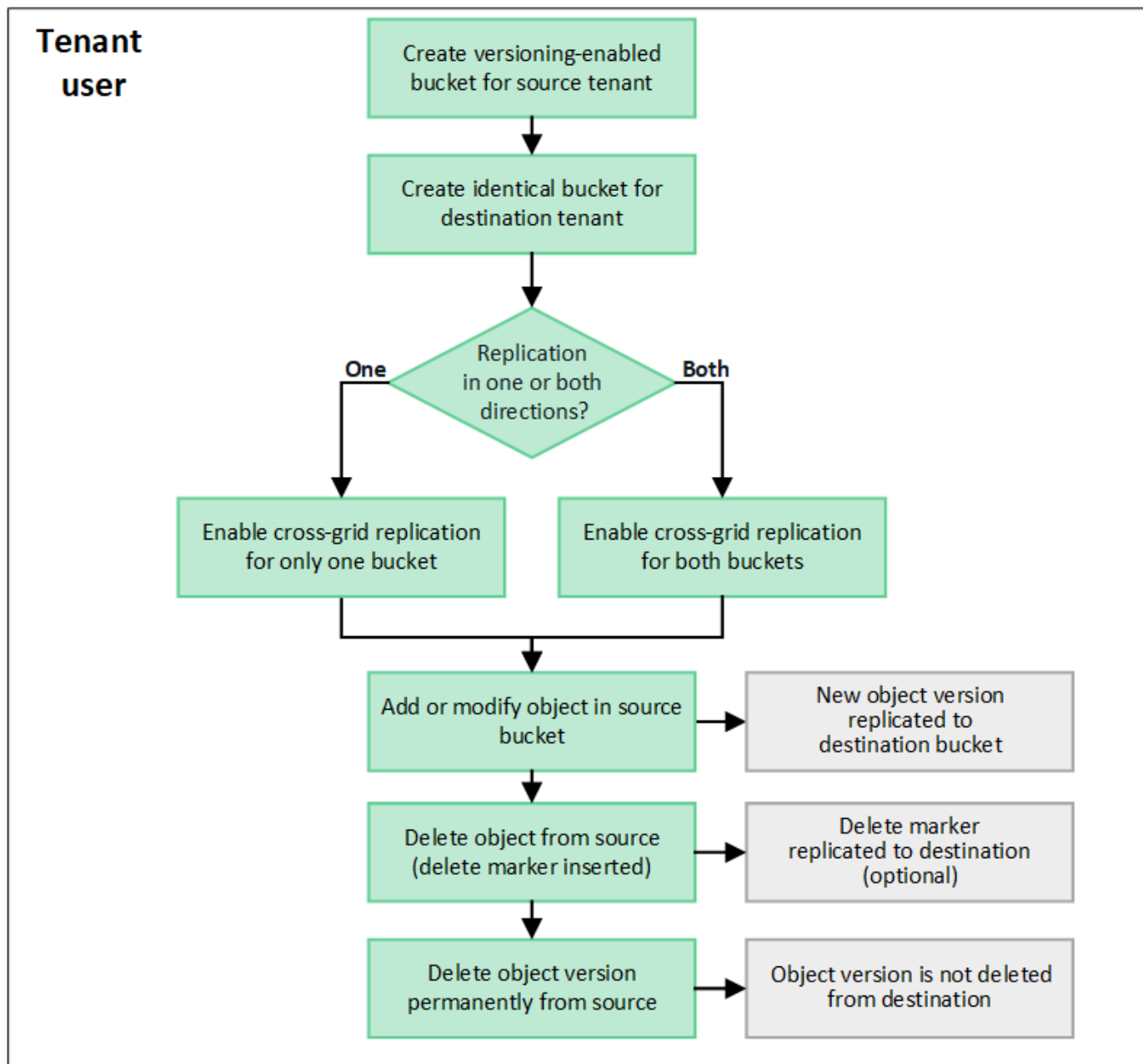
Per i dettagli sul flusso di lavoro dell'account tenant consentito e per sapere come vengono clonati gruppi, utenti e chiavi di accesso S3, vedere ["Clona gruppi tenant e utenti"](#) E ["Clona le chiavi di accesso S3 utilizzando l'API"](#).

Che cos'è la replicazione cross-grid?

La replicazione cross-grid è la replicazione automatica di oggetti tra bucket S3 selezionati in due sistemi StorageGRID connessi in un ["collegamento della federazione di rete"](#). ["Clonazione dell'account"](#) è necessario per la replicazione tra griglie.

Flusso di lavoro per la replicazione tra griglie

Il diagramma del flusso di lavoro riassume i passaggi per configurare la replica tra griglie tra bucket su due griglie.



Requisiti per la replicazione cross-grid

Se un account tenant ha l'autorizzazione **Usa connessione federazione griglia** per utilizzare una o più ["connessioni della federazione di rete"](#), un utente tenant con autorizzazione di accesso Root può creare bucket identici negli account tenant corrispondenti su ciascuna griglia. Questi secchi:

- Deve avere lo stesso nome ma può avere regioni diverse
- Deve essere abilitato il controllo delle versioni
- Deve avere il blocco oggetto S3 disabilitato
- Deve essere vuoto

Dopo aver creato entrambi i bucket, è possibile configurare la replica tra griglie per uno o entrambi i bucket.

Saperne di più

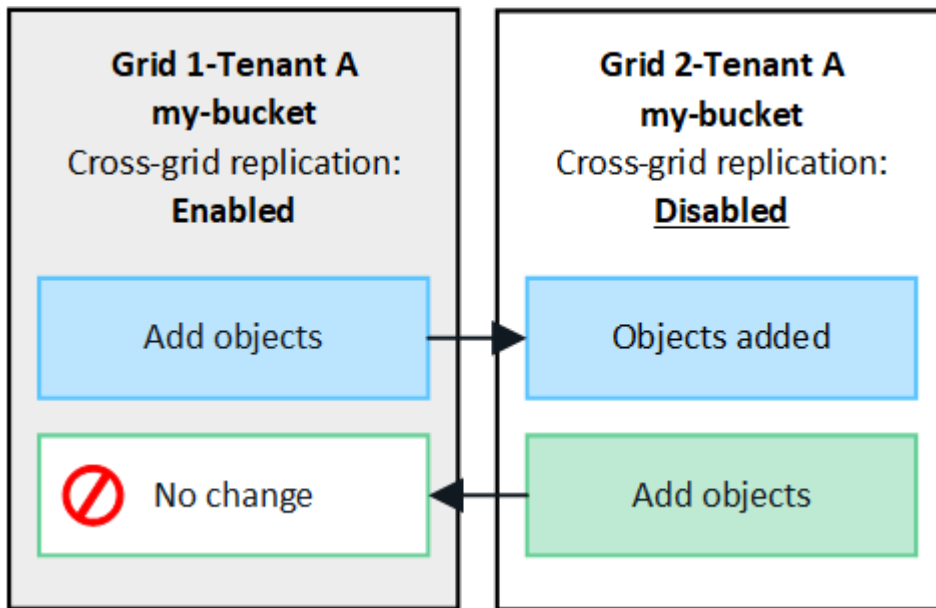
["Gestire la replicazione tra griglie"](#)

Come funziona la replicazione cross-grid

La replicazione tra griglie può essere configurata in modo che avvenga in una direzione o in entrambe le direzioni.

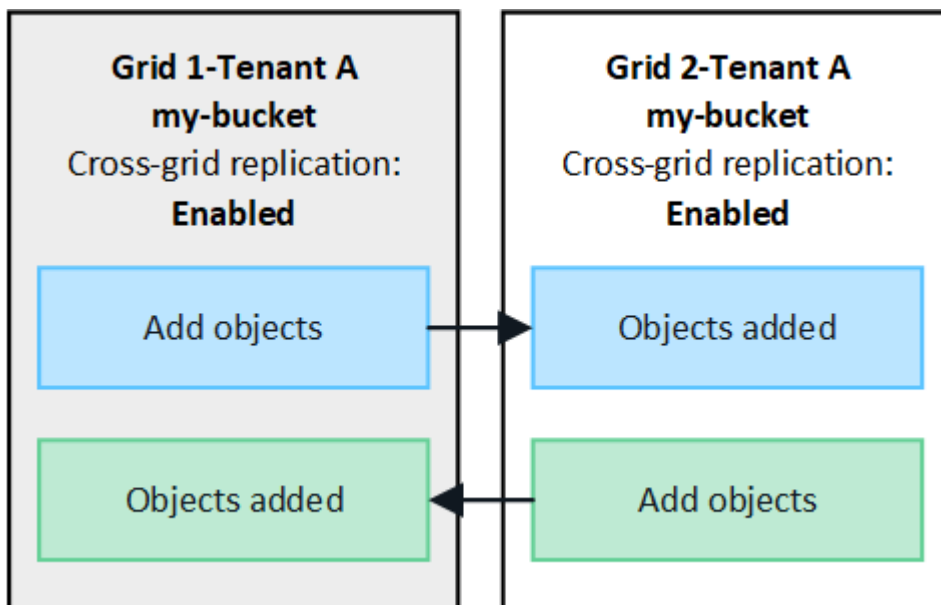
Replicazione in una direzione

Se si abilita la replica tra griglie 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 nell'origine. Nella figura, la replicazione cross-grid è abilitata per `my-bucket` dalla Griglia 1 alla Griglia 2, ma non è abilitato nella direzione opposta.



Replicazione in entrambe le direzioni

Se si abilita la replica tra griglie per lo stesso bucket su entrambe le griglie, gli oggetti aggiunti a uno dei due bucket vengono replicati sull'altra griglia. Nella figura, la replicazione cross-grid è abilitata per `my-bucket` in entrambe le direzioni.



Cosa succede quando gli oggetti vengono ingeriti?

Quando un client S3 aggiunge un oggetto a un bucket in cui è abilitata la replica tra griglie, 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 replicazione di un oggetto inviando una richiesta `GetObject` o `HeadObject`. La risposta include uno StorageGRID specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori: Il client S3 può verificare lo stato di replicazione di un oggetto emettendo una richiesta `GetObject` o `HeadObject`. La risposta include uno StorageGRID specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	• COMPLETO: La replica è riuscita per tutte le connessioni alla rete. • IN ATTESA: l'oggetto non è stato replicato su almeno una connessione alla griglia. • ERRORE: la replica non è in sospeso per nessuna connessione alla rete e almeno una è fallita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	REPLICA: L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta il `x-amz-replication-status` intestazione.

2. StorageGRID utilizza le policy ILM attive di ogni griglia per gestire gli oggetti, proprio come farebbe con qualsiasi altro oggetto. Ad esempio, l'Oggetto A sulla Griglia 1 potrebbe essere archiviato come due copie replicate e conservato per sempre, mentre la copia dell'Oggetto A replicata sulla Griglia 2 potrebbe essere archiviata utilizzando la codifica di cancellazione 2+1 ed eliminata dopo tre anni.

Cosa succede quando gli oggetti vengono eliminati?

Come descritto in "[Elimina flusso di dati](#)" StorageGRID può eliminare un oggetto per uno qualsiasi di questi motivi:

- Il client S3 invia una richiesta di eliminazione.
- Un utente Tenant Manager seleziona "[Elimina 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 specificati ulteriori posizionamenti.

Quando StorageGRID elimina un oggetto a causa di un'operazione di eliminazione degli oggetti nel bucket, della scadenza del ciclo di vita del bucket o della scadenza del posizionamento ILM, l'oggetto replicato non viene mai eliminato dall'altra griglia in una connessione di federazione di griglia. Tuttavia, i marcatori di eliminazione aggiunti al bucket di origine dalle eliminazioni del client S3 possono essere facoltativamente

replicati nel bucket di destinazione.

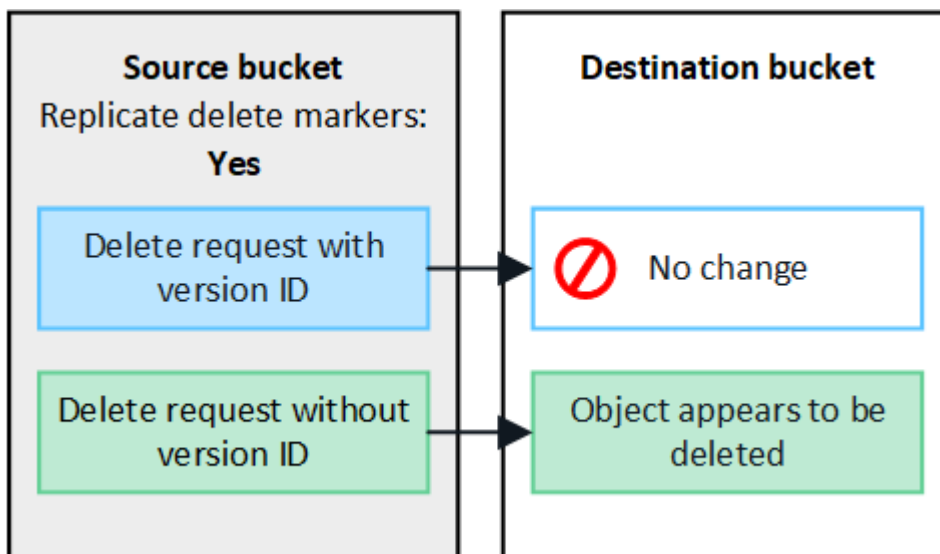
Per capire cosa succede quando un client S3 elimina oggetti da un bucket in cui è abilitata la replica tra griglie, esamina come i client S3 eliminano oggetti dai bucket in cui è abilitato il controllo delle versioni, come segue:

- Se un client S3 invia una richiesta di eliminazione che include un ID versione, quella versione dell'oggetto viene rimossa definitivamente. Nessun marcatore di eliminazione viene aggiunto al bucket.
- Se un client S3 invia una richiesta di eliminazione che non include un ID versione, StorageGRID non elimina alcuna versione dell'oggetto. Invece, aggiunge un marcatore di eliminazione al bucket. Il marcatore di eliminazione fa sì che StorageGRID agisca come se l'oggetto fosse stato eliminato:
 - Una richiesta `GetObject` senza un ID versione fallirà con `404 No Object Found`
 - Una richiesta `GetObject` con un ID versione valido avrà esito positivo e restituirà la versione dell'oggetto richiesta.

Quando un client S3 elimina un oggetto da un bucket in cui è abilitata la replica tra griglie, StorageGRID determina se replicare la richiesta di eliminazione nella destinazione, come segue:

- Se la richiesta di eliminazione include un ID versione, la versione dell'oggetto viene rimossa definitivamente dalla griglia di origine. Tuttavia, StorageGRID non replica le richieste di eliminazione che includono un ID versione, quindi la stessa versione dell'oggetto non viene eliminata dalla destinazione.
- Se la richiesta di eliminazione non include un ID versione, StorageGRID può facoltativamente replicare il marcatore di eliminazione, in base alla configurazione della replica tra griglie per il bucket:
 - Se si sceglie di replicare i marcatori di eliminazione (impostazione predefinita), un marcatore di eliminazione viene aggiunto al bucket di origine e replicato nel bucket di destinazione. In effetti, l'oggetto sembra essere stato eliminato su entrambe le griglie.
 - Se si sceglie di non replicare i marcatori di eliminazione, un marcatore 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 eliminati nella griglia di destinazione.

Nella figura, **Replica elimina marcatori** è stato impostato su **Sì** quando "[è stata abilitata la replicazione cross-grid](#)". Le richieste di eliminazione per il bucket di origine che includono un ID versione non elimineranno gli oggetti dal bucket di destinazione. Le richieste di eliminazione per il bucket di origine che non includono un ID versione verranno visualizzate per eliminare gli oggetti nel bucket di destinazione.





Se si desidera mantenere sincronizzate le eliminazioni degli oggetti tra le griglie, creare le corrispondenti ["Configurazioni del ciclo di vita S3"](#) per i bucket su entrambe le griglie.

Come vengono replicati gli oggetti crittografati

Quando si utilizza la replica tra griglie per replicare oggetti tra griglie, è possibile crittografare singoli oggetti, utilizzare la crittografia predefinita dei bucket o configurare la crittografia a livello di griglia. È possibile aggiungere, modificare o rimuovere le impostazioni di crittografia predefinite per bucket o griglia prima o dopo aver abilitato la replica tra griglie per un bucket.

Per crittografare singoli oggetti, è possibile utilizzare SSE (crittografia lato server con chiavi gestite StorageGRID) quando si aggiungono gli oggetti al bucket di origine. Utilizzare il `x-amz-server-side-encryption` intestazione della richiesta e specificare `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 tra griglie. L'operazione di acquisizione non andrà a buon fine.

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 ingeriti senza `x-amz-server-side-encryption` intestazione della richiesta. Vedere ["Operazioni sui bucket"](#).

Per utilizzare la crittografia a livello di griglia, impostare l'opzione **Crittografia degli oggetti memorizzati 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 vengono acquisiti senza `x-amz-server-side-encryption` intestazione della richiesta. Vedere ["Configurare le opzioni di rete e oggetto"](#).



SSE non supporta AES-128. Se l'opzione **Crittografia degli oggetti archiviati** è abilitata per la griglia di origine utilizzando l'opzione **AES-128**, l'uso dell'algoritmo AES-128 non verrà propagato all'oggetto replicato. Al contrario, l'oggetto replicato utilizzerà il bucket predefinito della destinazione o l'impostazione di crittografia a livello di griglia, se disponibile.

Quando si determina come crittografare gli oggetti sorgente, StorageGRID applica queste regole:

1. Utilizzare il `x-amz-server-side-encryption` intestazione di acquisizione, se presente.
2. Se non è presente un'intestazione di acquisizione, utilizzare l'impostazione di crittografia predefinita del bucket, se configurata.
3. Se non è configurata un'impostazione bucket, 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 sorgente.

Quando si determina come crittografare gli oggetti replicati, StorageGRID applica queste regole nel seguente ordine:

1. Utilizzare la stessa crittografia dell'oggetto sorgente, a meno che l'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 configurata.
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 tra griglie.

Se un client S3 emette 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

La dimensione massima del segmento della griglia di origine si applica agli oggetti replicati nella griglia di destinazione. Quando gli oggetti vengono replicati su un'altra griglia, l'impostazione **Dimensione massima segmento (CONFIGURAZIONE > Sistema > Opzioni di archiviazione)** della griglia di origine verrà utilizzata su entrambe le griglie. Ad esempio, supponiamo che la dimensione massima del segmento per la griglia di origine sia 1 GB, mentre la dimensione massima del segmento per la griglia di destinazione sia 50 MB. Se si acquisisce un oggetto da 2 GB nella griglia di origine, tale oggetto viene salvato come due segmenti da 1 GB. Verrà inoltre replicato nella griglia di destinazione come due segmenti da 1 GB, anche se la dimensione massima del segmento di quella griglia è di 50 MB.

Confronta la replicazione cross-grid e la replicazione CloudMirror

Quando inizi a utilizzare la federazione di griglia, rivedi le somiglianze e le differenze tra ["replicazione cross-grid"](#) e il ["Servizio di replica StorageGRID CloudMirror"](#).

	Replicazione cross-grid	Servizio di replica 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 CloudMirror crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente. Questa copia indipendente non viene utilizzata come backup, ma spesso viene ulteriormente elaborata nel cloud.
Come è impostato?	1. Configurare una connessione di federazione di rete tra due reti. 2. Aggiungere nuovi account tenant, che vengono automaticamente clonati nell'altra griglia. 3. Aggiungere nuovi gruppi di tenant e utenti, che vengono anch'essi clonati. 4. Crea bucket corrispondenti su ogni griglia e abilita la replica tra griglie 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) tramite Tenant Manager o l'API S3. 2. Qualsiasi bucket di proprietà di quell'account tenant può essere configurato in modo che punti all'endpoint CloudMirror.

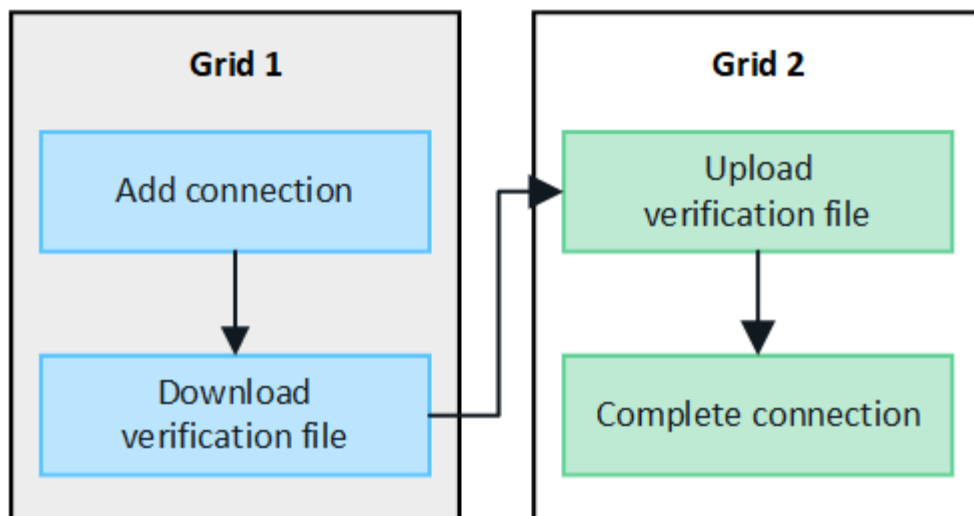
	Replicazione cross-grid	Servizio di replica CloudMirror
Chi è responsabile della sua istituzione?	• Un amministratore di rete configura la connessione e i tenant. • Gli utenti tenant configurano i gruppi, gli utenti, le chiavi e i bucket.	In genere, un utente tenant.
Qual è la destinazione?	Un bucket S3 corrispondente e identico sull'altro sistema StorageGRID nella connessione di federazione della griglia.	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3). • Piattaforma Google Cloud (GCP)
È necessario il controllo delle versioni degli oggetti?	Sì, sia il bucket di origine che quello di destinazione devono avere il controllo delle versioni degli oggetti abilitato.	No, la replica di CloudMirror supporta qualsiasi combinazione di bucket con e senza versione, sia nell'origine che nella destinazione.
Cosa determina lo spostamento degli oggetti verso la destinazione?	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket in cui è abilitata la replica tra griglie.	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket configurato con un endpoint CloudMirror. Gli oggetti presenti nel bucket di origine prima che il bucket fosse configurato con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come vengono replicati gli oggetti?	La replica tra griglie 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 su entrambe le griglie.	La replica di CloudMirror non richiede bucket abilitati al controllo delle versioni, quindi CloudMirror può gestire l'ordinamento solo per una chiave all'interno di un sito. Non vi è alcuna garanzia che l'ordinamento verrà mantenuto per le richieste di un oggetto in un sito diverso.
Cosa succede se un oggetto non può essere replicato?	L'oggetto viene messo in coda per la replica, nel rispetto dei limiti di archiviazione dei metadati.	L'oggetto è in coda per la replica, soggetto ai limiti dei servizi della piattaforma (vedere "Raccomandazioni per l'utilizzo dei servizi della piattaforma").
I metadati di sistema dell'oggetto vengono replicati?	Sì, quando un oggetto viene replicato sull'altra griglia, vengono replicati anche i suoi metadati di sistema. I metadati saranno identici su entrambe le griglie.	No, quando un oggetto viene replicato nel bucket esterno, i suoi metadati di sistema vengono aggiornati. I metadati varieranno a seconda della posizione, a seconda del momento dell'acquisizione e del comportamento dell'infrastruttura S3 indipendente.

	Replicazione cross-grid	Servizio di replica CloudMirror
Come vengono recuperati gli oggetti?	Le applicazioni possono recuperare o leggere oggetti inviando una richiesta al bucket su una delle due griglie.	Le applicazioni possono recuperare o leggere oggetti inviando una richiesta a StorageGRID o alla destinazione S3. Supponiamo, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti su un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è obbligatorio utilizzare StorageGRID .
Cosa succede se un oggetto viene eliminato?	• Le richieste di eliminazione che includono un ID versione non vengono mai replicate nella griglia di destinazione. • Le richieste di eliminazione che non includono un ID versione aggiungono un marcatore di eliminazione al bucket di origine, che può essere facoltativamente replicato nella griglia di destinazione. • Se la replica tra griglie è configurata per una sola direzione, gli oggetti nel bucket di destinazione possono essere eliminati senza influire sulla sorgente.	I risultati varieranno in base allo stato di versioning dei bucket di origine e di destinazione (che non devono essere necessariamente gli stessi): • Se entrambi i bucket sono sottoposti a versioning, una richiesta di eliminazione aggiungerà un marcatore di eliminazione in entrambe le posizioni. • Se solo il bucket di origine è sottoposto a versioning, una richiesta di eliminazione aggiungerà un marcatore di eliminazione all'origine ma non alla destinazione. • Se nessuno dei due bucket è sottoposto a versioning, una richiesta di eliminazione eliminerà l'oggetto dall'origine ma non dalla destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere eliminati senza influire sulla sorgente.

Creare connessioni di federazione di griglia

È possibile creare una connessione di federazione di griglia tra due sistemi StorageGRID se si desidera clonare i dettagli dei tenant e replicare i dati degli oggetti.

Come mostrato nella figura, la creazione di una connessione di federazione di griglia include passaggi su entrambe le griglie. Si aggiunge la connessione su una griglia e la si completa sull'altra griglia. È possibile iniziare da entrambe le griglie.



Prima di iniziare

- Hai esaminato il ["considerazioni e requisiti"](#) per configurare le connessioni della federazione di griglia.
- Se si prevede di utilizzare nomi di dominio completi (FQDN) per ogni griglia anziché indirizzi IP o VIP, si sa quali nomi utilizzare e si è verificato che il server DNS per ogni griglia disponga delle voci appropriate.
- Stai utilizzando un ["browser web supportato"](#) .
- Hai l'autorizzazione di accesso Root e la passphrase di provisioning per entrambe le griglie.

Aggiungi connessione

Eseguire questi passaggi su uno dei due sistemi StorageGRID .

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale su una delle due griglie.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Seleziona **Aggiungi connessione**.
4. Inserisci i dettagli per la connessione.

Campo	Descrizione
Nome della connessione	Un nome univoco che ti aiuti a riconoscere questa connessione, ad esempio "Griglia 1-Griglia 2".
FQDN o IP per questa griglia	Uno dei seguenti: • Il nome di dominio completo della griglia a cui hai effettuato l'accesso • Un indirizzo VIP di un gruppo HA su questa griglia • Un indirizzo IP di un nodo di amministrazione o di un nodo gateway su questa griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla griglia di destinazione.

Campo	Descrizione
Porta	La porta che vuoi utilizzare per questa connessione. È possibile immettere qualsiasi numero di porta non utilizzato compreso tra 23000 e 23999. Entrambe le griglie in questa connessione utilizzeranno la stessa porta. È necessario assicurarsi che nessun nodo in entrambe le griglie utilizzi questa porta per altre connessioni.
Giorni di validità del certificato per questa griglia	Numero di giorni per cui si desidera che i certificati di sicurezza per questa griglia nella connessione siano validi. Il valore predefinito è 730 giorni (2 anni), ma è possibile immettere qualsiasi 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	Uno dei seguenti: • Il nome di dominio completo della rete a cui vuoi connetterti • Un indirizzo VIP di un gruppo HA sull'altra griglia • Un indirizzo IP di un nodo di amministrazione o di un nodo gateway sull'altra griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla griglia sorgente.

5. Seleziona **Salva e continua**.

6. Per il passaggio Scarica file di verifica, seleziona **Scarica file di verifica**.

Una volta completata la connessione sull'altra griglia, non sarà più possibile scaricare il file di verifica da nessuna delle due griglie.

7. Individua il file scaricato(*connection-name.grid-federation*) e salvarlo in un luogo sicuro.



Questo file contiene segreti (mascherati come **★**) e altri dati sensibili e devono essere conservati e trasmessi in modo sicuro.

8. Selezionare **Chiudi** per tornare alla pagina Federazione Grid.

9. Verificare che la nuova connessione sia visualizzata e che il suo **Stato di connessione** sia **In attesa di connessione**.

10. Fornire il *connection-name.grid-federation* file all'amministratore della griglia per l'altra griglia.

Connessione completa

Eseguire questi passaggi sul sistema StorageGRID a cui ci si sta connettendo (l'altra griglia).

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Seleziona **Carica file di verifica** per accedere alla pagina di caricamento.
4. Seleziona **Carica file di verifica**. Quindi, vai e seleziona il file che è stato scaricato dalla prima griglia(`connection-name.grid-federation`).

Vengono mostrati i dettagli della connessione.

5. Facoltativamente, immettere un numero diverso di giorni validi per i certificati di sicurezza per questa griglia. Per impostazione predefinita, la voce **Giorni di validità del certificato** è impostata sul valore immesso nella prima griglia, ma ogni 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 su una delle estremità della connessione scadono, la connessione smetterà di funzionare e le repliche saranno in sospenso finché i certificati non verranno aggiornati.

6. Inserisci la passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
7. Seleziona **Salva e prova**.

I certificati vengono generati e la connessione viene testata. Se la connessione è valida, viene visualizzato un messaggio di conferma e la nuova connessione viene elencata nella pagina Federazione Grid. Lo **Stato della connessione** sarà **Connesso**.

Se viene visualizzato un messaggio di errore, risolvere eventuali problemi. Vedere "[Risolvere gli errori di federazione della griglia](#)".

8. Vai alla pagina della federazione Grid sulla prima griglia e aggiorna il browser. Verificare che lo **Stato della connessione** sia ora **Connesso**.
9. Dopo aver stabilito la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

Se modifichi questa connessione, verrà creato un nuovo file di verifica. Il file originale non può essere riutilizzato.

Dopo aver finito

- Rivedere le considerazioni per "[gestione degli inquilini autorizzati](#)".
- "[Crea uno o più nuovi account tenant](#)", assegnare l'autorizzazione **Usa connessione federazione griglia** e selezionare la nuova connessione.
- "[Gestisci la connessione](#)" come richiesto. È possibile modificare i valori di connessione, testare 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 alla clonazione dell'account e alla replica tra griglie.

Gestire le connessioni della federazione di rete

La gestione delle connessioni di federazione della griglia tra i sistemi StorageGRID include la modifica dei dettagli della connessione, la rotazione dei certificati, la rimozione delle autorizzazioni dei tenant e la rimozione delle connessioni non utilizzate.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su entrambe le griglie utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#) per la griglia a cui hai effettuato l'accesso.

Modifica una connessione di federazione di griglia

È possibile modificare una connessione di federazione di griglia accedendo al nodo di amministrazione principale su una delle griglie nella connessione. Dopo aver apportato modifiche alla prima griglia, è necessario scaricare un nuovo file di verifica e caricarlo sull'altra griglia.



Durante la modifica della connessione, le richieste di clonazione dell'account o di replica tra griglie continueranno a utilizzare le impostazioni di connessione esistenti. Tutte le modifiche apportate alla prima griglia vengono salvate localmente, ma non vengono utilizzate finché non vengono caricate sulla seconda griglia, salvate e testate.

Inizia a modificare la connessione

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale su una delle due griglie.
2. Seleziona **NODI** e verifica che tutti gli altri nodi amministrativi nel tuo sistema siano online.



Quando si modifica una connessione di federazione della griglia, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi amministrativi della prima griglia. Se questo file non può essere salvato su tutti i nodi di amministrazione, verrà visualizzato un messaggio di avviso quando si seleziona **Salva e verifica**.

3. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
4. Modifica i dettagli della connessione utilizzando il menu **Azioni** nella pagina Federazione Grid o nella pagina dei dettagli per una connessione specifica. Vedere ["Creare connessioni di federazione di griglia"](#) per cosa inserire.

Menu Azioni

- a. Selezionare il pulsante di opzione per la connessione.
- b. Selezionare **Azioni > Modifica**.
- c. Inserisci le nuove informazioni.

Pagina dei dettagli

- a. Selezionare il nome di una connessione per visualizzarne i dettagli.
- b. Selezionare **Modifica**.
- c. Inserisci le nuove informazioni.

5. Inserisci la passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
6. Seleziona **Salva e continua**.

I nuovi valori vengono salvati, ma non verranno applicati alla connessione finché non avrai caricato il nuovo file di verifica sull'altra griglia.

7. Seleziona **Scarica file di verifica**.

Per scaricare questo file in un secondo momento, vai alla pagina dei dettagli della connessione.

8. Individua il file scaricato(*connection-name.grid-federation*) e salvarlo in un luogo sicuro.



Il file di verifica contiene segreti e deve essere conservato e trasmesso in modo sicuro.

9. Selezionare **Chiudi** per tornare alla pagina Federazione Grid.

10. Verificare che lo **Stato della connessione** sia **In attesa di modifica**.



Se lo stato della connessione era diverso da **Connesso** quando hai iniziato a modificare la connessione, non cambierà in **In attesa di modifica**.

11. Fornire il *connection-name.grid-federation* file all'amministratore della griglia per l'altra griglia.

Completa la modifica della connessione

Completa la modifica della connessione caricando il file di verifica sull'altra griglia.

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Seleziona **Carica file di verifica** per accedere alla pagina di caricamento.
4. Seleziona **Carica file di verifica**. Quindi, cerca e seleziona il file scaricato dalla prima griglia.
5. Inserisci la passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
6. Seleziona **Salva e prova**.

Se la connessione può essere stabilita utilizzando i valori modificati, viene visualizzato un messaggio di successo. In caso contrario, verrà visualizzato un messaggio di errore. Rivedi il messaggio e risolvi eventuali problemi.

7. Chiudere la procedura guidata per tornare alla pagina Federazione Grid.
8. Verificare che lo **Stato della connessione** sia **Connesso**.
9. Vai alla pagina della federazione Grid sulla prima griglia e aggiorna il browser. Verificare che lo **Stato della connessione** sia ora **Connesso**.
10. Dopo aver stabilito la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

Testa una connessione di federazione di griglia

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Verificare la connessione utilizzando il menu **Azioni** nella pagina Federazione Grid o nella pagina dei dettagli per una connessione specifica.

Menu Azioni

- a. Selezionare il pulsante di opzione per la connessione.
- b. Selezionare **Azioni > Test**.

Pagina dei dettagli

- a. Selezionare il nome di una connessione per visualizzarne i dettagli.
- b. Selezionare **Test connessione**.

4. Controlla lo stato della connessione:

Stato della connessione	Descrizione
Collegato	Entrambe le reti sono collegate e comunicano normalmente.
Errore	La connessione è in stato di errore. Ad esempio, un certificato è scaduto o un valore di configurazione non è più valido.
Modifica in sospeso	Hai modificato la connessione su questa griglia, ma la connessione utilizza ancora la configurazione esistente. Per completare la modifica, carica il nuovo file di verifica nell'altra griglia.
In attesa di connessione	Hai configurato la connessione su questa griglia, ma la connessione non è stata completata sull'altra griglia. Scarica il file di verifica da questa griglia e caricalo sull'altra griglia.
Sconosciuto	La connessione è in uno stato sconosciuto, probabilmente a causa di un problema di rete o di un nodo offline.

5. Se lo stato della connessione è **Errore**, risolvere eventuali problemi. Quindi, seleziona nuovamente **Test connessione** per confermare che il problema è stato risolto.

Ruota i certificati di connessione

Ogni connessione di federazione di griglia utilizza quattro certificati SSL generati automaticamente per proteggere la connessione. Quando i due certificati per ciascuna griglia si avvicinano alla data di scadenza, l'avviso **Scadenza del certificato di federazione della griglia** ricorda di ruotare i certificati.



Se i certificati su una delle estremità della connessione scadono, la connessione smetterà di funzionare e le repliche saranno in sospeso finché i certificati non verranno aggiornati.

Passi

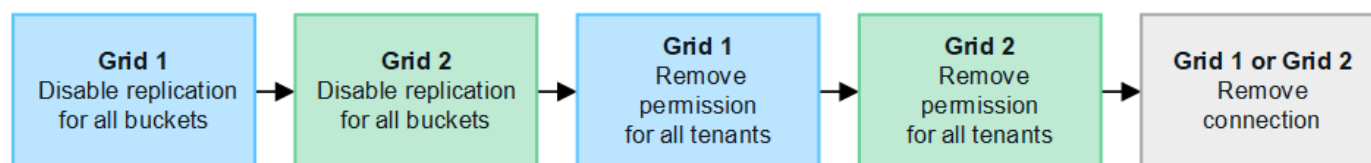
1. Sign in a Grid Manager dal nodo di amministrazione principale su una delle due griglie.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Da una delle due schede della pagina Federazione Grid, seleziona il nome della connessione per visualizzarne i dettagli.
4. Selezionare la scheda **Certificati**.

5. Seleziona **Ruota certificati**.
6. Specificare per quanti giorni i nuovi certificati devono essere validi.
7. Inserisci la passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
8. Seleziona **Ruota certificati**.
9. Se necessario, ripetere questi passaggi sull'altra griglia nella connessione.

In generale, utilizzare lo stesso numero di giorni per i certificati su entrambi i lati della connessione.

Rimuovere una connessione di federazione di griglia

È possibile rimuovere una connessione di federazione di griglia da entrambe le griglie nella connessione. Come mostrato nella figura, è necessario eseguire i passaggi preliminari su entrambe le griglie per confermare che la connessione non sia utilizzata da alcun tenant su nessuna delle due griglie.



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 tenant presenti su entrambe le griglie non vengono eliminati da nessuna delle due griglie 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 attesa di replicazione (ingeriti ma non ancora replicati nell'altra griglia) non riuscirà più.

Disabilita la replica per tutti i bucket tenant

Passi

1. Partendo da una delle due griglie, accedi a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Selezionare il nome della connessione per visualizzarne i dettagli.
4. Nella scheda **Tenant consentiti**, determinare se la connessione è utilizzata da qualche tenant.
5. Se sono elencati degli inquilini, istruire tutti gli inquilini a ["disabilitare la replicazione tra griglie"](#) per tutti i loro bucket su entrambe le griglie nella connessione.



Non è possibile rimuovere l'autorizzazione **Usa connessione federazione griglia** se in uno qualsiasi dei bucket tenant è abilitata la replica tra griglie. Ogni account tenant deve disabilitare la replica tra griglie per i propri bucket su entrambe le griglie.

Rimuovi l'autorizzazione per ogni tenant

Dopo aver disabilitato la replica tra griglie per tutti i bucket tenant, rimuovere l'autorizzazione **Usa federazione griglie** da tutti i tenant su entrambe le griglie.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
2. Selezionare il nome della connessione per visualizzarne i dettagli.
3. Per ogni tenant nella scheda **Tenant consentiti**, rimuovere l'autorizzazione **Usa connessione federazione griglia** da ciascun tenant. Vedere ["Gestire gli inquilini autorizzati"](#) .
4. Ripetere questi passaggi per gli inquilini autorizzati sull'altra griglia.

Rimuovi connessione

Passi

1. Se nessun tenant su nessuna delle due griglie utilizza la connessione, selezionare **Rimuovi**.
2. Rivedi il messaggio di conferma e seleziona **Rimuovi**.
 - Se la connessione può essere rimossa, viene visualizzato un messaggio di conferma. La connessione della federazione di rete è ora rimossa da entrambe le reti.
 - Se la connessione non può essere rimossa (ad esempio perché è ancora in uso o si è verificato un errore di connessione), viene visualizzato un messaggio di errore. Puoi procedere in uno dei seguenti modi:
 - Risolvi l'errore (consigliato). Vedere ["Risolvere gli errori di federazione della griglia"](#) .
 - Rimuovere la connessione con la forza. Vedere la sezione successiva.

Rimuovere forzatamente una connessione di federazione di griglia

Se necessario, è possibile forzare la rimozione di una connessione che non ha lo stato **Connesso**.

La rimozione forzata elimina solo la connessione dalla rete locale. Per rimuovere completamente la connessione, eseguire gli stessi passaggi su entrambe le griglie.

Passi

1. Nella finestra di dialogo di conferma, seleziona **Forza rimozione**.

Viene visualizzato un messaggio di successo. Questa connessione di federazione di rete non può più essere utilizzata. Tuttavia, nei bucket tenant potrebbe essere ancora abilitata la replica tra griglie e alcune copie degli oggetti potrebbero essere già state replicate tra le griglie nella connessione.

2. Dall'altra griglia nella connessione, accedi a Grid Manager dal nodo di amministrazione principale.
3. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
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 gli inquilini autorizzati per la federazione della rete

È possibile consentire agli account tenant S3 di utilizzare una connessione federata di griglia tra due sistemi StorageGRID . Quando agli inquilini è consentito utilizzare una connessione, sono necessari passaggi speciali per modificare i dettagli dell'inquilino o per rimuovere definitivamente l'autorizzazione di un inquilino a utilizzare la connessione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su entrambe le griglie utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) per la griglia a cui hai effettuato l'accesso.
- Hai ["ha creato una connessione di federazione di rete"](#) tra due griglie.
- Hai esaminato i flussi di lavoro per ["clonazione dell'account"](#) E ["replicazione cross-grid"](#) .
- Come richiesto, hai già configurato l'accesso singolo (SSO) o identificato la federazione per entrambe le griglie nella connessione. Vedere ["Che cosa è il clone dell'account"](#) .

Creare un inquilino autorizzato

Se si desidera consentire a un account tenant nuovo o esistente di utilizzare una connessione di federazione di griglia per la clonazione dell'account e la replica tra griglie, seguire le istruzioni generali per ["creare un nuovo tenant S3"](#) O ["modificare un account inquilino"](#) e notare quanto segue:

- È possibile creare il tenant da entrambe le griglie nella 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 abilitare l'autorizzazione **Usa connessione federazione griglia** e quindi salvato sulla prima griglia, un tenant identico viene automaticamente replicato sull'altra griglia. La griglia in cui viene replicato il tenant è la *griglia di destinazione del tenant*.
- Gli inquilini su entrambe le griglie avranno lo stesso ID account di 20 cifre, nome, descrizione, quota e autorizzazioni. Facoltativamente, puoi utilizzare il campo **Descrizione** per identificare quale sia il tenant di origine e quale quello di destinazione. Ad esempio, questa descrizione per un tenant creato sulla Griglia 1 apparirà 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 di griglia per quella griglia deve ["cambiare la password per l'utente root locale"](#) .

- Dopo che il tenant nuovo o modificato è disponibile su entrambe le griglie, gli utenti del tenant possono eseguire queste operazioni:
 - Dalla griglia di origine del tenant, crea gruppi e utenti locali, che vengono automaticamente clonati nella griglia di destinazione del tenant. Vedere ["Clona gruppi tenant e utenti"](#) .
 - Crea nuove chiavi di accesso S3, che possono essere facoltativamente clonate nella griglia di destinazione del tenant. Vedere ["Clona le chiavi di accesso S3 utilizzando l'API"](#) .
 - Crea bucket identici su entrambe le griglie nella connessione e abilita la replica tra griglie in una direzione o in entrambe le direzioni. Vedere ["Gestire la replicazione tra griglie"](#) .

Visualizza un inquilino autorizzato

È possibile visualizzare i dettagli di un tenant autorizzato a utilizzare una connessione di federazione di rete.

Passi

1. Selezionare **INQUILINI**.
2. Dalla pagina Inquilini, seleziona il nome dell'inquilino per visualizzare la pagina dei dettagli dell'inquilino.

Se questa è la griglia di origine del tenant (ovvero se il tenant è stato creato su 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.

Tenants > tenant A for grid federation

tenant A for grid federation

Tenant ID: 0899 6970 1700 0930 0009

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Description: this tenant was created on Grid 1

Sign in

Edit

Actions

This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

Space breakdown

Allowed features

Grid federation

Remove permission

Clear error

Search...

Displaying one result

Connection name	Connection status	Remote grid hostname	Last error
Grid 1 to Grid 2	Connected	10.96.106.230	Check for errors

3. Facoltativamente, seleziona la scheda **Federazione griglia** per"monitorare la connessione della federazione di rete" .

Modifica un inquilino autorizzato

Se è necessario modificare un tenant che dispone dell'autorizzazione **Usa connessione federazione griglia**, seguire le istruzioni generali per"modifica di un account inquilino" e notare quanto segue:

- Se un tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile modificare i dettagli del tenant da entrambe le griglie nella connessione. Tuttavia, le modifiche apportate non verranno copiate nell'altra griglia. Se si desidera mantenere sincronizzati i dettagli del tenant tra le griglie, è necessario apportare le stesse modifiche su entrambe le griglie.
- Non è possibile cancellare l'autorizzazione **Usa connessione federazione griglia** quando si modifica un tenant.
- Non è possibile selezionare una connessione di federazione di griglia diversa quando si modifica un tenant.

Elimina un inquilino autorizzato

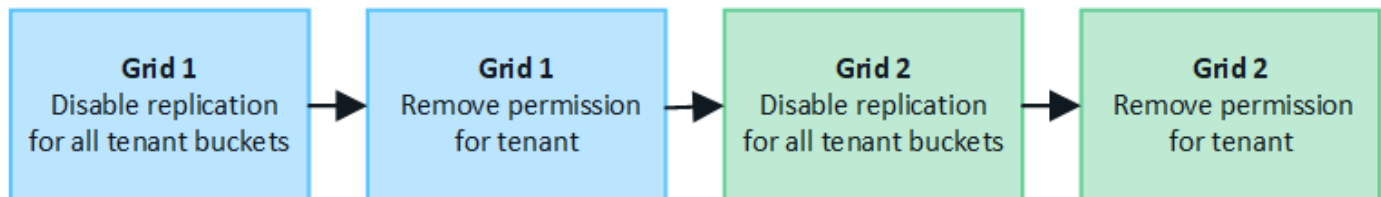
Se è necessario rimuovere un tenant che dispone dell'autorizzazione **Usa connessione federazione griglia**, seguire le istruzioni generali per ["eliminazione di un account tenant"](#) e notare quanto segue:

- Prima di poter rimuovere il tenant originale dalla griglia di origine, è necessario rimuovere tutti i bucket per l'account dalla griglia di origine.
- Prima di poter rimuovere il tenant clonato dalla griglia di destinazione, è necessario rimuovere tutti i bucket per l'account dalla griglia di destinazione.
- Se si rimuove il tenant originale o quello clonato, l'account non potrà più essere utilizzato per la replica tra griglie.
- Se si rimuove il tenant originale dalla griglia di origine, eventuali gruppi di tenant, utenti o chiavi clonati nella griglia di destinazione non saranno interessati. È possibile eliminare il tenant clonato oppure consentirgli di gestire i propri gruppi, utenti, chiavi di accesso e bucket.
- Se si rimuove il tenant clonato dalla griglia di destinazione, si verificheranno errori di clonazione se nuovi gruppi o utenti vengono aggiunti al tenant originale.

Per evitare questi errori, rimuovere l'autorizzazione del tenant a utilizzare la connessione federata della griglia prima di eliminare il tenant da questa griglia.

Rimuovi Usa autorizzazione di connessione alla federazione della griglia

Per impedire a un tenant di utilizzare una connessione federata alla griglia, è necessario rimuovere l'autorizzazione **Usa connessione federata alla griglia**.



Prima di revocare l'autorizzazione di un tenant a utilizzare una connessione di federazione di rete, tenere presente quanto segue:

- Non è possibile rimuovere l'autorizzazione **Usa connessione federazione griglia** se uno qualsiasi dei bucket del tenant ha abilitata la replica tra griglie. L'account tenant deve prima disabilitare la replica tra griglie per tutti i propri bucket.
- La rimozione dell'autorizzazione **Usa connessione federazione griglia** non elimina gli elementi che sono già stati replicati tra le griglie. Ad esempio, tutti gli utenti, i gruppi e gli oggetti tenant presenti su entrambe le griglie non vengono eliminati da nessuna delle due griglie 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, la riattivazione di questa autorizzazione genererà un errore.



Riattivando l'autorizzazione **Usa connessione federazione griglia**, la griglia locale diventa la griglia di origine e viene attivata la clonazione sulla griglia remota specificata dalla connessione federazione griglia selezionata. Se l'account tenant esiste già sulla griglia remota, la clonazione genererà un errore di conflitto.

Prima di iniziare

- Stai utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) per entrambe le griglie.

Disabilita la replica per i bucket tenant

Come primo passaggio, disabilitare la replica tra griglie per tutti i bucket tenant.

Passi

1. Partendo da una delle due griglie, accedi a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
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 l'inquilino è elencato, istruirlo a ["disabilitare la replicazione tra griglie"](#) per tutti i loro bucket su entrambe le griglie nella connessione.



Non è possibile rimuovere l'autorizzazione **Usa connessione federazione griglia** se in uno qualsiasi dei bucket tenant è abilitata la replica tra griglie. Il tenant deve disabilitare la replica tra griglie per i propri bucket su entrambe le griglie.

Rimuovi l'autorizzazione per l'inquilino

Dopo aver disabilitato la replica tra griglie per i bucket tenant, è possibile rimuovere l'autorizzazione del tenant a utilizzare la connessione federata della griglia.

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Rimuovere l'autorizzazione dalla pagina Federazione della griglia o dalla pagina Tenant.

Pagina della federazione della griglia

- a. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
- b. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
- c. Nella scheda **Locatari consentiti**, selezionare il pulsante di opzione per il locatario.
- d. Seleziona **Rimuovi autorizzazione**.

Pagina degli inquilini

- a. Selezionare **INQUILINI**.
- b. Selezionare il nome dell'inquilino per visualizzare la pagina dei dettagli.
- c. Nella scheda **Federazione di griglia**, selezionare il pulsante di opzione per la connessione.
- d. Seleziona **Rimuovi autorizzazione**.

3. Esaminare gli avvisi nella finestra di dialogo di conferma e selezionare **Rimuovi**.
 - Se l'autorizzazione può essere rimossa, verrai reindirizzato alla pagina dei dettagli e verrà visualizzato un messaggio di conferma dell'operazione. Questo tenant non può più utilizzare la connessione alla federazione di rete.

- Se uno o più bucket tenant hanno ancora la replica tra griglie abilitata, viene visualizzato un errore.

 **Remove permission to use grid federation connection** 

Are you sure you want to prevent **Tenant A** from performing account sync and cross-grid replication using grid federation connection **Grid 1-Grid 2**?

- Removing this permission does not delete any items that have already been copied to the other grid.
- After removing this permission for the tenant on this grid, go to the other grid and remove the permission for the corresponding tenant account.

 Connection '5427cbf8-0dd0-4b83-a2c8-e5e23cc49cc5' is used by bucket 'my-cgr-bucket' for cross-grid replication, so it can't be removed. From Tenant Manager, remove the cross-grid configuration from the tenant bucket and retry.

 Using **Force remove** removes the tenant's permission to use the grid federation connection even if tenant buckets still have cross-grid replication enabled. When the permission is removed, data in these buckets can no longer be copied between the grids.

Cancel

Force remove

Remove

Puoi procedere in uno dei seguenti modi:

- (Raccomandato.) Sign in a Tenant Manager e disabilita la replica per ciascun bucket del tenant. Vedere ["Gestire la replicazione tra griglie"](#). Quindi, ripetere i passaggi per rimuovere l'autorizzazione **Usa connessione alla rete**.
- Rimuovere l'autorizzazione con la forza. Vedere la sezione successiva.

4. Passare all'altra griglia e ripetere questi passaggi per rimuovere l'autorizzazione per lo stesso tenant sull'altra griglia.

Rimuovi il permesso con la forza

Se necessario, è possibile forzare la rimozione dell'autorizzazione di un tenant a utilizzare una connessione di federazione di griglia anche se nei bucket del tenant è abilitata la replica tra griglie.

Prima di revocare con la forza il permesso di un inquilino, tenere presente le considerazioni generali per [rimozione del permesso](#) oltre a queste considerazioni aggiuntive:

- Se si rimuove forzatamente l'autorizzazione **Usa connessione federazione griglia**, tutti gli oggetti in

attesa di replica sull'altra griglia (ingeriti ma non ancora replicati) continueranno a essere replicati. Per impedire che questi oggetti in corso raggiungano il bucket di destinazione, è necessario rimuovere l'autorizzazione del tenant anche sull'altra griglia.

- Tutti gli oggetti inseriti nel bucket di origine dopo aver rimosso l'autorizzazione **Usa connessione federazione griglia** non verranno mai replicati nel bucket di destinazione.

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
4. Nella scheda **Locatari consentiti**, selezionare il pulsante di opzione per il locatario.
5. Seleziona **Rimuovi autorizzazione**.
6. Rivedi gli avvisi nella finestra di dialogo di conferma e seleziona **Forza rimozione**.

Viene visualizzato un messaggio di successo. Questo tenant non può più utilizzare la connessione alla federazione di rete.

7. Se necessario, vai all'altra griglia e ripeti questi passaggi per forzare la rimozione dell'autorizzazione per lo stesso account tenant sull'altra griglia. Ad esempio, dovresti ripetere questi passaggi sull'altra griglia per impedire che gli oggetti in corso di elaborazione raggiungano il bucket di destinazione.

Risolvere gli errori di federazione della griglia

Potrebbe essere necessario risolvere avvisi ed errori relativi alle connessioni della federazione della griglia, alla clonazione degli account e alla replica tra griglie.

Avvisi ed errori di connessione della federazione di rete

Potresti ricevere avvisi o riscontrare errori con le connessioni della federazione di rete.

Dopo aver apportato modifiche per risolvere un problema di connessione, testare la connessione per assicurarsi che lo stato della connessione torni a **Connesso**. Per le istruzioni, vedere ["Gestire le connessioni della federazione di rete"](#).

Avviso di errore di connessione alla federazione di rete

Problema

È stato attivato l'avviso **Errore di connessione alla federazione di rete**.

Dettagli

Questo avviso indica che la connessione di federazione di rete tra le reti non funziona.

Azioni consigliate

1. Rivedere le impostazioni nella pagina Federazione della griglia per entrambe le griglie. Verificare che tutti i valori siano corretti. Vedere ["Gestire le connessioni della federazione di rete"](#).
2. Esaminare i certificati utilizzati per la connessione. Assicurarsi che non vi siano avvisi relativi a certificati di federazione della griglia scaduti e che i dettagli di ciascun certificato siano validi. Vedere le istruzioni per la rotazione dei certificati di connessione in ["Gestire le connessioni della federazione di rete"](#).
3. Verificare che tutti i nodi Admin e Gateway in entrambe le griglie siano online e disponibili. Risolvi eventuali avvisi che potrebbero interessare questi nodi e riprova.

4. Se hai fornito un nome di dominio completo (FQDN) per la griglia locale o remota, verifica che il server DNS sia online e disponibile. Vedere ["Che cos'è la federazione di rete?"](#) per requisiti di rete, indirizzo IP e DNS.

Avviso di scadenza del certificato di federazione della griglia

Problema

È stato attivato l'avviso **Scadenza del certificato di federazione della griglia**.

Dettagli

Questo avviso indica che uno o più certificati di federazione della griglia stanno per scadere.

Azioni consigliate

Vedere le istruzioni per la rotazione dei certificati di connessione in ["Gestire le connessioni della federazione di rete"](#).

Errore durante la modifica di una connessione di federazione di griglia

Problema

Quando si modifica una connessione di federazione di griglia, viene visualizzato il seguente messaggio di avviso quando si seleziona **Salva e verifica**: "Impossibile creare un file di configurazione candidato su uno o più nodi".

Dettagli

Quando si modifica una connessione di federazione della griglia, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi amministrativi della prima griglia. Viene visualizzato un messaggio di avviso se il file non può essere salvato su tutti i nodi amministrativi, ad esempio perché un nodo amministrativo è offline.

Azioni consigliate

1. Dalla griglia che stai utilizzando per modificare la connessione, seleziona **NODI**.
2. Verificare che tutti i nodi amministrativi per quella griglia siano online.
3. Se alcuni nodi sono offline, riportali online e prova a modificare nuovamente la connessione.

Errori di clonazione dell'account

Impossibile accedere a un account tenant clonato

Problema

Non è possibile 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. Per favore riprova."

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 sua griglia di origine, le password degli utenti 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 ["cambiare 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 sulla griglia di destinazione. Per le istruzioni, vedere ["Gestisci gli utenti locali"](#) nelle istruzioni per l'utilizzo di Tenant Manager.

Tenant creato senza un clone

Problema

Dopo aver creato un nuovo tenant con l'autorizzazione **Usa connessione federazione griglia**, viene visualizzato il messaggio "Tenant creato senza un clone".

Dettagli

Questo problema può verificarsi se gli aggiornamenti allo stato della connessione vengono ritardati, il che potrebbe causare l'elenco di una connessione non funzionante come **Connesso**.

Azioni consigliate

1. Esaminare il motivo elencato 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 alla federazione di rete](#).
2. Seguire le istruzioni per testare una connessione di federazione di griglia in ["Gestire le connessioni della federazione di rete"](#) per confermare che il problema è stato risolto.
3. Dalla griglia di origine dell'inquilino, seleziona **INQUILINI**.
4. Individuare l'account tenant che non è stato possibile clonare.
5. Selezionare il nome del tenant per visualizzare la pagina dei dettagli.
6. Seleziona **Riprova clonazione account**.

Tenants > test

test

Tenant ID: 0040 2213 8117 4859 6503

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Sign in

Edit

Actions

✖

Tenant account could not be cloned to the other grid.
Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

Retry account clone

Se l'errore è stato risolto, l'account tenant verrà ora clonato nell'altra griglia.

Avvisi ed errori di replicazione tra griglie

Ultimo errore visualizzato per la connessione o il tenant

Problema

Quando "visualizzazione di una connessione di federazione di rete" (o quando "gestione degli inquilini autorizzati" per una connessione), si nota un errore nella colonna **Ultimo errore** nella pagina dei dettagli della connessione. Per esempio:

Grid 1 - Grid 2

Local hostname (this grid):10.96.130.64

Port:23000

Remote hostname (other grid):10.96.130.76

Connection status:

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Remove permission

Clear error

Search...

Displaying one result

Tenant name	Last error
Tenant A	2022-12-22 16:19:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 13916508109026943924) Check for errors

Dettagli

Per ogni connessione di federazione di griglia, la colonna **Ultimo errore** mostra l'errore più recente verificatosi, se presente, durante la replica dei dati di un tenant sull'altra griglia. Questa colonna mostra solo l'ultimo errore di replicazione tra griglie verificatosi; gli errori precedenti che potrebbero essersi verificati non verranno mostrati. Un errore in questa colonna potrebbe verificarsi per uno dei seguenti motivi:

- La versione dell'oggetto sorgente non è stata trovata.
- Il bucket di origine non è stato trovato.
- Il bucket di destinazione è stato eliminato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il controllo delle versioni del bucket di destinazione è sospeso.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più sottoposto a controllo di versione.

Azioni consigliate

Se nella colonna **Ultimo errore** viene visualizzato un messaggio di errore, procedere come segue:

1. Rivedi il testo del messaggio.
2. Eseguire tutte le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso sul bucket di destinazione per la replica tra griglie, riattivare il controllo delle versioni per quel bucket.

3. Selezionare la connessione o l'account tenant dalla tabella.
4. Seleziona **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Aspetta 5-6 minuti e poi ingerisci un nuovo oggetto nel secchio. Verificare che il messaggio di errore non venga più visualizzato.



Per garantire che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo il timestamp nel messaggio prima di acquisire un nuovo oggetto.



Dopo aver eliminato l'errore, potrebbe apparire un nuovo **Ultimo errore** se gli oggetti vengono inseriti in un bucket diverso che presenta anch'esso un errore.

7. Per determinare se la replica di alcuni oggetti non è riuscita a causa dell'errore del bucket, vedere ["Identificare e riprovare le operazioni di replicazione non riuscite"](#).

Avviso di errore permanente della replicazione tra griglie

Problema

È stato attivato l'avviso **Errore permanente nella replicazione tra griglie**.

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 essere risolto. Questo avviso è in genere causato da una modifica al bucket di origine o di destinazione.

Azioni consigliate

1. Sign in alla griglia in cui è stato attivato l'avviso.
2. Vai su **CONFIGURAZIONE > Sistema > Federazione di griglia** e individua il nome della connessione elencato nell'avviso.
3. Nella scheda Tenant autorizzati, controlla la colonna **Ultimo errore** per determinare quali account tenant presentano errori.
4. Per saperne di più sul guasto, vedere le istruzioni in ["Monitorare le connessioni della federazione di rete"](#) per rivedere le metriche di replicazione tra griglie.
5. Per ogni account inquilino interessato:
 - a. Vedere le istruzioni in ["Monitorare l'attività degli inquilini"](#) per confermare che il tenant non ha superato la sua quota sulla griglia di destinazione per la replica tra griglie.
 - 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 in cui è abilitata la replica tra griglie, confermare quanto segue:
 - Esiste un bucket corrispondente per lo stesso tenant sull'altra griglia (è necessario utilizzare il nome esatto).
 - In entrambi i bucket è abilitato il controllo delle versioni degli oggetti (il controllo delle versioni non può essere sospeso su nessuna delle due griglie).
 - In entrambi i bucket il blocco oggetti S3 è disabilitato.

◦ Nessuno dei bucket è nello stato **Eliminazione oggetti: sola lettura**.

8. Per confermare che il problema è stato risolto, consultare le istruzioni in "[Monitorare le connessioni della federazione di rete](#)" per rivedere le metriche di replicazione tra griglie oppure eseguire questi passaggi:
 - a. Torna alla pagina Federazione Grid.
 - 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. Aspetta 5-6 minuti e poi ingerisci un nuovo oggetto nel secchio. Verificare che il messaggio di errore non venga più visualizzato.



Per garantire che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo il timestamp nel messaggio prima di acquisire un nuovo oggetto.



Potrebbe volerci fino a un giorno prima che l'avviso venga cancellato una volta risolto.

- a. Vai a "[Identificare e riprovare le operazioni di replicazione non riuscite](#)" per identificare eventuali oggetti o eliminare i marcatori che non sono riusciti a replicare nell'altra griglia e per riprovare la replicazione se necessario.

Avviso di risorsa di replicazione tra griglie non disponibile

Problema

È stato attivato l'avviso **Risorsa di replicazione tra griglie non disponibile**.

Dettagli

Questo avviso indica che le richieste di replica tra griglie sono in sospeso perché una risorsa non è disponibile. Ad esempio, potrebbe esserci un errore di rete.

Azioni consigliate

1. Monitorare l'avviso per verificare se il problema si risolve da solo.
2. Se il problema persiste, verificare se una delle due griglie presenta un avviso **Errore di connessione alla federazione della griglia** per la stessa connessione o un avviso **Impossibile comunicare con il nodo** per un nodo. Questo avviso potrebbe essere risolto quando risolvi gli avvisi precedenti.
3. Per saperne di più sul guasto, vedere le istruzioni in "[Monitorare le connessioni della federazione di rete](#)" per rivedere le metriche di replicazione tra griglie.
4. Se non riesci a risolvere il problema, contatta l'assistenza tecnica.

Una volta risolto il problema, la replica tra griglie proseguirà normalmente.

Identificare e riprovare le operazioni di replicazione non riuscite

Dopo aver risolto l'avviso **Errore permanente nella replica tra griglie**, dovresti determinare se qualche oggetto o marcatore di eliminazione non è riuscito a essere replicato sull'altra griglia. È quindi possibile reingestire questi oggetti o utilizzare l'API Grid Management per riprovare la replica.

L'avviso **Errore permanente nella replica tra griglie** 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 essere risolto. Questo avviso è in genere causato da una modifica al bucket di origine o di destinazione. Per maggiori dettagli, vedere

"Risolvere gli errori di federazione della griglia" .

Determina se qualche oggetto non è stato replicato

Per determinare se oggetti o marcatori di eliminazione non sono stati replicati nell'altra griglia, è possibile cercare nel registro di controllo "[CGRR \(richiesta di replica tra griglie\)](#)" messaggi. Questo messaggio viene aggiunto al registro quando StorageGRID non riesce a replicare un oggetto, un oggetto multiparte o a eliminare un marcatore nel bucket di destinazione.

Puoi usare il "[strumento di verifica e spiegazione](#)" per tradurre i risultati in un formato più facile da leggere.

Prima di iniziare

- Hai i permessi di accesso Root.
- Tu hai il `Passwords.txt` file.
- Conosci l'indirizzo IP del nodo di amministrazione primario.

Passi

1. Accedi al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#` .

2. Cercare i messaggi CGRR nel file `audit.log` e utilizzare lo strumento `audit-explain` per formattare i risultati.

Ad esempio, questo comando cerca tutti i messaggi CGRR degli ultimi 30 minuti e utilizza lo strumento `audit-explain`.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
print }' audit.log | grep CGRR | audit-explain
```

I risultati del comando saranno simili a questo esempio, che contiene voci per sei messaggi CGRR. Nell'esempio, tutte le richieste di replica tra griglie hanno restituito un errore generale perché l'oggetto non poteva essere replicato. I primi tre errori riguardano le operazioni di "replica oggetto", mentre gli ultimi tre errori riguardano le operazioni di "replica eliminazione marcatore".

```

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

```

Ogni voce contiene le seguenti informazioni:

Campo	Descrizione
Richiesta di replicazione tra griglie CGRR	Il nome della richiesta
inquilino	ID account dell'inquilino
connessione	L'ID della connessione della federazione di rete
operazione	Tipo di operazione di replicazione che si stava tentando: • replicare l'oggetto • replica elimina marcatore • replicare un oggetto multiparte
secchio	Il nome del bucket
oggetto	Il nome dell'oggetto
versione	L'ID della versione per l'oggetto

Campo	Descrizione
errore	Il tipo di errore. Se la replica tra griglie non riesce, l'errore è "Errore generale".

Riprova le repliche non riuscite

Dopo aver generato un elenco di oggetti ed eliminato i marcatori che non sono stati replicati nel bucket di destinazione e aver risolto i problemi sottostanti, è possibile riprovare la replica in uno dei due modi seguenti:

- Reinserisci ogni oggetto nel bucket di origine.
- Utilizzare l'API privata di Grid Management, come descritto.

Passi

1. Nella parte superiore di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API**.
2. Seleziona **Vai alla documentazione API privata**.



Gli endpoint dell'API StorageGRID contrassegnati come "Privati" sono soggetti a modifiche senza preavviso. Anche gli endpoint privati StorageGRID ignorano la versione API della richiesta.

3. Nella sezione **cross-grid-replication-advanced**, seleziona il seguente endpoint:

```
POST /private/cross-grid-replication-retry-failed
```

4. Seleziona **Provalo**.
5. Nella casella di testo **corpo**, sostituire la voce di esempio per **versionID** con un ID versione dal file audit.log corrispondente a una richiesta di replica tra griglie non riuscita.

Assicuratevi di mantenere le virgolette doppie attorno alla stringa.
6. Selezionare **Esegui**.
7. Verificare che il codice di risposta del server sia **204**, a indicare che l'oggetto o il marcatore di eliminazione è stato contrassegnato come in sospeso per la replica tra griglie sull'altra griglia.



In sospeso significa che la richiesta di replicazione tra griglie è stata aggiunta alla coda interna per l'elaborazione.

Monitorare i tentativi di replicazione

È necessario monitorare le operazioni di ripetizione della replica per assicurarsi che vengano completate.



Potrebbero volerci diverse ore o più prima che un oggetto o un marcatore di eliminazione venga replicato nell'altra griglia.

È possibile monitorare le operazioni di ripetizione in uno dei due modi seguenti:

- Utilizzare un S3 **"HeadObject"** O **"OttieniOggetto"** richiesta. La risposta include StorageGRID-specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	• COMPLETO: La replica è riuscita. • IN ATTESA: 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 di Grid Management, come descritto.

Passi

1. Nella sezione **cross-grid-replication-advanced** della documentazione API privata, seleziona il seguente endpoint:

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Seleziona **Provalo**.
3. Nella sezione Parametro, inserisci l'ID della versione utilizzata 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 replicazione, che sarà uno dei seguenti:
 - **IN ATTESA**: L'oggetto non è stato ancora replicato.
 - **COMPLETO**: La replica è riuscita.
 - **FAILED**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.

Gestire la sicurezza

Gestire la sicurezza

È possibile configurare diverse impostazioni di sicurezza da Grid Manager per proteggere il sistema StorageGRID .

Gestisci la crittografia

StorageGRID offre diverse opzioni per la crittografia dei dati. Dovresti [rivedere i metodi di crittografia disponibili](#) per determinare quali soddisfano i tuoi requisiti di protezione dei dati.

Gestisci i certificati

Puoi [configurare e gestire i certificati del server](#) utilizzato per le connessioni HTTP o i certificati client utilizzati per autenticare l'identità di un client o di un utente sul server.

Configurare i server di gestione delle chiavi

Utilizzando un [server di gestione delle chiavi](#) consente di proteggere i dati StorageGRID anche se un dispositivo viene rimosso dal data center. Dopo aver crittografato i volumi dell'appliance, non sarà possibile

accedere ai dati sull'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 abilitare l'impostazione **Crittografia nodo** per ogni appliance durante l'installazione, prima che l'appliance venga aggiunta alla griglia.

Gestisci le impostazioni proxy

Se si utilizzano servizi della piattaforma S3 o pool di archiviazione cloud, è possibile configurare un "[server proxy di archiviazione](#)" tra i nodi di archiviazione e gli endpoint S3 esterni. Se si inviano pacchetti AutoSupport tramite HTTPS o HTTP, è possibile configurare un "[server proxy di amministrazione](#)" tra i nodi amministrativi e il supporto tecnico.

Controllare i firewall

Per migliorare la sicurezza del sistema, è possibile controllare l'accesso ai nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche a livello "[firewall esterno](#)". È inoltre possibile controllare l'accesso alla rete per ciascun nodo configurandone "[firewall interno](#)". È possibile impedire l'accesso a tutte le porte, ad eccezione di quelle necessarie per la distribuzione.

Esaminare i metodi di crittografia StorageGRID

StorageGRID offre diverse opzioni per la crittografia dei dati. Dovresti esaminare i metodi disponibili per determinare quali metodi soddisfano i tuoi requisiti di protezione dei dati.

La tabella fornisce un riepilogo di alto livello dei metodi di crittografia disponibili in StorageGRID.

Opzione di crittografia	Come funziona	Si applica a
Server di gestione delle chiavi (KMS) in Grid Manager	Voi " 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 (KEK). Questa chiave crittografa e decrittografa la chiave di crittografia dei dati (DEK) su ciascun volume.	Nodi dell'appliance in cui è abilitata la Crittografia nodo durante l'installazione. Tutti i dati presenti sull'appliance sono protetti contro la perdita fisica o la 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	Si applica a
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 per l'unità, è impossibile per chiunque recuperare dati validi dalle unità rimosse dal sistema, a meno che non si conosca la passphrase. Prima di iniziare l'installazione, vai su Configura hardware > Crittografia unità per impostare una passphrase dell'unità che si applichi a tutte le unità auto-crittografanti gestite da StorageGRID in un nodo.	Dispositivi che contengono unità auto-crittografanti. Tutti i dati presenti sulle unità protette sono protetti contro la perdita fisica o la rimozione dal data center. La crittografia dell'unità non si applica alle unità gestite SANtricity. Se si dispone di un dispositivo di archiviazione con unità auto-crittografanti e controller SANtricity, è possibile abilitare la sicurezza delle unità in SANtricity.
Sicurezza dell'unità in SANtricity System Manager	Se la funzionalità Drive Security è abilitata per l'appliance StorageGRID, è possibile utilizzare "Gestore del sistema SANtricity" per creare e gestire la chiave di sicurezza. La chiave è necessaria per accedere ai dati presenti sulle unità protette.	Dispositivi di archiviazione dotati di unità FDE (Full Disk Encryption) o unità auto-crittografanti. Tutti i dati presenti sulle unità protette sono protetti contro la perdita fisica o la rimozione dal data center. Non può essere utilizzato con alcuni elettrodomestici o con apparecchi di servizio.
Crittografia degli oggetti memorizzati	Si abilita il "Crittografia degli oggetti memorizzati" opzione nel Grid Manager. Se abilitata, tutti i nuovi oggetti che non sono crittografati a livello di bucket o a livello di oggetto vengono crittografati durante l'acquisizione.	Dati di oggetti S3 appena acquisiti. Gli oggetti archiviati esistenti non sono crittografati. I metadati degli oggetti e altri dati sensibili non sono crittografati.
Crittografia del bucket S3	Si invia 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 dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per il bucket. Gli oggetti bucket esistenti non sono crittografati. I metadati degli oggetti e altri dati sensibili non sono crittografati. "Operazioni sui bucket"

Opzione di crittografia	Come funziona	Si applica a
Crittografia lato server (SSE) degli oggetti S3	Si invia una richiesta S3 per memorizzare un oggetto e includere <code>x-amz-server-side-encryption</code> intestazione della richiesta.	Solo dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non sono crittografati. StorageGRID gestisce le chiavi. "Utilizzare la crittografia lato server"
Crittografia lato server degli oggetti S3 con chiavi fornite dal cliente (SSE-C)	Si invia una richiesta S3 per memorizzare un oggetto e si includono tre intestazioni di richiesta. • <code>x-amz-server-side-encryption-customer-algorithm</code> • <code>x-amz-server-side-encryption-customer-key</code> • <code>x-amz-server-side-encryption-customer-key-MD5</code>	Solo dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non sono crittografati. Le chiavi vengono gestite all'esterno di StorageGRID. "Utilizzare la crittografia lato server"
Crittografia del volume esterno o dell'archivio dati	Per crittografare un intero volume o un intero datastore, è possibile utilizzare un metodo di crittografia esterno a StorageGRID , se supportato dalla piattaforma di distribuzione.	Tutti i dati degli oggetti, i metadati e i dati di configurazione del sistema, presupponendo che ogni volume o archivio dati sia crittografato. Un metodo di crittografia esterno garantisce un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati.

Opzione di crittografia	Come funziona	Si applica a
Crittografia degli oggetti al di fuori di StorageGRID	Si utilizza un metodo di crittografia esterno a StorageGRID per crittografare i dati e i metadati degli oggetti prima che vengano acquisiti in StorageGRID.	Solo dati e metadati degli oggetti (i dati di configurazione del sistema non sono crittografati). Un metodo di crittografia esterno garantisce 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 l'utente: protezione dei dati mediante crittografia lato client"

Utilizzare più metodi di crittografia

A seconda delle esigenze, è possibile utilizzare più di un metodo di crittografia contemporaneamente. Per esempio:

- È possibile utilizzare un KMS per proteggere i nodi degli apparecchi e anche utilizzare la funzionalità di sicurezza dell'unità in SANtricity System Manager per "crittografare due volte" i dati sulle unità auto-crittografanti negli stessi apparecchi.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e utilizzare anche l'opzione di crittografia degli oggetti archiviati per crittografare tutti gli oggetti quando vengono acquisiti.

Se solo una piccola parte dei tuoi oggetti richiede la crittografia, valuta la possibilità di controllare la crittografia a livello di bucket o di singolo oggetto. L'abilitazione di più livelli di crittografia comporta un costo aggiuntivo in termini di prestazioni.

Gestisci i certificati

Gestire i certificati di sicurezza

I certificati di sicurezza sono piccoli file di dati utilizzati per creare connessioni sicure e affidabili tra i componenti StorageGRID e tra i componenti StorageGRID e i sistemi esterni.

StorageGRID utilizza due tipi di certificati di sicurezza:

- **I certificati del server** sono obbligatori quando si utilizzano connessioni HTTPS. I certificati server vengono utilizzati per stabilire connessioni sicure tra client e server, autenticando l'identità di un server rispetto ai suoi client e fornendo un percorso di comunicazione sicuro per i dati. Sia il server che il client dispongono ciascuno di una copia del certificato.
- **I certificati client** autenticano l'identità di un client o di un utente sul server, garantendo un'autenticazione più sicura rispetto alle sole password. I certificati client non crittografano i dati.

Quando un client si connette al server tramite 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 presente sulla propria copia del certificato. Se le firme corrispondono, il client avvia una sessione con il server utilizzando la stessa chiave pubblica.

StorageGRID funge da server per alcune connessioni (ad esempio l'endpoint del bilanciatore del carico) o da client per altre connessioni (ad esempio il servizio di replica CloudMirror).

Certificato CA predefinito della griglia

StorageGRID include un'autorità di certificazione (CA) integrata che genera un certificato CA Grid interno durante l'installazione del sistema. Per impostazione predefinita, il certificato Grid CA viene utilizzato per proteggere il traffico StorageGRID interno. Un'autorità di certificazione (CA) esterna può rilasciare certificati personalizzati pienamente conformi alle policy di sicurezza delle informazioni della tua organizzazione. Sebbene sia possibile utilizzare il certificato Grid CA per un ambiente non di produzione, la procedura consigliata per un ambiente di produzione è quella di utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Sono supportate anche le connessioni non protette senza certificato, ma non sono consigliate.

- I certificati CA personalizzati non rimuovono i certificati interni; tuttavia, i certificati personalizzati dovrebbero essere quelli specificati per la verifica delle connessioni al server.
- Tutti i certificati personalizzati devono soddisfare i ["linee guida per il rafforzamento del sistema per i certificati del server"](#).
- StorageGRID supporta il raggruppamento dei certificati di una CA in un singolo file (noto come pacchetto 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 StorageGRID.

Certificati di sicurezza di accesso

È possibile accedere alle informazioni su tutti i certificati StorageGRID in un'unica posizione, insieme ai collegamenti al flusso di lavoro di configurazione per ciascun certificato.

Passi

1. Da Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global

Grid CA

Client

Load balancer endpoints

Tenants

Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type 	Expiration date  
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Selezionare una scheda nella pagina Certificati per informazioni su ciascuna categoria di certificato e per accedere alle impostazioni del certificato. Puoi accedere a una scheda se hai ["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 bilanciatore del carico:** protegge le connessioni tra i client S3 e il bilanciatore del carico StorageGRID .
- **Tenant:** protegge le connessioni ai server di federazione delle identità o dagli endpoint dei servizi di piattaforma alle risorse di archiviazione S3.
- **Altro:** protegge le connessioni StorageGRID che richiedono certificati specifici.

Di seguito viene descritta ogni scheda con link ad ulteriori dettagli sul certificato.

Globale

I certificati globali proteggono l'accesso a StorageGRID dai browser Web e dai client API S3 esterni. Durante l'installazione, inizialmente l'autorità di certificazione StorageGRID genera due certificati globali. La procedura migliore per un ambiente di produzione è quella di utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna.

- [Certificato di interfaccia di gestione](#): Protegge le connessioni del browser Web del client alle interfacce di gestione StorageGRID .
- [Certificato API S3](#): Protegge le connessioni API client ai nodi di archiviazione, ai nodi di amministrazione e ai nodi gateway, che le applicazioni client S3 utilizzano 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**
- **Tipo**: personalizzato o predefinito. + Per una maggiore sicurezza della rete, dovresti sempre utilizzare un certificato personalizzato.
- **Data di scadenza**: se si utilizza il certificato predefinito, non viene visualizzata alcuna data di scadenza.

Puoi:

- Sostituisci i certificati predefiniti con certificati personalizzati firmati da un'autorità di certificazione esterna per migliorare la sicurezza della griglia:
 - ["Sostituisci il certificato dell'interfaccia di gestione predefinita generata da StorageGRID"](#) utilizzato per le connessioni Grid Manager e Tenant Manager.
 - ["Sostituisci il certificato API S3"](#) utilizzato per le connessioni del nodo di archiviazione e dell'endpoint del bilanciatore del carico (facoltativo).
- ["Ripristina il certificato dell'interfaccia di gestione predefinita"](#) .
- ["Ripristina il certificato API S3 predefinito"](#) .
- ["Utilizzare uno script per generare un nuovo certificato di interfaccia di gestione autofirmato"](#) .
- Copia o scarica il ["certificato di interfaccia di gestione"](#) O ["Certificato API S3"](#) .

Griglia CA

IL [Certificato CA di Grid](#) , generato dall'autorità di certificazione StorageGRID durante l'installazione StorageGRID , protegge tutto il traffico interno StorageGRID .

Le informazioni sul certificato includono la data di scadenza e il contenuto del certificato.

Puoi ["copia o scarica il certificato Grid CA"](#) , ma non puoi cambiarlo.

Cliente

[Certificati client](#), generati da un'autorità di certificazione esterna, proteggono le connessioni tra gli strumenti di monitoraggio esterni e il database StorageGRID Prometheus.

La tabella dei certificati contiene una riga per ogni certificato client configurato e indica se il certificato può essere utilizzato per l'accesso al database Prometheus, insieme alla data di scadenza del certificato.

Puoi:

- ["Carica o genera un nuovo certificato client."](#)
- Seleziona un nome di certificato per visualizzarne i dettagli, dove puoi:
 - ["Cambia il nome del certificato client."](#)
 - ["Imposta l'autorizzazione di accesso a Prometheus."](#)
 - ["Carica e sostituisci il certificato client."](#)
 - ["Copia o scarica il certificato client."](#)
 - ["Rimuovere il certificato client."](#)
- Seleziona **Azioni** per eseguire rapidamente ["modificare"](#), ["allegare"](#), o ["rimuovere"](#) un certificato client. È possibile selezionare fino a 10 certificati client e rimuoverli contemporaneamente utilizzando **Azioni > Rimuovi**.

Endpoint del bilanciatore del carico

[Certificati degli endpoint del bilanciatore del carico](#) proteggere le connessioni tra i client S3 e il servizio StorageGRID Load Balancer sui nodi gateway e sui nodi amministrativi.

La tabella degli endpoint del bilanciatore del carico contiene una riga per ogni endpoint del bilanciatore del carico configurato e indica se per l'endpoint viene utilizzato il certificato API S3 globale o un certificato endpoint del bilanciatore del carico personalizzato. Per ogni certificato viene visualizzata anche la data di scadenza.



Le modifiche al certificato di un endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Puoi:

- ["Visualizza un endpoint del bilanciatore del carico"](#), compresi i dettagli del suo certificato.
- ["Specificare un certificato dell'endpoint del bilanciatore del carico per FabricPool."](#)
- ["Utilizzare il certificato API S3 globale"](#) invece di generare un nuovo certificato dell'endpoint del bilanciatore del carico.

inquilini

Gli inquilini possono utilizzare [certificati del server di federazione delle identità](#) o [certificati endpoint del servizio di piattaforma](#) per proteggere le loro connessioni con StorageGRID.

La tabella dei tenant contiene una riga per ogni tenant e indica se ogni tenant ha l'autorizzazione a utilizzare la propria fonte di identità o i servizi della piattaforma.

Puoi:

- ["Seleziona un nome di tenant per accedere a Tenant Manager"](#)
- ["Seleziona un nome tenant per visualizzare i dettagli della federazione dell'identità del tenant"](#)
- ["Seleziona un nome tenant per visualizzare i dettagli dei servizi della piattaforma tenant"](#)
- ["Specificare un certificato dell'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 loro nome funzionale. Altri certificati di sicurezza includono:

- [Certificati del pool di archiviazione cloud](#)
- [Certificati di notifica di avviso via e-mail](#)
- [Certificati del server syslog esterno](#)
- [Certificati di connessione alla federazione di rete](#)
- [Certificati di federazione delle identità](#)
- [Certificati del server di gestione delle chiavi \(KMS\)](#)
- [Certificati Single Sign-On](#)

Le informazioni indicano il tipo di certificato utilizzato da una funzione e le date di scadenza dei certificati server e client, se applicabile. 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 per altri certificati solo se si dispone dell'"[autorizzazione appropriata](#)".

Puoi:

- ["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 della federazione di rete"](#)
- ["Visualizzare e modificare un certificato di federazione delle identità"](#)
- ["Carica i certificati del server e del client del server di gestione delle chiavi \(KMS\)"](#)
- ["Specificare manualmente un certificato SSO per un trust della parte affidabile"](#)

Dettagli del certificato di sicurezza

Di seguito viene descritto ciascun tipo di certificato di sicurezza, con link alle istruzioni di implementazione.

Certificato di 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 StorageGRID , consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza. Questo certificato autentica anche le connessioni Grid Management API e Tenant Management API. È possibile utilizzare il certificato predefinito creato durante l'installazione oppure caricare un certificato personalizzato.	CONFIGURAZIONE > Sicurezza > Certificati , seleziona la scheda Globale , quindi seleziona Certificato dell'interfaccia di gestione	"Configurare i certificati dell'interfaccia di gestione"

Certificato API S3

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica le connessioni client S3 sicure a un nodo di archiviazione e agli endpoint del bilanciatore del carico (facoltativo).	CONFIGURAZIONE > Sicurezza > Certificati , seleziona la scheda Globale , quindi seleziona Certificato API S3	"Configurare i certificati API S3"

Certificato CA di Grid

Vedi il [Descrizione del certificato CA Grid predefinito](#) .

Certificato client amministratore

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Cliente	Installato su ciascun client, consente a StorageGRID di autenticare l'accesso dei client esterni. • Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus. • Consente il monitoraggio sicuro di StorageGRID tramite strumenti esterni.	CONFIGURAZIONE > Sicurezza > Certificati e quindi selezionare la scheda Client	"Configurare i certificati client"

Certificato dell'endpoint del bilanciatore del carico

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i client S3 e il servizio StorageGRID Load Balancer sui nodi gateway e sui nodi amministrativi. È possibile caricare o generare un certificato del bilanciatore del carico quando si configura un endpoint del bilanciatore del carico. Le applicazioni client utilizzano il certificato del bilanciatore del carico quando si connettono a StorageGRID per salvare e recuperare i dati degli oggetti. Puoi anche utilizzare una versione personalizzata del globale Certificato API S3 certificato per autenticare le connessioni al servizio Load Balancer. Se il certificato globale viene utilizzato per autenticare le connessioni del bilanciatore del carico, non è necessario caricare o generare un certificato separato per ogni endpoint del bilanciatore del carico. Nota: il certificato utilizzato per l'autenticazione del bilanciatore del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID .	CONFIGURAZIONE > Rete > Endpoint del bilanciatore del carico	• "Configurare gli endpoint del bilanciatore del carico" • "Creare un endpoint del bilanciatore del carico per FabricPool"

Certificato endpoint del pool di archiviazione cloud

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione da un pool di archiviazione cloud StorageGRID a una posizione di archiviazione esterna, ad esempio S3 Glacier o Microsoft Azure Blob Storage. Per ogni tipo di provider cloud è richiesto un certificato diverso.	ILM > Pool di archiviazione	"Creare un pool di archiviazione cloud"

Certificato di notifica di avviso via e-mail

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra un server di posta elettronica SMTP e StorageGRID utilizzata per le notifiche di avviso. • Se le comunicazioni con il server SMTP richiedono Transport Layer Security (TLS), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta elettronica SMTP richiede certificati client per l'autenticazione.	AVVISI > Configurazione e-mail	"Imposta notifiche e-mail per gli avvisi"

Certificato del 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 del server syslog esterno per le connessioni TCP, RELP/TCP e UDP a un server syslog esterno.	CONFIGURAZIONE > Monitoraggio > Server di audit e syslog	"Utilizzare un server syslog esterno"

Certificato di connessione alla federazione di rete

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autenticare e crittografare le informazioni inviate tra l'attuale sistema StorageGRID e un'altra griglia in una connessione di federazione di griglia.	CONFIGURAZIONE > Sistema > Federazione di griglia	• "Creare connessioni di federazione di griglia" • "Ruota i certificati di connessione"

Certificato di federazione dell'identità

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra StorageGRID e un provider di identità esterno, come Active Directory, OpenLDAP o Oracle Directory Server. Utilizzato per la federazione delle identità, che consente la gestione di gruppi di amministratori e utenti da parte di un sistema esterno.	CONFIGURAZIONE > Controllo accessi > Federazione identità	"Utilizzare la federazione delle identità"

Certificato del server di gestione delle chiavi (KMS)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra StorageGRID e un server di gestione delle chiavi esterno (KMS), che fornisce chiavi di crittografia ai nodi dell'appliance StorageGRID .	CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi	" Aggiungi 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 archiviazione S3.	Gestore inquilino > ARCHIVIAZIONE (S3) > Endpoint dei servizi della piattaforma	" Crea endpoint dei servizi della piattaforma " " Modifica endpoint dei servizi della piattaforma "

Certificato Single Sign-On (SSO)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i servizi di federazione delle identità, come Active Directory Federation Services (AD FS) e StorageGRID , utilizzati per le richieste Single Sign-On (SSO).	CONFIGURAZIONE > Controllo accessi > Single sign-on	" Configurare l'accesso singolo "

Esempi di certificati

Esempio 1: servizio Load Balancer

In questo esempio, StorageGRID funge da server.

1. È possibile configurare un endpoint del bilanciatore del carico e caricare o generare un certificato del server in StorageGRID.
2. Si configura una connessione client S3 all'endpoint del bilanciatore del carico e si carica lo stesso certificato sul client.
3. Quando il client desidera salvare o recuperare dati, si connette all'endpoint del bilanciatore del carico tramite 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 presente sulla propria 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 di gestione delle chiavi esterno (KMS)

In questo esempio, StorageGRID funge da client.

1. Utilizzando il software Key Management Server esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server firmato da una CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, puoi configurare un server KMS e caricare i certificati del server e del client, nonché la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, invia 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 StorageGRID può essere considerato attendibile.
5. Il server KMS risponde utilizzando la connessione convalidata.

Tipi di certificati server supportati

Il sistema StorageGRID supporta certificati personalizzati crittografati con RSA o ECDSA (Elliptic Curve Digital Signature Algorithm).



Il tipo di cifratura per la policy di sicurezza deve corrispondere al tipo di certificato del server. Ad esempio, i cifrari RSA richiedono certificati RSA, mentre i cifrari ECDSA richiedono certificati ECDSA. Vedere ["Gestire i certificati di sicurezza"](#). Se si configura un criterio di sicurezza personalizzato che non è compatibile con il certificato del server, è possibile ["ripristinare temporaneamente la politica di sicurezza predefinita"](#).

Per ulteriori informazioni su come StorageGRID protegge le connessioni client, vedere ["Sicurezza per i client S3"](#).

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 Tenant Manager senza visualizzare avvisi di sicurezza. È anche possibile ripristinare il certificato dell'interfaccia di gestione predefinito o generarne uno nuovo.

Informazioni su questo compito

Per impostazione predefinita, a ogni nodo amministrativo viene rilasciato un certificato firmato dalla CA della griglia. Questi certificati firmati da CA possono essere sostituiti da un singolo certificato di interfaccia di gestione personalizzata comune e dalla corrispondente chiave privata.

Poiché per tutti i nodi amministrativi viene utilizzato un singolo certificato di interfaccia di gestione personalizzata, è necessario specificare il certificato come certificato jolly o multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definisci il certificato personalizzato in modo che corrisponda a tutti i nodi amministrativi nella griglia.

È necessario completare la configurazione sul server e, a seconda dell'autorità di certificazione radice (CA) utilizzata, gli utenti potrebbero dover installare anche il certificato Grid CA nel browser Web che utilizzeranno per accedere a Grid Manager e Tenant Manager.



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza del certificato server per l'interfaccia di gestione** viene attivato quando il certificato server sta per scadere. Se necessario, è possibile visualizzare la data di scadenza del certificato corrente selezionando **CONFIGURAZIONE > Sicurezza > Certificati** e controllando 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 anziché un indirizzo IP, il browser visualizza un errore di certificato senza un'opzione per ignorarlo se si verifica una delle seguenti situazioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- [Voi ripristinare un certificato di interfaccia di gestione personalizzato al certificato del server predefinito](#) .

Aggiungi un certificato di interfaccia di gestione personalizzato

Per aggiungere un certificato di interfaccia di gestione personalizzato, puoi fornire il tuo certificato o generarne uno utilizzando Grid Manager.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
3. Seleziona **Usa certificato personalizzato**.
4. Carica o genera il certificato.

Carica il certificato

Caricare i file del certificato del server richiesti.

a. Seleziona **Carica certificato**.

b. Carica i file del certificato del server richiesti:

- **Certificato del server**: file del certificato del server personalizzato (codificato PEM).
- **Chiave privata del certificato**: file della chiave privata del certificato del server personalizzato(`.key`).



Le chiavi private EC devono essere di 224 bit o più grandi. Le chiavi private RSA devono essere di 2048 bit o più grandi.

- **Bundle CA**: un singolo file facoltativo contenente i certificati di ciascuna autorità di certificazione (CA) emittente intermedia. Il file dovrebbe contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.

c. Espandi **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se hai caricato un bundle CA facoltativo, ogni certificato verrà visualizzato in una scheda separata.

- Selezionare **Scarica certificato** per salvare il file del certificato oppure selezionare **Scarica bundle CA** per salvare il bundle del certificato.

Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Seleziona **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.

Genera certificato

Generare i file del certificato del server.



La procedura consigliata per un ambiente di produzione è quella di utilizzare un certificato di interfaccia di gestione personalizzato firmato da un'autorità di certificazione esterna.

a. Seleziona **Genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completamente qualificati da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.

Campo	Descrizione
Proprietà intellettuale	Uno o più indirizzi IP da includere nel certificato.
Oggetto (facoltativo)	Soggetto X.509 o nome distinto (DN) del proprietario del certificato. Se non viene immesso alcun valore in questo campo, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni validi	Numero di giorni dopo la creazione in cui scade il certificato.
Aggiungi estensioni di utilizzo delle chiavi	Se selezionata (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e per l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

- Selezionare **Scarica certificato** per salvare il file del certificato.

Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.

e. Seleziona **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. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno affinché tutti gli avvisi di scadenza del certificato correlati vengano cancellati.

6. Dopo aver aggiunto un certificato di interfaccia di gestione personalizzato, la pagina Certificato di interfaccia di gestione visualizza informazioni dettagliate sui certificati in uso. + È possibile scaricare o copiare il certificato PEM a seconda delle necessità.

Ripristina il certificato dell'interfaccia di gestione predefinita

È possibile tornare a utilizzare il certificato dell'interfaccia di gestione predefinito per le connessioni Grid

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina il certificato dell'interfaccia di gestione predefinita, i file del certificato del server personalizzato configurati vengono eliminati e non possono essere recuperati dal sistema. Per tutte le successive nuove connessioni client verrà utilizzato il certificato dell'interfaccia di gestione predefinita.

4. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.

Utilizzare uno script per generare un nuovo certificato di interfaccia di gestione autofirmato

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

- Hai ["autorizzazioni di accesso specifiche"](#).
- Tu hai il `Passwords.txt` file.

Informazioni su questo compito

La procedura migliore per un ambiente di produzione è quella di utilizzare un certificato firmato da un'autorità di certificazione esterna.

Passi

1. Ottieni il nome di dominio completo (FQDN) di ciascun nodo di amministrazione.
2. Accedi al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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. Per esempio, `*.ui.storagegrid.example.com` usa il carattere jolly `*` per rappresentare `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
- Impostato `--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. Puoi usare il `--days` argomento per sovrascrivere il periodo di validità

predefinito.



Il periodo di validità di un certificato inizia quando `make-certificate` è in esecuzione. È necessario assicurarsi che il client di gestione sia sincronizzato con la stessa origine oraria 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 richiesto dal client API di gestione.

4. Seleziona e copia il certificato.

Includi i tag BEGIN e END nella tua selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`

6. Conferma che il certificato è stato configurato:

- a. Accedi al Grid Manager.
- b. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**
- c. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.

7. Configura il tuo client di gestione per utilizzare il certificato pubblico che hai copiato. Includi i tag BEGIN e END.

Scarica o copia il certificato dell'interfaccia di gestione

È possibile salvare o copiare il contenuto del certificato dell'interfaccia di gestione per utilizzarlo altrove.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scarica il file del certificato o il pacchetto CA

Scarica il certificato o il pacchetto CA .pem file. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Scarica certificato** o **Scarica pacchetto CA**.

Se si scarica un bundle CA, tutti i certificati nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione .pem .

Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copia il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM**.

Se si copia un bundle CA, tutti i certificati nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incolla il certificato copiato in un editor di testo.

c. Salva il file di testo con l'estensione .pem .

Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati API S3

È possibile sostituire o ripristinare il certificato del server utilizzato per le connessioni client S3 ai nodi di archiviazione o agli endpoint del bilanciatore del carico. Il certificato server personalizzato sostitutivo è specifico per la tua organizzazione.



I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere ["StorageGRID 11.8: configurare i certificati API S3 e Swift"](#) .

Informazioni su questo compito

Per impostazione predefinita, a ogni nodo di archiviazione viene rilasciato un certificato server X.509 firmato dalla CA della griglia. Questi certificati firmati da CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla corrispondente chiave privata.

Per tutti i nodi di archiviazione viene utilizzato un singolo certificato server personalizzato, pertanto è necessario specificare il certificato come carattere jolly o certificato multidominio se i client devono verificare il nome host durante la connessione all'endpoint di archiviazione. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi di archiviazione nella griglia.

Dopo aver completato la configurazione sul server, potrebbe essere necessario installare anche il certificato Grid CA nel client API S3 che utilizzerai per accedere al sistema, a seconda dell'autorità di certificazione

radice (CA) che stai utilizzando.



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza del certificato server globale per l'API S3** viene attivato quando il certificato del server radice sta per scadere. Se necessario, è possibile visualizzare la data di scadenza del certificato corrente selezionando **CONFIGURAZIONE > Sicurezza > Certificati** e controllando la data di scadenza del certificato API S3 nella scheda Globale.

È possibile caricare o generare un certificato API S3 personalizzato.

Aggiungi un certificato API S3 personalizzato

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato API S3**.
3. Seleziona **Usa certificato personalizzato**.
4. Carica o genera il certificato.

Carica il certificato

Caricare i file del certificato del server richiesti.

a. Seleziona **Carica certificato**.

b. Carica i file del certificato del server richiesti:

- **Certificato del server:** file del certificato del server personalizzato (codificato PEM).
- **Chiave privata del certificato:** file della chiave privata del certificato del server personalizzato(`.key`).



Le chiavi private EC devono essere di 224 bit o più grandi. Le chiavi private RSA devono essere di 2048 bit o più grandi.

- **Bundle CA:** un singolo file facoltativo contenente i certificati di ciascuna autorità di certificazione emittente intermedia. Il file dovrebbe contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.

c. Selezionare i dettagli del certificato per visualizzare i metadati e il PEM per ciascun certificato API S3 personalizzato caricato. Se hai caricato un bundle CA facoltativo, ogni certificato verrà visualizzato in una scheda separata.

- Selezionare **Scarica certificato** per salvare il file del certificato oppure selezionare **Scarica bundle CA** per salvare il bundle del certificato.

Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Seleziona **Salva**.

Il certificato server personalizzato viene utilizzato per le successive nuove connessioni client S3.

Genera certificato

Generare i file del certificato del server.

a. Seleziona **Genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completamente qualificati da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
Proprietà intellettuale	Uno o più indirizzi IP da includere nel certificato.

Campo	Descrizione
Oggetto (facoltativo)	Soggetto X.509 o nome distinto (DN) del proprietario del certificato. Se non viene immesso alcun valore in questo campo, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni validi	Numero di giorni dopo la creazione in cui scade il certificato.
Aggiungi estensioni di utilizzo delle chiavi	Se selezionata (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e per l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati e il PEM per il certificato API S3 personalizzato generato.

- Selezionare **Scarica certificato** per salvare il file del certificato.

Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.

e. Seleziona **Salva**.

Il certificato server personalizzato viene utilizzato per le successive nuove connessioni client S3.

5. Selezionare una scheda per visualizzare i metadati per il certificato del server StorageGRID predefinito, un certificato firmato da una CA caricato o un certificato personalizzato generato.



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno affinché tutti gli avvisi di scadenza del certificato correlati vengano cancellati.

6. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.

7. Dopo aver aggiunto un certificato API S3 personalizzato, la pagina del certificato API S3 visualizza informazioni dettagliate sul certificato API S3 personalizzato in uso. + È possibile scaricare o copiare il certificato PEM a seconda delle necessità.

Ripristina il certificato API S3 predefinito

È possibile tornare a utilizzare il certificato API S3 predefinito per le connessioni client S3 ai nodi di archiviazione. Tuttavia, non è possibile utilizzare il certificato API S3 predefinito per un endpoint del bilanciatore del carico.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato API S3**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina la versione predefinita del certificato API S3 globale, i file del certificato del server personalizzato configurati vengono eliminati e non possono essere recuperati dal sistema. Per le successive nuove connessioni client S3 ai nodi di archiviazione verrà utilizzato il certificato API S3 predefinito.

4. Selezionare **OK** per confermare l'avviso e ripristinare il certificato API S3 predefinito.

Se si dispone dell'autorizzazione di accesso Root e per le connessioni degli endpoint del bilanciatore del carico è stato utilizzato il certificato API S3 personalizzato, verrà visualizzato un elenco degli endpoint del bilanciatore del carico che non saranno più accessibili utilizzando il certificato API S3 predefinito. Vai a ["Configurare gli endpoint del bilanciatore del carico"](#) per modificare o rimuovere gli endpoint interessati.

5. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.

Scarica o copia il certificato API S3

È possibile salvare o copiare il contenuto del certificato API S3 per utilizzarlo altrove.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato API S3**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scarica il file del certificato o il pacchetto CA

Scarica il certificato o il pacchetto CA .pem file. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Scarica certificato** o **Scarica pacchetto CA**.

Se si scarica un bundle CA, tutti i certificati nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione .pem .

Ad esempio: storagegrid_certificate.pem

Copia certificato o pacchetto CA PEM

Copia il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM**.

Se si copia un bundle CA, tutti i certificati nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incolla il certificato copiato in un editor di testo.

c. Salva il file di testo con l'estensione .pem .

Ad esempio: storagegrid_certificate.pem

Informazioni correlate

- ["Utilizzare l'API REST S3"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)

Copia il certificato Grid CA

StorageGRID utilizza un'autorità di certificazione (CA) interna per proteggere il traffico interno. Questo certificato non cambia se carichi i tuoi certificati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Informazioni su questo compito

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 .

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati** e quindi selezionare la scheda **CA griglia**.

2. Nella sezione **Certificato PEM**, scaricare o copiare il certificato.

Scarica il file del certificato

Scarica il certificato .pem file.

- Seleziona **Scarica certificato**.
- Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione .pem .

Ad esempio: `storagegrid_certificate.pem`

Copia certificato PEM

Copia il testo del certificato per incollarlo altrove.

- Selezionare **Copia certificato PEM**.
- Incolla il certificato copiato in un editor di testo.
- Salva 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 la convalida rigorosa del nome host e non supportano la disabilitazione della convalida rigorosa del nome host, come i client ONTAP che utilizzano FabricPool, è possibile generare o caricare un certificato server quando si configura l'endpoint del bilanciatore del carico.

Prima di iniziare

- Hai ["autorizzazioni di accesso specifiche"](#) .
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

Informazioni su questo compito

Quando si crea un endpoint del bilanciatore 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 consigliabile utilizzare un certificato firmato da una CA nota. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono anche più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

I passaggi seguenti forniscono linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, vedere ["Configurare StorageGRID per FabricPool"](#) .

Passi

- Facoltativamente, configurare un gruppo ad alta disponibilità (HA) da utilizzare per FabricPool .
- Creare un endpoint del bilanciatore del carico S3 da utilizzare per FabricPool .

Quando si crea un endpoint del bilanciatore del carico HTTPS, viene richiesto di caricare il certificato del server, la chiave privata del certificato e il bundle CA facoltativo.

3. Collegare StorageGRID come livello cloud in ONTAP.

Specificare la porta dell'endpoint del bilanciatore del carico e il nome di dominio completo utilizzato nel certificato CA caricato. Quindi, fornire il certificato CA.



Se il certificato StorageGRID è stato emesso da una CA intermedia, è necessario fornire il certificato della CA intermedia. Se il certificato StorageGRID è stato emesso direttamente dalla CA radice, è necessario fornire il certificato della CA radice.

Configurare i certificati client

I certificati client consentono ai client esterni autorizzati di accedere al database StorageGRID Prometheus, offrendo agli strumenti esterni un modo sicuro per monitorare StorageGRID.

Se è necessario accedere a StorageGRID tramite uno strumento di monitoraggio esterno, è necessario caricare o generare un certificato client tramite 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 server non riuscito, l'avviso **Scadenza dei certificati client configurati nella pagina Certificati** viene attivato quando il certificato server sta per scadere. Se necessario, è possibile visualizzare la data di scadenza del certificato corrente selezionando **CONFIGURAZIONE > Sicurezza > Certificati** e controllando la data di scadenza del certificato client nella scheda Client.



Se si utilizza un server di gestione delle chiavi (KMS) per proteggere i dati sui nodi appliance configurati in modo speciale, consultare le informazioni specifiche su ["caricamento di un certificato client KMS"](#) .

Prima di iniziare

- Hai i permessi di accesso Root.
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Per configurare un certificato client:
 - Hai l'indirizzo IP o il nome di dominio del nodo di amministrazione.
 - Se hai configurato il certificato dell'interfaccia di gestione StorageGRID , disponi della CA, del certificato client e della chiave privata utilizzati per configurare il certificato dell'interfaccia di gestione.
 - Per caricare il tuo certificato, la chiave privata del certificato è disponibile sul tuo computer locale.
 - La chiave privata deve essere stata salvata o registrata al momento della sua creazione. Se non si dispone della chiave privata originale, è necessario crearne una nuova.
- Per modificare un certificato client:
 - Hai l'indirizzo IP o il nome di dominio del nodo di amministrazione.
 - Per caricare il tuo certificato o un nuovo certificato, la chiave privata, il certificato client e la CA (se utilizzata) sono disponibili sul tuo computer locale.

Aggiungi certificati client

Per aggiungere il certificato client, utilizzare una di queste procedure:

- [Certificato dell'interfaccia di gestione già configurato](#)
- [Certificato client rilasciato da 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 fornita dal cliente, un certificato client e una chiave privata.

Passi

1. In Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Inserisci un nome per il certificato.
4. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.
5. Selezionare **Continua**.
6. Per il passaggio **Allega certificati**, caricare il certificato dell'interfaccia di gestione.
 - a. Seleziona **Carica certificato**.
 - b. Selezionare **Sfoglia** e selezionare il file del certificato dell'interfaccia di gestione(.pem).
 - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
 - Selezionare **Copia certificato PEM** 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 rilasciato da CA

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si prevede di aggiungere un certificato client per Prometheus che utilizza un certificato client rilasciato da una CA e una chiave privata.

Passi

1. Eseguire i passaggi per ["configurare un certificato di interfaccia di gestione"](#) .
2. In Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
3. Selezionare **Aggiungi**.
4. Inserisci un nome per il certificato.
5. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.

6. Selezionare **Continua**.
7. Per la fase **Allega certificati**, carica i file del certificato client, della chiave privata e del bundle CA:
 - a. Seleziona **Carica certificato**.
 - b. Selezionare **Sfoggia** e selezionare il certificato client, la chiave privata e i file bundle CA(`.pem`).
 - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
 - Selezionare **Copia certificato PEM** 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 prevede di aggiungere un certificato client per Prometheus che utilizza la funzione di generazione del certificato in Grid Manager.

Passi

1. In Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Inserisci un nome per il certificato.
4. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.
5. Selezionare **Continua**.
6. Per il passaggio **Allega certificati**, seleziona **Genera certificato**.
7. Specificare le informazioni del certificato:
 - **Oggetto** (facoltativo): soggetto X.509 o nome distinto (DN) del proprietario del certificato.
 - **Giorni di validità**: numero di giorni di validità del certificato generato, a partire dal momento in cui viene generato.
 - **Aggiungi estensioni per l'utilizzo delle chiavi**: se selezionato (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



Lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

8. Seleziona **Genera**.
9. Selezionare **Dettagli del certificato client** per visualizzare i metadati del certificato e il PEM del certificato.



Dopo aver chiuso la finestra di dialogo, non sarà possibile visualizzare la chiave privata del certificato. Copia o scarica la chiave in un luogo sicuro.

- Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.
- Selezionare **Scarica certificato** per salvare il file del certificato.

Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia chiave privata** per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Scarica chiave privata** per salvare la chiave privata come file.

Specificare il nome del file della chiave privata e il percorso di download.

10. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

11. In Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e quindi seleziona la scheda **Globale**.

12. Selezionare **Certificato interfaccia di gestione**.

13. Seleziona **Usa certificato personalizzato**.

14. Carica i file `certificate.pem` e `private_key.pem` da [dettagli del certificato client](#) fare un passo. Non è necessario caricare il bundle CA.
 - a. Selezionare **Carica certificato** e poi **Continua**.
 - b. Carica ogni file di certificato (`.pem`).
 - c. Selezionare **Salva** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella pagina dei certificati dell'interfaccia di gestione.

15. [Configurare uno strumento di monitoraggio esterno](#), come Grafana.

Configura uno strumento di monitoraggio esterno

Passi

1. Configura le seguenti impostazioni sul tuo strumento di monitoraggio esterno, come Grafana.

- a. **Nome**: inserisci un nome per la connessione.

StorageGRID non richiede queste informazioni, ma è necessario fornire un nome per testare 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. Abilita **TLS Client Auth** e **Con certificato CA**.
- d. In Dettagli autorizzazione TLS/SSL, copia e incolla: +

- Il certificato CA dell'interfaccia di gestione per **CA Cert**
- Il certificato client per **Client Cert**
- La chiave privata per **Chiave client**

e. **ServerName**: immettere il nome di dominio del nodo di amministrazione.

ServerName deve corrispondere al nome di dominio così come appare nel certificato dell'interfaccia di gestione.

2. Salvare e testare 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 strumento di monitoraggio esterno.

Per informazioni sulle metriche, vedere ["istruzioni per il monitoraggio StorageGRID"](#) .

Modifica i certificati client

È possibile modificare un certificato client amministratore per cambiarne il nome, abilitare o disabilitare l'accesso a Prometheus o caricare un nuovo certificato quando quello attuale è scaduto.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.

Nella tabella sono elencate le date di scadenza dei certificati e le autorizzazioni di accesso a Prometheus. Se un certificato sta per scadere o è già scaduto, nella tabella viene visualizzato un messaggio e viene attivato un avviso.

2. Seleziona il certificato che vuoi modificare.

3. Seleziona **Modifica** e poi seleziona **Modifica nome e autorizzazione**

4. Inserisci un nome per il certificato.

5. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.

6. Selezionare **Continua** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

Allega nuovo certificato client

È possibile caricare un nuovo certificato quando quello attuale è scaduto.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.

Nella tabella sono elencate le date di scadenza dei certificati e le autorizzazioni di accesso a Prometheus. Se un certificato sta per scadere o è già scaduto, nella tabella viene visualizzato un messaggio e viene attivato un avviso.

2. Seleziona il certificato che vuoi modificare.

3. Selezionare **Modifica** e quindi selezionare un'opzione di modifica.

Carica il certificato

Copia il testo del certificato per incollarlo altrove.

- a. Selezionare **Carica certificato** e poi **Continua**.
- b. Carica il nome del certificato client(.pem).

Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

- Selezionare **Scarica certificato** per salvare il file del certificato.

Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione .pem .

Ad esempio: storagegrid_certificate.pem

- Selezionare **Copia certificato PEM** 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.

Genera certificato

Genera il testo del certificato da incollare altrove.

- a. Seleziona **Genera certificato**.
- b. Specificare le informazioni del certificato:

- **Oggetto** (facoltativo): soggetto X.509 o nome distinto (DN) del proprietario del certificato.
- **Giorni di validità**: numero di giorni di validità del certificato generato, a partire dal momento in cui viene generato.
- **Aggiungi estensioni per l'utilizzo delle chiavi**: se selezionato (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



Lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

- c. Seleziona **Genera**.
- d. Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.



Dopo aver chiuso la finestra di dialogo, non sarà possibile visualizzare la chiave privata del certificato. Copia o scarica la chiave in un luogo sicuro.

- Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.

- Selezionare **Scarica certificato** per salvare il file del certificato.

Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia chiave privata** per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Scarica chiave privata** per salvare la chiave privata come file.

Specificare il nome del file della chiave privata e il percorso di download.

e. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

Scarica o copia i certificati client

È possibile scaricare o copiare un certificato client per utilizzarlo altrove.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.
2. Seleziona il certificato che vuoi copiare o scaricare.
3. Scarica o copia il certificato.

Scarica il file del certificato

Scarica il certificato `.pem` file.

- a. Seleziona **Scarica certificato**.
- b. Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Copia il certificato

Copia il testo del certificato per incollarlo altrove.

- a. Selezionare **Copia certificato PEM**.
- b. Incolla il certificato copiato in un editor di testo.
- c. Salva il file di testo con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Rimuovere i certificati client

Se non hai più bisogno di un certificato client amministratore, puoi rimuoverlo.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.
2. Seleziona il certificato che desideri rimuovere.
3. Selezionare **Elimina** e quindi confermare.



Per rimuovere fino a 10 certificati, seleziona ciascun certificato da rimuovere nella scheda Client, quindi seleziona **Azioni > Elimina**.

Dopo la rimozione di un certificato, i client che lo utilizzavano devono specificare un nuovo certificato client per accedere al database StorageGRID Prometheus.

Configurare le impostazioni di sicurezza

Gestire la politica TLS e SSH

La policy TLS e SSH determina quali protocolli e cifrari vengono utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure con i servizi StorageGRID interni.

La policy di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. In generale, utilizzare il criterio di compatibilità moderna (predefinito), a meno che il sistema non debba essere conforme ai Common Criteria o non sia necessario utilizzare altri cifrari.



Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare le cifrature in queste policy.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .

Seleziona una politica di sicurezza

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza**.

La scheda **Criteri TLS e SSH** mostra i criteri disponibili. La policy attualmente attiva è contrassegnata da un segno di spunta verde nel riquadro della policy.



2. Esamina i riquadri per scoprire le policy disponibili.

Politica	Descrizione
Compatibilità moderna (predefinita)	Utilizzare il criterio predefinito se è necessaria una crittografia avanzata e a meno che non si abbiano requisiti particolari. Questa policy è compatibile con la maggior parte dei client TLS e SSH.
Compatibilità legacy	Utilizza questa policy se hai bisogno di opzioni di compatibilità aggiuntive per i client più vecchi. Le opzioni aggiuntive presenti in questa policy potrebbero renderla meno sicura rispetto alla policy di compatibilità moderna.
Criteri comuni	Utilizzare questa politica se è necessaria la certificazione Common Criteria.
FIPS rigoroso	Utilizzare questa policy se è richiesta la certificazione Common Criteria e si deve utilizzare NetApp Cryptographic Security Module 3.0.8 per le connessioni client esterne agli endpoint del bilanciatore del carico, Tenant Manager e Grid Manager. L'utilizzo di questa policy potrebbe ridurre le prestazioni. Nota: Dopo aver selezionato questa policy, tutti i nodi devono essere "riavviato in modo progressivo" per attivare il modulo di sicurezza crittografica NetApp . Utilizzare Manutenzione > Riavvio progressivo per avviare e monitorare i riavvii.
Costume	Crea una policy personalizzata se devi applicare i tuoi cifrari.

3. Per visualizzare i dettagli sui cifrari, i protocolli e gli algoritmi di ogni policy, seleziona **Visualizza dettagli**.

4. Per modificare la policy corrente, seleziona **Usa policy**.

Accanto a **Criterio attuale** nel riquadro del criterio appare un segno di spunta verde.

Crea una policy di sicurezza personalizzata

È possibile creare una policy personalizzata se è necessario applicare cifrari personalizzati.

Passi

1. Dal riquadro della policy più simile alla policy personalizzata che desideri creare, seleziona **Visualizza dettagli**.
2. Selezionare **Copia negli appunti**, quindi selezionare **Annulla**.



3. Dal riquadro **Criterio personalizzato**, seleziona **Configura e usa**.
4. Incolla il JSON che hai copiato e apporta le modifiche necessarie.
5. Seleziona **Utilizza policy**.

Accanto a **Criterio attuale** nel riquadro Criterio personalizzato appare un segno di spunta verde.

6. Facoltativamente, seleziona **Modifica configurazione** per apportare ulteriori modifiche alla nuova policy personalizzata.

Ripristina temporaneamente la politica di sicurezza predefinita

Se hai configurato un criterio di sicurezza personalizzato, potresti non essere in grado di accedere a Grid Manager se il criterio TLS configurato non è compatibile con ["certificato del server configurato"](#).

È possibile ripristinare temporaneamente i criteri di sicurezza predefiniti.

Passi

1. Accedi a un nodo di amministrazione:
 - a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Esegui il seguente comando:

```
restore-default-cipher-configurations
```

3. Da un browser Web, accedi a Grid Manager sullo stesso nodo di amministrazione.
4. Segui i passaggi in [Seleziona una politica di sicurezza](#) per configurare nuovamente la policy.

È possibile configurare la sicurezza di rete e degli oggetti per crittografare gli oggetti archiviati, per impedire determinate richieste S3 o per consentire alle connessioni client ai nodi di archiviazione di utilizzare HTTP anziché HTTPS.

Crittografia degli oggetti memorizzati

La crittografia degli oggetti archiviati consente la crittografia di tutti i dati degli oggetti quando vengono acquisiti tramite S3. Per impostazione predefinita, gli oggetti archiviati non sono crittografati, ma è possibile scegliere di crittografarli utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando si abilita l'impostazione, tutti gli oggetti appena acquisiti vengono crittografati, ma non viene apportata alcuna modifica agli oggetti archiviati esistenti. Se si disabilita la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena acquisiti non vengono crittografati.

L'impostazione di crittografia degli oggetti archiviati si applica solo agli oggetti S3 che non sono stati crittografati tramite crittografia a livello di bucket o di oggetto.

Per maggiori dettagli sui metodi di crittografia StorageGRID , vedere ["Esaminare i metodi di crittografia StorageGRID"](#) .

Impedisci la modifica del client

Impedisci modifiche al client è un'impostazione a livello di sistema. Quando è selezionata l'opzione **Impedisci modifiche 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

Abilita HTTP per le connessioni del nodo di archiviazione

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per tutte le connessioni dirette ai nodi di archiviazione. Facoltativamente, è possibile abilitare HTTP per queste connessioni, ad esempio quando si testa una griglia non di produzione.

Utilizzare HTTP per le connessioni ai nodi di archiviazione solo se i client S3 devono effettuare connessioni HTTP direttamente ai nodi di archiviazione. 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 ogni endpoint del bilanciatore del carico"](#) per utilizzare HTTP o HTTPS).

Vedere ["Riepilogo: indirizzi IP e porte per le connessioni client"](#) per scoprire quali porte utilizzano i client S3 quando si connettono ai nodi di archiviazione tramite HTTP o HTTPS.

Seleziona le opzioni

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai i permessi di accesso Root.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **Rete e oggetti**.
3. Per la crittografia degli oggetti archiviati, utilizzare l'impostazione **Nessuno** (predefinita) se non si desidera che gli oggetti archiviati vengano crittografati oppure selezionare **AES-128** o **AES-256** per crittografare gli oggetti archiviati.
4. Facoltativamente, seleziona **Impedisci modifica client** se vuoi impedire ai client S3 di effettuare richieste specifiche.



Se si modifica questa impostazione, ci vorrà circa un minuto prima che la nuova impostazione venga applicata. Il valore configurato viene memorizzato nella cache per migliorare le prestazioni e il ridimensionamento.

5. Facoltativamente, selezionare **Abilita HTTP per le connessioni ai nodi di archiviazione** se i client si connettono direttamente ai nodi di archiviazione e si desidera utilizzare le connessioni HTTP.



Prestare attenzione quando si abilita HTTP per una griglia di produzione perché le richieste verranno inviate non crittografate.

6. Seleziona **Salva**.

Modificare le impostazioni di sicurezza dell'interfaccia

Le impostazioni di sicurezza dell'interfaccia consentono di controllare se gli utenti vengono disconnessi se rimangono inattivi per un periodo di tempo superiore a quello specificato e se una traccia dello stack viene inclusa nelle risposte di errore dell'API.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai "[Permesso di accesso root](#)".

Informazioni su questo compito

La pagina **Impostazioni di sicurezza** include le impostazioni **Timeout di inattività del browser** e **Stack trace dell'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. Il valore predefinito è 15 minuti.

Il timeout di inattività del browser è controllato anche da quanto segue:

- Un timer StorageGRID separato e non configurabile, incluso per la sicurezza del sistema. Il token di autenticazione di ciascun utente scade 16 ore dopo l'accesso dell'utente. Quando scade l'autenticazione di un utente, l'utente viene automaticamente disconnesso, anche se il timeout di inattività del browser è disabilitato o il valore per il timeout del browser non è stato raggiunto. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.
- Impostazioni di timeout per il provider di identità, presupponendo che l'accesso Single Sign-On (SSO) sia abilitato per StorageGRID.

Se l'SSO è abilitato e il browser di un utente scade, l'utente deve reinserire le proprie credenziali SSO per accedere nuovamente a StorageGRID. Vedere "[Configurare l'accesso singolo](#)".

Stack trace dell'API di gestione

Controlla se viene restituita una traccia dello stack nelle risposte di errore dell'API Grid Manager e Tenant Manager.

Questa opzione è disabilitata per impostazione predefinita, ma potrebbe essere opportuno abilitare questa funzionalità per un ambiente di prova. In generale, negli ambienti di produzione è consigliabile lasciare la traccia dello stack disabilitata per evitare di rivelare dettagli software interni quando si verificano errori API.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **Interfaccia**.
3. Per modificare l'impostazione del timeout di inattività del browser:
 - a. Espandi la fisarmonica.
 - b. Per modificare il periodo di timeout, specificare un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è 15 minuti.
 - c. Per disattivare questa funzione, deselezionare la casella di controllo.
 - d. Seleziona **Salva**.

La nuova impostazione non ha effetto sugli utenti che hanno effettuato l'accesso. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser affinché la nuova impostazione di timeout abbia effetto.

4. Per modificare l'impostazione per la traccia dello stack dell'API di gestione:
 - a. Espandi la fisarmonica.
 - b. Selezionare la casella di controllo per restituire una traccia dello stack nelle risposte di errore dell'API Grid Manager e Tenant Manager.



Lasciare la traccia dello stack disabilitata negli ambienti di produzione per evitare di rivelare dettagli software interni quando si verificano errori API.

- c. Seleziona **Salva**.

Configurare i server di gestione delle chiavi

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).

StorageGRID supporta solo determinati server di gestione delle chiavi. Per un elenco dei prodotti e delle versioni supportati, utilizzare ["Strumento matrice di interoperabilità NetApp \(IMT\)"](#).

È possibile utilizzare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi per tutti i nodi dell'appliance StorageGRID in cui è abilitata l'impostazione **Crittografia nodi** durante l'installazione. Utilizzando server di gestione delle chiavi con questi nodi appliance è possibile proteggere i dati anche se un'appliance viene rimossa dal data center. Dopo aver crittografato i volumi dell'appliance, non sarà possibile accedere ai dati sull'appliance a meno che il nodo non sia in grado di comunicare con il KMS.



StorageGRID non crea né gestisce le chiavi esterne utilizzate per crittografare e decrittografare i nodi dell'appliance. Se si prevede di 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 di attività di gestione chiave esula dallo scopo di queste istruzioni. Se hai bisogno di aiuto, consulta la documentazione del tuo server di gestione delle chiavi o contatta l'assistenza tecnica.

Configurazione KMS e appliance

Prima di poter utilizzare un server di gestione delle chiavi (KMS) per proteggere i dati StorageGRID sui nodi dell'appliance, è necessario completare due attività di configurazione: impostare uno o più server KMS e abilitare la crittografia dei nodi per i nodi dell'appliance. Una volta completate queste due attività di configurazione, il processo di gestione delle chiavi avviene automaticamente.

Il diagramma di flusso mostra i passaggi principali per utilizzare un KMS per proteggere i dati StorageGRID sui nodi dell'appliance.

Il diagramma di flusso mostra la configurazione di KMS e la configurazione dell'appliance che avvengono in parallelo; tuttavia, è possibile configurare i server di gestione delle chiavi prima o dopo aver abilitato la crittografia dei nodi per i nuovi nodi dell'appliance, in base alle proprie esigenze.

Configurare il server di gestione delle chiavi (KMS)

La configurazione di un server di gestione delle chiavi comprende i seguenti passaggi generali.

Fare un passo	Fare riferimento a
Accedi al software KMS e aggiungi un client per StorageGRID a ciascun KMS o cluster KMS.	"Configurare StorageGRID come client nel KMS"
Ottenere le informazioni richieste per il client StorageGRID sul KMS.	"Configurare StorageGRID come client nel KMS"
Aggiungere il KMS a Grid Manager, assegnarlo a un singolo sito o a un gruppo predefinito di siti, caricare i certificati richiesti e salvare la configurazione del KMS.	"Aggiungere un server di gestione delle chiavi (KMS)"

Impostare l'apparecchio

La configurazione di un nodo appliance per l'utilizzo KMS include i seguenti passaggi generali.

1. Durante la fase di configurazione hardware dell'installazione dell'appliance, utilizzare StorageGRID Appliance Installer per abilitare l'impostazione **Crittografia nodo** per l'appliance.



Non è possibile abilitare l'impostazione **Crittografia nodo** dopo aver aggiunto un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia nodo abilitata.

2. Eseguire il programma di installazione dell'appliance StorageGRID . Durante l'installazione, a ciascun volume dell'appliance viene assegnata una chiave di crittografia dati casuale (DEK), come segue:
 - Le DEK vengono utilizzate 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 è crittografato da una chiave di crittografia a chiave master (KEK). La KEK iniziale è una chiave temporanea che crittografa le DEK finché l'appliance non riesce a connettersi al KMS.
3. Aggiungere il nodo dell'appliance a StorageGRID.

Vedere ["Abilita la crittografia del nodo"](#) per i dettagli.

Processo di crittografia della gestione delle chiavi (avviene automaticamente)

La crittografia della gestione delle chiavi include i seguenti passaggi di alto livello che vengono eseguiti automaticamente.

1. Quando si installa un'appliance con crittografia dei nodi abilitata nella griglia, StorageGRID determina se esiste una configurazione KMS per il sito che contiene il nuovo nodo.
 - Se per il sito è già stato configurato un KMS, l'appliance riceve la configurazione KMS.
 - Se non è ancora stato configurato un KMS per il sito, i dati sull'appliance continuano a essere crittografati dalla KEK temporanea finché 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 ora viene utilizzata per crittografare e decrittografare le DEK per i volumi dell'appliance.



Tutti i dati esistenti prima che il nodo dell'appliance crittografata 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 finché la chiave temporanea non viene sostituita dalla chiave di crittografia KMS.

4. Se l'appliance viene accesa o riavviata, si riconnette al KMS per richiedere la chiave. La chiave, che viene salvata nella memoria volatile, non può sopravvivere a un'interruzione di corrente o a un riavvio.

Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi

Prima di configurare un server di gestione delle chiavi esterno (KMS), è necessario comprendere le considerazioni e i requisiti.

Quale versione di KMIP è supportata?

StorageGRID supporta KMIP versione 1.4.

["Specifiche del protocollo di interoperabilità per la gestione delle chiavi versione 1.4"](#)

Quali sono le considerazioni da fare in merito alla rete?

Le impostazioni del firewall di rete devono consentire a ciascun nodo dell'appliance di comunicare tramite 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 dei nodi abbia accesso alla rete del KMS o del cluster 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 effettua connessioni KMIP a un KMS o a un cluster KMS, in base a ciò che il KMS supporta e a quale ["Politica TLS e SSH"](#) che stai utilizzando.

StorageGRID negozia il protocollo e la crittografia (TLS 1.2) o la suite di crittografia (TLS 1.3) con il KMS quando effettua la connessione. Per vedere quali versioni del protocollo e cifrari/suite di cifrari sono disponibili, rivedere `tlsOutbound` sezione della policy TLS e SSH attiva della griglia (**CONFIGURAZIONE > Sicurezza Impostazioni di sicurezza**).

Quali elettrodomestici sono supportati?

È possibile utilizzare un server di gestione delle chiavi (KMS) per gestire le chiavi di crittografia per qualsiasi appliance StorageGRID nella griglia in cui sia abilitata l'impostazione **Crittografia nodo**. Questa impostazione può essere abilitata solo durante la fase di configurazione hardware dell'installazione dell'appliance tramite StorageGRID Appliance Installer.



Non è possibile abilitare la crittografia dei nodi dopo aver aggiunto 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 basati su software (non appliance), inclusi i seguenti:

- Nodi distribuiti come macchine virtuali (VM)
- Nodi distribuiti all'interno di motori di container su host Linux

I nodi distribuiti su queste altre piattaforme possono utilizzare la crittografia al di fuori di StorageGRID a livello di datastore o disco.

Quando dovrei 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 i tenant. Questo ordine garantisce che i nodi siano protetti prima che i dati degli oggetti vengano memorizzati su di essi.

È possibile configurare i server di gestione delle chiavi in Grid Manager prima o dopo aver installato i nodi dell'appliance.

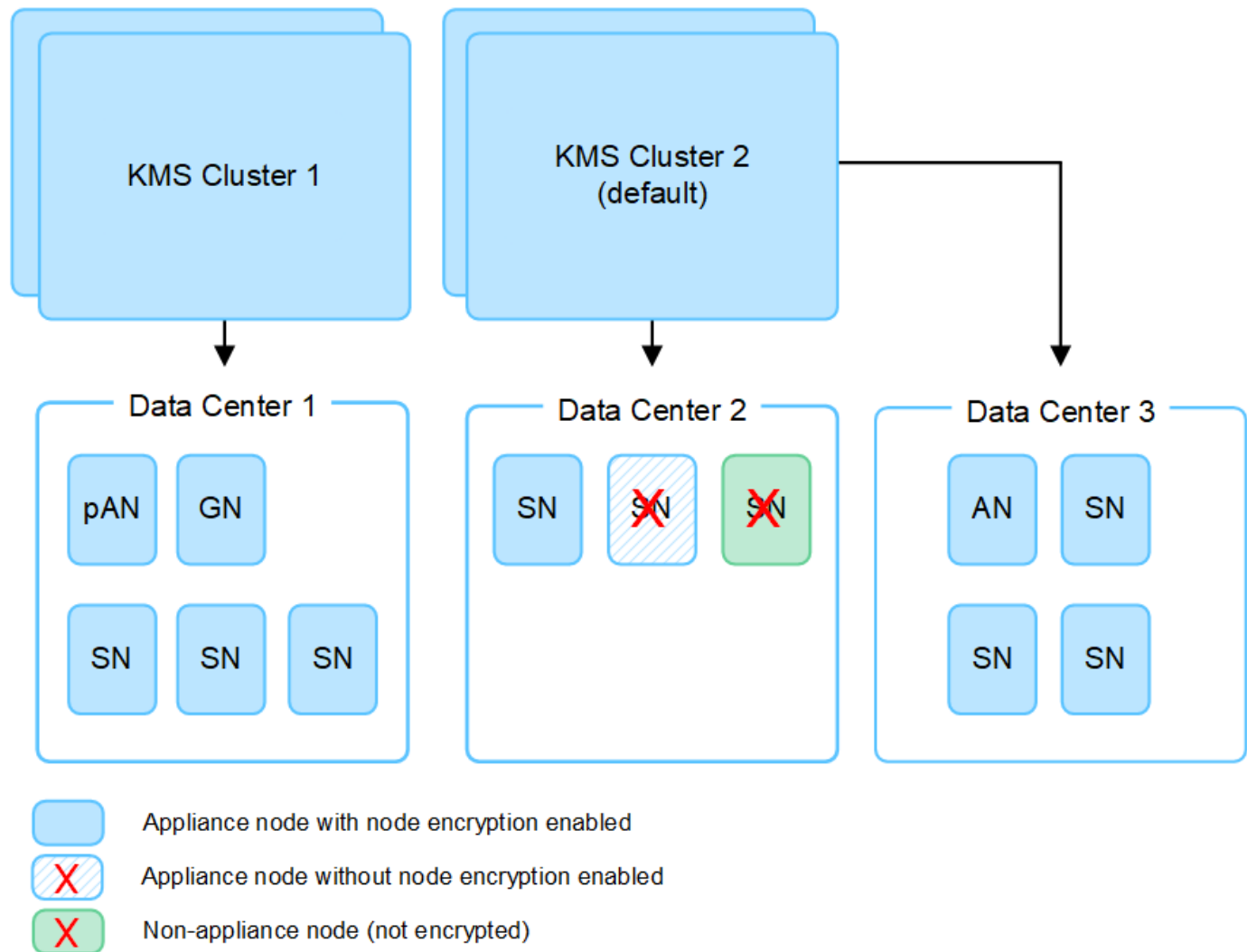
Di quanti server di gestione delle chiavi ho bisogno?

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'uso di cluster KMS. Ogni cluster KMS contiene più server di gestione delle chiavi replicati che condividono impostazioni di configurazione e chiavi di crittografia. Si consiglia di utilizzare cluster KMS per la gestione delle chiavi perché migliorano le capacità di failover di una configurazione ad alta disponibilità.

Ad esempio, supponiamo che il tuo sistema StorageGRID abbia tre siti di data center. È possibile configurare un cluster KMS per fornire una chiave a tutti i nodi dell'appliance nel Data Center 1 e un secondo cluster KMS per fornire una chiave a tutti i nodi dell'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.

Tieni presente che non puoi utilizzare un KMS per nodi non appliance o per nodi appliance per i quali non è stata abilitata l'impostazione **Crittografia nodo** durante l'installazione.



Cosa succede quando si ruota una chiave?

Come buona pratica di sicurezza, dovresti periodicamente ["ruotare la chiave di crittografia"](#) utilizzato da ciascun KMS configurato.

Quando sarà disponibile la nuova versione della chiave:

- Viene distribuito automaticamente ai nodi dell'appliance crittografata nel sito o nei siti associati al KMS. La distribuzione dovrebbe avvenire entro un'ora dalla rotazione della chiave.
- Se il nodo dell'appliance crittografata è offline quando viene distribuita la nuova versione della chiave, il nodo riceverà la nuova chiave non appena si riavvia.
- Se per qualsiasi motivo non è possibile utilizzare la nuova versione della chiave per crittografare i volumi dell'appliance, viene attivato l'avviso **Rotazione chiave di crittografia KMS non riuscita** per il nodo

dell'appliance. Potrebbe essere necessario contattare l'assistenza tecnica per ricevere aiuto nella risoluzione di questo avviso.

Posso riutilizzare un nodo appliance dopo averlo crittografato?

Se è necessario installare un'appliance crittografata in un altro sistema StorageGRID, è necessario prima disattivare il nodo della griglia per spostare i dati dell'oggetto su un altro nodo. Quindi, è possibile utilizzare StorageGRID Appliance Installer per ["cancellare la configurazione KMS"](#). La cancellazione della configurazione KMS disabilita l'impostazione **Crittografia nodo** e rimuove l'associazione tra il nodo dell'appliance e la configurazione KMS per il sito StorageGRID.



Senza accesso alla chiave di crittografia KMS, tutti i dati rimasti sul dispositivo non saranno più accessibili e saranno bloccati in modo permanente.

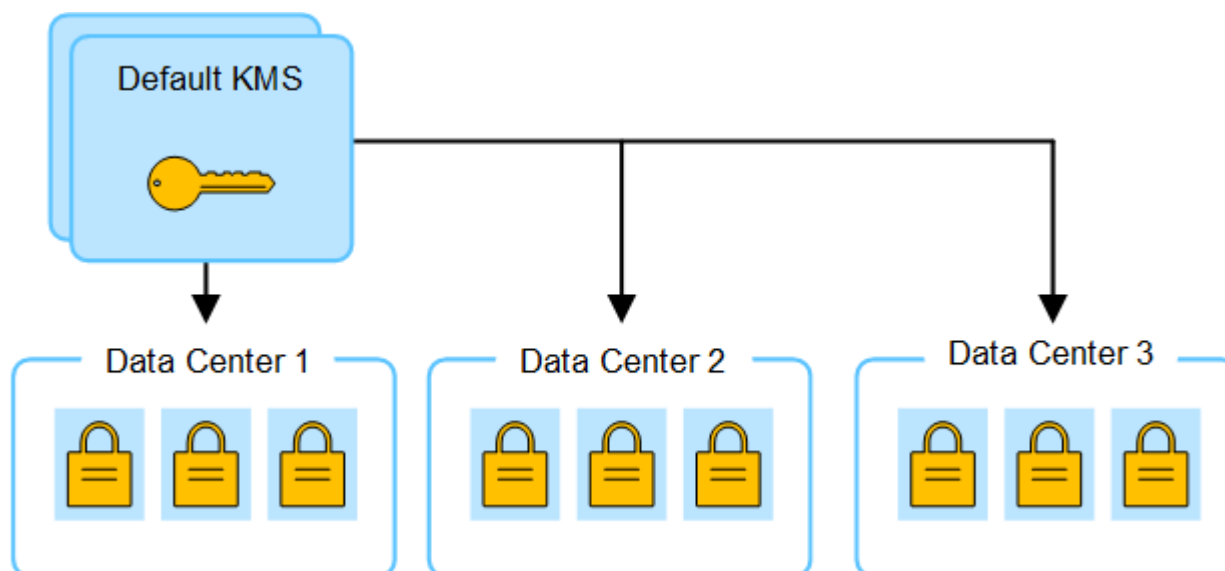
Considerazioni sulla modifica del KMS per un sito

Ogni server di gestione delle chiavi (KMS) o cluster KMS fornisce una chiave di crittografia a tutti i nodi dell'appliance in un singolo sito o in 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 a un altro.

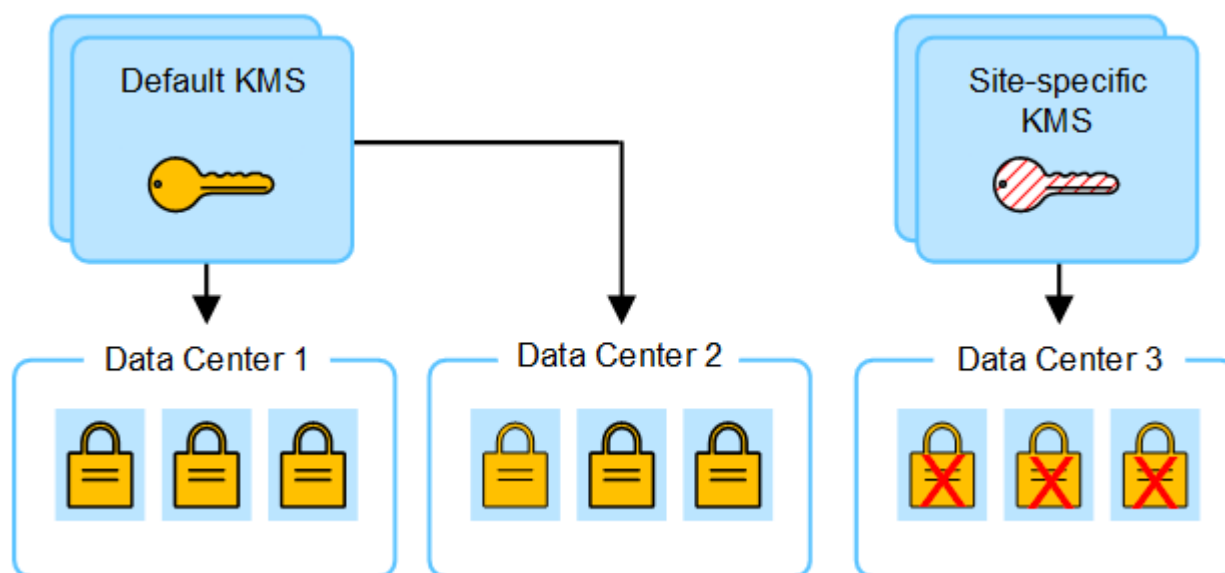
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi dell'appliance precedentemente crittografati in quel sito possano essere decrittografati utilizzando la chiave memorizzata sul nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia dal KMS originale al nuovo KMS. È necessario assicurarsi che il KMS disponga della chiave corretta per decrittografare i nodi dell'appliance crittografati nel sito.

Per esempio:

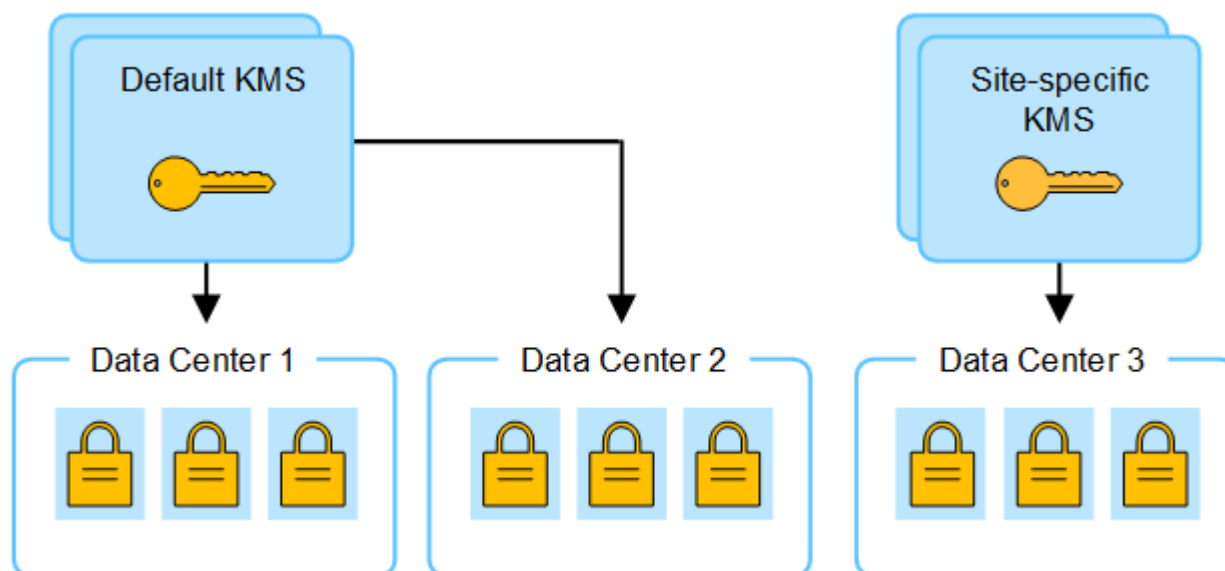
1. Inizialmente si configura un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi dell'appliance in cui è abilitata l'impostazione **Crittografia nodo** si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi dell'appliance in tutti i siti. La stessa chiave deve essere utilizzata anche per decifrare tali apparecchi.



3. Si decide di aggiungere un KMS specifico 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 decrittografare 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 ora dispone della chiave corretta per decrittografare i nodi dell'appliance nel Data Center 3, in modo che possa essere salvata in StorageGRID.



Casi d'uso per modificare il KMS utilizzato per un sito

La tabella riassume i passaggi richiesti nei casi più comuni di modifica del KMS per un sito.

Caso d'uso per la modifica del KMS di un sito	Passaggi richiesti
Hai una o più voci KMS specifiche del sito e vuoi usarne una come KMS predefinito.	Modifica il KMS specifico del sito. Nel campo Gestisci chiavi per, seleziona Siti non gestiti da un altro KMS (KMS predefinito). Il KMS specifico del sito verrà ora utilizzato come KMS predefinito. Si applicherà a tutti i siti che non dispongono di un KMS dedicato. "Modifica un server di gestione delle chiavi (KMS)"
Hai un KMS predefinito e aggiungi un nuovo sito in un'espansione. Non vuoi utilizzare il KMS predefinito per il nuovo sito.	1. Se i nodi dell'appliance nel nuovo sito sono già stati crittografati dal 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, aggiungi il nuovo KMS e seleziona il sito. "Aggiungere 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, modifica la configurazione KMS esistente e inserisci il nuovo nome host o indirizzo IP. "Aggiungere un server di gestione delle chiavi (KMS)"

Configurare StorageGRID come client nel KMS

È necessario configurare StorageGRID come client per ciascun server di gestione delle chiavi esterno o cluster KMS prima di poter aggiungere il KMS a StorageGRID.



Queste istruzioni si applicano a Thales CipherTrust Manager e Hashicorp Vault. Per un elenco dei prodotti e delle versioni supportati, utilizzare ["Strumento matrice di interoperabilità NetApp \(IMT\)"](#).

Passi

1. Dal software KMS, crea un client StorageGRID per ogni KMS o cluster KMS che intendi utilizzare.

Ogni KMS gestisce una singola chiave di crittografia per i nodi degli appliance StorageGRID in un singolo sito o in un gruppo di siti.

2. Crea 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 KMS o cluster KMS.

La chiave di crittografia deve essere pari o superiore a 2.048 bit e deve essere esportabile.

- Chiedi a StorageGRID di creare la chiave. Ti verrà chiesto quando esegui il test e salvi dopo ["caricamento dei certificati client"](#).
3. Registrare le seguenti informazioni per ciascun KMS o cluster KMS.

Quando aggiungi il KMS a StorageGRID, hai bisogno di queste informazioni:

- Nome host o indirizzo IP per ciascun server.
 - Porta KMIP utilizzata dal KMS.
 - Alias della chiave per la chiave di crittografia nel KMS.
4. Per ogni KMS o cluster 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 codificati in 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 Base-64 Privacy Enhanced Mail (PEM).
- 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 conatterà.



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 client pubblico rilasciato a StorageGRID dal KMS esterno e la chiave privata per il certificato client.

Il certificato client consente a StorageGRID di autenticarsi al KMS.

Aggiungere un server di gestione delle chiavi (KMS)

Per aggiungere ciascun KMS o cluster KMS, utilizzare la procedura guidata StorageGRID Key Management Server.

Prima di iniziare

- Hai esaminato il "[considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi](#)".
- Hai "[StorageGRID configurato come client nel KMS](#)" e disponi delle informazioni richieste per ciascun KMS o cluster KMS.
- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[Permesso di accesso root](#)".

Informazioni su questo compito

Se possibile, configurare eventuali server di gestione delle chiavi specifici del sito prima di configurare un KMS predefinito che si applichi a tutti i siti non gestiti da un altro KMS. Se si crea prima il KMS predefinito, tutti gli apparecchi crittografati tramite nodo nella griglia verranno crittografati dal KMS predefinito. Se in un secondo momento si desidera creare un KMS specifico per il sito, è necessario prima copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Vedere "[Considerazioni sulla modifica del KMS per un sito](#)" per i dettagli.

Passaggio 1: dettagli KMS

Nel passaggio 1 (dettagli KMS) della procedura guidata Aggiungi un server di gestione delle chiavi, è necessario fornire dettagli sul KMS o sul cluster KMS.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina del server di gestione delle chiavi con la scheda Dettagli configurazione selezionata.

2. Seleziona **Crea**.

Viene visualizzato il passaggio 1 (dettagli KMS) della procedura guidata Aggiungi un server di gestione delle chiavi.

3. Immettere le seguenti informazioni per il KMS e il client StorageGRID configurato in tale KMS.

Campo	Descrizione
Nome KMS	Un nome descrittivo che ti aiuti a identificare questo KMS. Deve contenere tra 1 e 64 caratteri.
Nome chiave	L'alias chiave esatto per il client StorageGRID nel KMS. Deve contenere tra 1 e 255 caratteri. Nota: se non hai creato una chiave utilizzando il tuo prodotto KMS, ti verrà chiesto di farla creare a StorageGRID .
Gestisce le chiavi per	Il sito StorageGRID che sarà associato a questo KMS. Se possibile, è opportuno configurare eventuali server di gestione delle chiavi specifici del sito prima di configurare un KMS predefinito che si applichi a tutti i siti non gestiti da un altro KMS. • Selezionare un sito se questo KMS gestirà le chiavi di crittografia per i nodi dell'appliance in un sito specifico. • Seleziona Siti non gestiti da un altro KMS (KMS predefinito) per configurare un KMS predefinito che verrà applicato a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti nelle espansioni successive. Nota: si verificherà un errore di convalida quando si salva la configurazione KMS se si seleziona un sito precedentemente crittografato dal KMS predefinito ma non è stata fornita 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, che è la porta standard KMIP.

Campo	Descrizione
Nome host	Il nome di dominio completo o l'indirizzo IP per il 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 in un cluster KMS.

- Se si sta configurando un cluster KMS, selezionare **Aggiungi un altro nome host** per aggiungere un nome host per ciascun server nel cluster.
- Selezionare **Continua**.

Passaggio 2: carica il certificato del server

Nel passaggio 2 (Carica certificato server) della procedura guidata Aggiungi un server di gestione delle chiavi, caricare il certificato server (o il pacchetto di certificati) per il KMS. Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

Passi

- Dal **Passaggio 2 (Carica certificato server)**, vai alla posizione del certificato server salvato o del pacchetto di certificati.
- Carica il file del certificato.

Vengono visualizzati i metadati del certificato del server.



Se hai caricato un pacchetto di certificati, i metadati di ciascun certificato vengono visualizzati in una scheda separata.

- Selezionare **Continua**.

Passaggio 3: Carica i certificati client

Nel passaggio 3 (Caricamento dei certificati client) della procedura guidata Aggiungi un server di gestione delle chiavi, caricare il certificato client e la chiave privata del certificato client. Il certificato client consente a StorageGRID di autenticarsi presso il KMS.

Passi

- Dal **Passaggio 3 (Caricamento certificati client)**, accedere alla posizione del certificato client.
- Carica il file del certificato client.

Vengono visualizzati i metadati del certificato client.

- Passare alla posizione della chiave privata per il certificato client.
- Carica il file della chiave privata.
- Seleziona **Test e salva**.

Se non esiste una chiave, verrà richiesto a StorageGRID di crearne una.

Vengono testate 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 sul 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 Key Management Server appare come Sconosciuto. StorageGRID potrebbe impiegare fino a 30 minuti per ottenere lo stato effettivo di ciascun certificato. Per visualizzare lo stato attuale, è necessario aggiornare il browser web.

6. Se viene visualizzato un messaggio di errore quando si seleziona **Test e salva**, rivedere i dettagli del messaggio e quindi selezionare **OK**.

Ad esempio, potresti ricevere un errore 422: Entità non elaborabile se un test di connessione non riesce.

7. Se è necessario salvare la configurazione corrente senza testare la connessione esterna, selezionare **Forza salvataggio**.



Selezionando **Forza salvataggio** la configurazione KMS viene salvata, ma non viene testata la connessione esterna da ciascun dispositivo a quel KMS. Se si verifica un problema con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance in cui è abilitata la crittografia dei nodi nel sito interessato. Potresti perdere l'accesso ai tuoi dati finché i problemi non saranno risolti.

8. Rivedi l'avviso di conferma e seleziona **OK** se sei sicuro di voler forzare il salvataggio della configurazione.

La configurazione KMS viene salvata ma la connessione al KMS non viene testata.

Gestire un KMS

La gestione di un server di gestione delle chiavi (KMS) implica 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](#)".
- Tu hai il "[autorizzazione di accesso richiesta](#)".

Visualizza i dettagli 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 del server e del client.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina del server di gestione delle chiavi, che mostra le seguenti informazioni:

- Nella scheda Dettagli configurazione sono elencati tutti i server di gestione delle chiavi configurati.
- Nella scheda Nodi crittografati sono elencati tutti i nodi in cui è abilitata la crittografia dei nodi.

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. Per esempio: 10.10.10.10 and 10.10.10.11 O 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 chiave	L'alias chiave per il client StorageGRID nel KMS.
UID chiave	L'identificatore univoco dell'ultima versione della chiave.	Ultima modifica
Data e 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 cliente	Metadati	I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.

4. Seleziona **Ruota chiave** o utilizza il software KMS ogni volta che le pratiche di sicurezza della tua organizzazione lo richiedono, 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 tonalità completamente diversa.



Non tentare mai di ruotare una chiave modificando 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 modifichi l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittografare i dati.

Gestisci i certificati

Risolvere tempestivamente eventuali problemi relativi ai certificati del server o del client. Se possibile, sostituire i certificati prima che scadano.



Per mantenere l'accesso ai dati, è necessario risolvere il prima possibile eventuali problemi relativi ai certificati.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.
2. Nella tabella, osserva il valore della Scadenza del certificato per ciascun KMS.
3. Se la scadenza del certificato per un KMS è sconosciuta, attendere fino a 30 minuti e quindi aggiornare il browser Web.
4. Se la colonna Scadenza certificato indica che un certificato è scaduto o sta per scadere, selezionare il KMS per andare alla pagina dei dettagli del KMS.
 - a. Selezionare **Certificato server** e verificare il valore per il campo "Scade il".
 - b. Per sostituire il certificato, seleziona **Modifica certificato** per caricare un nuovo certificato.
 - c. Ripetere questi sotto-passaggi e selezionare **Certificato client** anziché 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.

Potrebbero volerci fino a 30 minuti prima che StorageGRID riceva gli aggiornamenti sulla scadenza del certificato. Aggiorna il browser web per visualizzare i valori correnti.



Se viene visualizzato lo stato **Lo stato del certificato del server è sconosciuto**, accertarsi che il KMS consenta di ottenere un certificato del server senza richiedere un certificato del client.

Visualizza i nodi crittografati

È possibile visualizzare informazioni sui nodi dell'appliance nel sistema StorageGRID in cui è abilitata l'impostazione **Crittografia nodi**.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key Management Server. La scheda Dettagli configurazione mostra tutti i server di gestione delle chiavi che sono stati configurati.

2. Nella parte superiore della pagina, seleziona la scheda **Nodi crittografati**.

Nella scheda Nodi crittografati sono elencati i nodi dell'appliance nel sistema StorageGRID in cui è abilitata l'impostazione **Crittografia nodi**.

3. Esaminare le informazioni nella tabella per ciascun nodo dell'appliance.

Colonna	Descrizione
Nome del nodo	Il nome del nodo dell'appliance.
Tipo di nodo	Tipo di nodo: Storage, Admin o Gateway.
Sito	Nome del sito StorageGRID in cui è installato il nodo.
Nome KMS	Nome descrittivo del KMS utilizzato per il nodo. Se non è elencato alcun KMS, selezionare la scheda Dettagli configurazione per aggiungerne uno. "Aggiungere un server di gestione delle chiavi (KMS)"
UID chiave	ID univoco della chiave di crittografia utilizzata per crittografare e decrittografare i dati sul nodo dell'appliance. Per visualizzare l'intero UID della chiave, selezionare il testo. Un trattino (--) indica che l'UID della chiave è sconosciuto, 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, il timestamp viene aggiornato ogni 30 minuti. Dopo le modifiche alla configurazione KMS, potrebbero essere necessari diversi minuti prima che lo stato della connessione venga aggiornato. Nota: aggiorna il browser web per visualizzare i nuovi valori.

4. Se la colonna Stato indica un problema KMS, risolverlo immediatamente.

Durante le normali operazioni KMS, lo stato sarà **Connesso a KMS**. Se un nodo è disconnesso dalla rete, viene visualizzato lo stato di connessione del nodo (Amministrativamente inattivo o Sconosciuto).

Altri messaggi di stato corrispondono agli avvisi StorageGRID con gli stessi nomi:

- Impossibile caricare la configurazione KMS
- Errore di connettività KMS
- Nome della chiave di crittografia KMS non trovato
- Rotazione della chiave di crittografia KMS non riuscita
- La chiave KMS non è riuscita a decrittografare un volume dell'appliance
- KMS non è configurato

Eseguire le azioni consigliate per questi avvisi.



È necessario risolvere immediatamente qualsiasi problema per garantire la completa protezione dei dati.

Modifica 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 necessario aver esaminato il ["considerazioni sulla modifica del KMS per un sito"](#).
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Server di gestione delle chiavi, che mostra tutti i server di gestione delle chiavi configurati.

2. Seleziona il KMS che vuoi modificare e seleziona **Azioni > Modifica**.

È anche possibile modificare un KMS selezionando il nome del KMS nella tabella e selezionando **Modifica** nella pagina dei dettagli del KMS.

3. Facoltativamente, aggiornare i dettagli nel **Passaggio 1 (Dettagli KMS)** della procedura guidata Modifica un server di gestione delle chiavi.

Campo	Descrizione
Nome KMS	Un nome descrittivo che ti aiuti a identificare questo KMS. Deve contenere tra 1 e 64 caratteri.
Nome chiave	L'alias chiave esatto per il client StorageGRID nel KMS. Deve contenere tra 1 e 255 caratteri. Solo in rari casi è necessario modificare il nome della chiave. Ad esempio, è necessario modificare il nome della chiave se l'alias è stato rinominato nel KMS o se tutte le versioni della chiave precedente sono state copiate nella cronologia delle versioni del nuovo alias.

Campo	Descrizione
Gestisce le chiavi per	Se stai modificando un KMS specifico del sito e non hai ancora un KMS predefinito, seleziona facoltativamente Siti non gestiti da un altro KMS (KMS predefinito). 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 di un sito, non puoi selezionare un altro sito. Se stai modificando il KMS predefinito, non puoi selezionare un sito specifico.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, che è la porta standard KMIP.
Nome host	Il nome di dominio completo o l'indirizzo IP per il 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 in un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Aggiungi un altro nome host** per aggiungere un nome host per ciascun server nel cluster.

5. Selezionare **Continua**.

Viene visualizzato il passaggio 2 (Carica certificato server) della procedura guidata Modifica un server di gestione delle chiavi.

6. Se è necessario sostituire il certificato del server, selezionare **Sfoggia** e caricare il nuovo file.

7. Selezionare **Continua**.

Viene visualizzato il passaggio 3 (Caricamento dei 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 **Sfoggia** e caricare i nuovi file.

9. Seleziona **Test e salva**.

Vengono testate le connessioni tra il server di gestione delle chiavi e tutti i nodi dell'appliance crittografati tramite nodo nei siti interessati. Se tutte le connessioni dei nodi sono valide e la chiave corretta viene trovata sul 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, rivedere i dettagli del messaggio e selezionare **OK**.

Ad esempio, potresti ricevere un errore 422: Entità non elaborabile se il sito selezionato per questo KMS è già gestito da un altro KMS o se un test di connessione non è riuscito.

11. Se è necessario salvare la configurazione corrente prima di risolvere gli errori di connessione, selezionare **Forza salvataggio**.



Selezionando **Forza salvataggio** la configurazione KMS viene salvata, ma non viene testata la connessione esterna da ciascun dispositivo a quel KMS. Se si verifica un problema con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance in cui è abilitata la crittografia dei nodi nel sito interessato. Potresti perdere l'accesso ai tuoi dati finché i problemi non saranno risolti.

La configurazione KMS è stata salvata.

12. Rivedi l'avviso di conferma e seleziona **OK** se sei sicuro di voler forzare il salvataggio della configurazione.

La configurazione KMS viene salvata, ma la connessione al KMS non viene testata.

Rimuovere un server di gestione delle chiavi (KMS)

In alcuni casi potrebbe essere necessario rimuovere un server di gestione delle chiavi. Ad esempio, potresti voler rimuovere un KMS specifico di un sito se hai dismesso il sito.

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"](#) .
- Tu hai il ["Permesso di accesso root"](#) .

Informazioni su questo compito

È possibile rimuovere un KMS nei seguenti casi:

- È possibile rimuovere un KMS specifico del sito se il sito è stato dismesso o se non include nodi appliance con crittografia dei nodi abilitata.
- È possibile rimuovere il KMS predefinito se per ogni sito che dispone di nodi appliance con crittografia dei nodi abilitata esiste già un KMS specifico.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Server di gestione delle chiavi, che mostra tutti i server di gestione delle chiavi configurati.

2. Seleziona il KMS che vuoi rimuovere e seleziona **Azioni > Rimuovi**.

È anche possibile rimuovere un KMS selezionando il nome del KMS nella tabella e selezionando **Rimuovi** dalla pagina dei dettagli del KMS.

3. Conferma che quanto segue è vero:

- Si sta rimuovendo un KMS specifico del sito per un sito che non dispone di alcun nodo appliance con crittografia del nodo abilitata.
- Stai rimuovendo il KMS predefinito, ma per ogni sito esiste già un KMS specifico con crittografia dei nodi.

4. Selezionare **Sì**.

La configurazione KMS è stata rimossa.

Gestisci le impostazioni proxy

Configurare il proxy di archiviazione

Se si utilizzano servizi di piattaforma o pool di archiviazione cloud, è possibile configurare un proxy non trasparente tra i nodi di archiviazione e gli endpoint S3 esterni. Ad esempio, potrebbe essere necessario un proxy non trasparente per consentire l'invio di messaggi dei servizi della piattaforma a endpoint esterni, come un endpoint su Internet.



Le impostazioni del proxy di archiviazione configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Prima di iniziare

- Hai ["autorizzazioni di accesso specifiche"](#).
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

Informazioni su questo compito

È possibile configurare le impostazioni per un singolo proxy di archiviazione.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni proxy**.
2. Nella scheda **Archiviazione**, seleziona la casella di controllo **Abilita proxy di archiviazione**.
3. Selezionare il protocollo per il proxy di archiviazione.
4. Inserisci il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, immettere 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. Seleziona **Salva**.

Dopo aver salvato il proxy di archiviazione, è possibile configurare e testare nuovi endpoint per i servizi della piattaforma o i pool di archiviazione cloud.



Le modifiche apportate al proxy potrebbero richiedere fino a 10 minuti per diventare effettive.

7. Controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma provenienti 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 tramite HTTP o HTTPS, è possibile configurare un server proxy non trasparente tra i nodi di amministrazione e il supporto tecnico (AutoSupport).

Per ulteriori informazioni su AutoSupport, vedere ["Configura AutoSupport"](#).

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche" .
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato" .

Informazioni su questo compito

È possibile configurare le impostazioni per un singolo proxy amministratore.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni proxy**.

Viene visualizzata la pagina Impostazioni proxy. Per impostazione predefinita, nel menu delle schede è selezionata l'opzione Archiviazione.

2. Selezionare la scheda **Amministrazione**.
3. Selezionare la casella di controllo **Abilita proxy amministratore**.
4. Inserisci il nome host o l'indirizzo IP del server proxy.
5. Inserisci la porta utilizzata per connettersi al server proxy.
6. Facoltativamente, inserisci un nome utente e una password per il server proxy.

Lasciare vuoti questi campi se il server proxy non richiede un nome utente o una password.

7. Seleziona una delle seguenti opzioni:

- Se si desidera proteggere la connessione al proxy di amministrazione, selezionare **Verifica certificato proxy**. Carica un bundle CA per verificare l'autenticità dei certificati SSL presentati dal server proxy di amministrazione.



AutoSupport on Demand, E-Series AutoSupport tramite StorageGRID e la determinazione del percorso di aggiornamento nella pagina di aggiornamento StorageGRID non funzioneranno se è verificato un certificato proxy.

Dopo aver caricato il bundle CA, vengono visualizzati i relativi metadati.

- Se non si desidera convalidare i certificati durante la comunicazione con il server proxy di amministrazione, selezionare **Non verificare il certificato proxy**.

8. Seleziona **Salva**.

Dopo aver salvato il proxy di amministrazione, viene configurato il server proxy tra i nodi di amministrazione e il supporto tecnico.



Le modifiche apportate al proxy potrebbero richiedere fino a 10 minuti per diventare effettive.

9. Se è necessario disattivare il proxy amministratore, deselezionare la casella di controllo **Abilita proxy amministratore**, quindi selezionare **Salva**.

Controllare i firewall

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, potresti voler impedire ai tenant di connettersi a Grid Manager tramite il firewall, oltre a utilizzare altri metodi per controllare l'accesso al sistema.

Se si desidera configurare il firewall interno 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 parte del traffico interno.
8443	Porta Grid Manager limitata sui nodi amministrativi	• I browser Web e i client API di gestione possono accedere a Grid Manager e alla Grid Management API tramite HTTPS. • I browser Web e i client API di gestione non possono accedere a Tenant Manager o all'API Tenant Management. • Le richieste di contenuti interni verranno respinte.
9443	Porta Tenant Manager limitata sui nodi amministrativi	• I browser Web e i client API di gestione possono accedere a Tenant Manager e all'API Tenant Management tramite HTTPS. • I browser Web e i client API di gestione non possono accedere a Grid Manager o all'API Grid Management. • Le richieste di contenuti interni verranno respinte.



L'accesso Single Sign-On (SSO) non è disponibile sulle porte riservate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione tramite Single Sign-On, è necessario utilizzare la porta HTTPS predefinita (443).

Informazioni correlate

- ["Sign in a Grid Manager"](#)
- ["Crea un account inquilino"](#)
- ["Comunicazioni esterne"](#)

Gestire i controlli del firewall interno

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della griglia consentendo di controllare l'accesso di rete al nodo. Utilizzare il firewall per impedire l'accesso alla rete su tutte le porte, ad eccezione di quelle necessarie per la

distribuzione specifica della griglia. Le modifiche alla configurazione apportate nella pagina di controllo del firewall vengono distribuite a ciascun nodo.

Utilizza le tre schede nella pagina di controllo del firewall per personalizzare l'accesso necessario per la tua griglia.

- **Elenco indirizzi privilegiati:** utilizzare questa scheda per consentire l'accesso selezionato alle porte chiuse. È possibile aggiungere indirizzi IP o subnet in notazione CIDR che possono accedere alle porte chiuse utilizzando la scheda Gestisci accesso esterno.
- **Gestisci accesso esterno:** usa questa scheda per chiudere le porte aperte per impostazione predefinita o per riaprire quelle chiuse in precedenza.
- **Rete client non attendibile:** utilizzare questa scheda per specificare se un nodo considera attendibile il traffico in entrata dalla rete client.

Le impostazioni in questa scheda sostituiscono quelle nella scheda Gestisci accesso esterno.

- Un nodo con una rete client non attendibile accetterà solo connessioni sulle porte degli endpoint del bilanciatore del carico configurate su quel nodo (endpoint globali, interfaccia nodo e tipo nodo).
- Le porte degli endpoint del bilanciatore 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 Gestisci accesso esterno sono accessibili, così come tutti gli endpoint del bilanciatore del carico aperti sulla rete client.



Le impostazioni effettuate in una scheda possono influire sulle modifiche di accesso effettuate in un'altra scheda. Assicurati di controllare le impostazioni in tutte le schede per verificare che la tua rete si comporti come previsto.

Per configurare i controlli del firewall interno, vedere ["Configurare i controlli del firewall"](#).

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere ["Controllare l'accesso al firewall esterno"](#).

Elenco indirizzi privilegiati e schede Gestisci accesso esterno

La scheda Elenco indirizzi privilegiati consente di registrare uno o più indirizzi IP a cui è concesso l'accesso alle porte della griglia chiuse. La scheda 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 di griglia). Spesso è possibile utilizzare insieme queste due schede per personalizzare l'esatto accesso alla rete che si desidera consentire alla propria griglia.



Per impostazione predefinita, gli indirizzi IP privilegiati non hanno accesso alla porta della griglia interna.

Esempio 1: utilizzare un jump host per le attività di manutenzione

Supponiamo di voler utilizzare un jump host (un host con sicurezza rafforzata) per l'amministrazione della rete. Potresti seguire questi passaggi generali:

1. Utilizzare la scheda Elenco indirizzi privilegiati per aggiungere l'indirizzo IP dell'host jump.
2. Utilizzare la scheda 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 te, 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 jump. È quindi possibile utilizzare l'host jump per eseguire attività di manutenzione sulla griglia in modo più sicuro.

Esempio 2: Bloccare le porte sensibili

Supponiamo di voler bloccare porte sensibili e il servizio su quella porta (ad esempio, SSH sulla porta 22). È possibile seguire i seguenti passaggi generali:

1. Utilizzare la scheda Elenco indirizzi privilegiati per concedere l'accesso solo agli host che necessitano di accedere al servizio.
2. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte.



Aggiungere l'indirizzo IP privilegiato prima di bloccare l'accesso a qualsiasi porta assegnata 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 te, 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, potresti disattivare alcuni servizi che non intendi utilizzare. Ad esempio, per bloccare il traffico client HTTP S3, è necessario utilizzare l'interruttore nella scheda Gestisci accesso esterno per bloccare la porta 18084.

Scheda Reti client non attendibili

Se si utilizza una rete client, è possibile proteggere StorageGRID da attacchi ostili accettando il traffico client in entrata solo su endpoint configurati in modo esplicito.

Per impostazione predefinita, la rete client su ciascun nodo della griglia è *attendibile*. Ciò significa che, per impostazione predefinita, StorageGRID considera attendibili le connessioni in ingresso 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 su ciascun nodo sia *non attendibile*. Se la rete client di un nodo non è attendibile, il nodo accetta solo connessioni in entrata su porte configurate esplicitamente come endpoint del bilanciatore del carico. Vedere ["Configurare gli endpoint del bilanciatore del carico"](#) e ["Configurare i controlli del firewall"](#).

Esempio 1: il nodo gateway accetta solo richieste HTTPS S3

Supponiamo di voler far sì che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste HTTPS S3. Dovresti eseguire questi passaggi generali:

1. Dal ["Endpoint del bilanciatore del carico"](#) pagina, configura un endpoint del bilanciatore del carico per S3 su

HTTPS sulla porta 443.

2. Nella pagina Controllo firewall, selezionare 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: il nodo di archiviazione invia richieste di servizi della piattaforma S3

Supponiamo di voler abilitare il traffico dei servizi della piattaforma S3 in uscita da un nodo di archiviazione, ma di voler impedire qualsiasi connessione in ingresso a tale nodo di archiviazione sulla rete client. Dovresti eseguire questo passaggio generale:

- Dalla scheda Reti client non attendibili della pagina di controllo del firewall, indicare che la rete client sul nodo di archiviazione non è attendibile.

Dopo aver salvato la configurazione, il nodo di archiviazione non accetta più traffico in entrata sulla rete client, ma continua a consentire richieste in uscita verso le destinazioni dei servizi della piattaforma configurati.

Esempio 3: limitazione dell'accesso a Grid Manager a una subnet

Supponiamo di voler consentire l'accesso a Grid Manager solo su una subnet specifica. Dovresti eseguire i seguenti passaggi:

1. Collega la rete client dei tuoi nodi amministrativi alla subnet.
2. Utilizzare la scheda Rete client non attendibile per configurare la rete client come non attendibile.
3. Quando si crea un endpoint del bilanciatore del carico dell'interfaccia di gestione, immettere la porta e selezionare l'interfaccia di gestione a cui la porta accederà.
4. Selezionare **Sì** per Rete client non attendibile.
5. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte esterne (con o senza indirizzi IP privilegiati impostati per gli host esterni a quella subnet).

Dopo aver salvato la configurazione, solo gli host nella subnet specificata potranno accedere a Grid Manager. Tutti gli altri host sono bloccati.

Configurare il firewall interno

È possibile configurare il firewall StorageGRID per controllare l'accesso alla rete a porte specifiche sui nodi StorageGRID .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Hai esaminato le informazioni in ["Gestire i controlli del firewall"](#) E ["Linee guida per il networking"](#) .
- Se si desidera che un nodo di amministrazione o un nodo gateway accetti il traffico in entrata solo su endpoint configurati in modo esplicito, è necessario definire gli endpoint del bilanciatore del carico.



Quando si modifica la configurazione della rete client, le connessioni client esistenti potrebbero non funzionare se gli endpoint del bilanciatore del carico non sono stati configurati.

Informazioni su questo compito

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 sulla rete Grid, sulla rete di amministrazione e sulla rete client. È anche 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 si fida del traffico in entrata dalla rete client e configurare l'accesso di porte specifiche sulla rete client.

Limitare il numero di porte aperte agli indirizzi IP esterni alla rete solo a quelle assolutamente necessarie aumenta la sicurezza della rete stessa. Utilizzare le impostazioni in ciascuna delle tre schede di controllo del firewall per garantire che siano aperte solo le porte necessarie.

Per ulteriori informazioni sull'utilizzo dei controlli del firewall, inclusi esempi, vedere ["Gestire i controlli del firewall"](#).

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere ["Controllare l'accesso al firewall esterno"](#).

Controlli del firewall di accesso

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Controllo firewall**.

Le tre schede in questa pagina sono descritte in ["Gestire i controlli del firewall"](#).

2. Selezionare una scheda qualsiasi per configurare i controlli del firewall.

È possibile utilizzare queste schede in qualsiasi ordine. Le configurazioni impostate in una scheda non limitano le operazioni eseguibili nelle altre schede; tuttavia, le modifiche apportate alla configurazione in una scheda potrebbero modificare il comportamento delle porte configurate nelle altre schede.

Elenco indirizzi privilegiati

Utilizzare la scheda Elenco indirizzi privilegiati per concedere agli host l'accesso alle porte chiuse per impostazione predefinita o chiuse dalle impostazioni nella scheda Gestisci accesso esterno.

Per impostazione predefinita, gli indirizzi IP e le subnet privilegiati non dispongono di accesso alla griglia interna. Inoltre, gli endpoint del bilanciatore del carico e le porte aggiuntive aperte nella scheda Elenco indirizzi privilegiati sono accessibili anche se bloccati nella scheda Gestisci accesso esterno.



Le impostazioni nella scheda Elenco indirizzi privilegiati non possono sovrascrivere le impostazioni nella scheda Rete client non attendibile.

Passi

1. Nella scheda Elenco indirizzi privilegiati, immettere l'indirizzo o la subnet IP a cui si desidera concedere l'accesso alle porte chiuse.
2. Facoltativamente, seleziona **Aggiungi un altro indirizzo IP o subnet in notazione CIDR** per aggiungere altri client privilegiati.



Aggiungere il minor numero possibile di indirizzi all'elenco privilegiato.

3. Facoltativamente, seleziona ***Consenti agli indirizzi IP privilegiati di accedere alle porte interne**

StorageGRID *. Vedere ["Porte interne StorageGRID"](#) .



Questa opzione rimuove alcune protezioni per i servizi interni. Se possibile, lascialo disattivato.

4. Seleziona **Salva**.

Gestisci l'accesso esterno

Quando una porta viene chiusa nella scheda Gestisci accesso esterno, non è possibile accedervi da nessun indirizzo IP non in rete, a meno che non si aggiunga l'indirizzo IP all'elenco degli indirizzi privilegiati. Puoi chiudere solo le porte che sono aperte per impostazione predefinita e puoi aprire solo le porte che hai chiuso.



Le impostazioni nella scheda Gestisci accesso esterno non possono sostituire le impostazioni nella scheda 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 Gestisci accesso esterno. Le impostazioni nella scheda Rete client non attendibile sovrascrivono le porte chiuse (ad esempio 443, 8443, 9443) sulla rete client.

Passi

1. Seleziona **Gestisci accesso esterno**. La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non in griglia) per i nodi nella griglia.
2. Configura le porte che vuoi aprire e chiudere utilizzando le seguenti opzioni:
 - Utilizzare il pulsante accanto a ciascuna porta per aprire o chiudere la porta selezionata.
 - Selezionare **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 chiudi le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi su una porta bloccata, incluso te, 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 assicurarsi di aver visualizzato tutte le porte disponibili. Utilizzare il campo di ricerca per trovare le impostazioni per qualsiasi porta esterna inserendo un numero di porta. È possibile immettere un numero di porta parziale. Ad esempio, se si immette **2**, vengono visualizzate tutte le porte che contengono la stringa "2" nel loro nome.

3. Seleziona **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 bilanciatore del carico e, facoltativamente, sulle porte aggiuntive selezionate in questa scheda. È possibile utilizzare questa scheda anche per specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.



Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciatore del carico non sono stati configurati.

Le modifiche alla configurazione apportate nella scheda **Rete client non attendibile** sovrascrivono le impostazioni nella scheda **Gestisci accesso esterno**.

Passi

1. Selezionare **Rete client non attendibile**.
2. Nella sezione Imposta nuovo nodo predefinito, specificare quale deve essere l'impostazione predefinita quando vengono aggiunti nuovi nodi alla griglia in una procedura di espansione.
 - **Affidabile** (predefinito): quando un nodo viene aggiunto in un'espansione, la sua rete client è attendibile.
 - **Non attendibile**: quando un nodo viene aggiunto a un'espansione, la sua rete client non è attendibile.

Se necessario, è possibile tornare a questa scheda per modificare l'impostazione per 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 connessioni client solo su endpoint del bilanciatore del carico configurati in modo esplicito o porte aggiuntive selezionate:
 - Selezionare **Non considerare attendibili i nodi visualizzati** per aggiungere tutti i nodi visualizzati nella tabella all'elenco Reti client non attendibili.
 - Selezionare **Considera attendibili i nodi visualizzati** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Reti client non attendibili.
 - Utilizzare il pulsante di attivazione/disattivazione accanto a ciascun nodo per impostare la rete client come attendibile o non attendibile per il nodo selezionato.

Ad esempio, è possibile selezionare **Non considerare attendibili i nodi visualizzati** per aggiungere tutti i nodi all'elenco Reti client non attendibili e quindi utilizzare il pulsante di attivazione/disattivazione accanto a un singolo nodo per aggiungere quel singolo nodo all'elenco Reti client attendibili.



Utilizzare la barra di scorrimento sul lato destro della tabella per assicurarsi di aver visualizzato tutti i nodi disponibili. Utilizzare il campo di ricerca per trovare le impostazioni di qualsiasi nodo immettendone il nome. È possibile immettere un nome parziale. Ad esempio, se si immette **GW**, verranno visualizzati tutti i nodi che hanno la stringa "GW" come parte del loro nome.

4. Seleziona **Salva**.

Le nuove impostazioni del firewall vengono applicate e rese effettive immediatamente. Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciatore del carico non sono stati configurati.

Gestire gli inquilini

Cosa sono i conti degli inquilini?

Un account tenant consente di utilizzare l'API REST Simple Storage Service (S3) per archiviare e recuperare oggetti in un sistema StorageGRID .



I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere ["StorageGRID 11.8: Gestisci i tenant"](#).

In qualità di amministratore della griglia, crei e gestisci gli account tenant che i client S3 utilizzano per archiviare e recuperare gli oggetti.

Ogni account tenant ha gruppi, utenti, bucket S3 e oggetti federati o locali.

Gli account tenant possono essere utilizzati per separare gli oggetti archiviati da entità diverse. Ad esempio, è possibile utilizzare più account tenant per uno qualsiasi di questi casi d'uso:

- **Caso d'uso aziendale:** se si amministra un sistema StorageGRID in un'applicazione aziendale, potrebbe essere opportuno separare l'archiviazione degli oggetti della griglia in base ai diversi reparti dell'organizzazione. In questo caso, potresti 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 bucket S3 e policy di bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario utilizzare account tenant. Vedi le istruzioni per l'implementazione ["Bucket S3 e policy dei bucket"](#) per maggiori informazioni.

- **Caso d'uso del fornitore di servizi:** se si amministra un sistema StorageGRID come fornitore di servizi, è possibile separare l'archiviazione degli oggetti della griglia in base alle diverse entità che prenderanno in leasing l'archiviazione sulla griglia. In questo caso, dovresti creare account tenant per la Società A, la Società B, la Società C e così via.

Per ulteriori informazioni, consultare ["Utilizzare un account tenant"](#).

Come posso creare un account tenant?

Utilizzare Grid Manager per creare 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) e la quota di archiviazione facoltativa.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine identità, utilizzare S3 Select o utilizzare una connessione di federazione di griglia.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione delle identità o Single Sign-On (SSO).

Inoltre, è possibile abilitare l'impostazione S3 Object Lock per il sistema StorageGRID se gli account tenant S3 devono essere conformi ai requisiti normativi. Quando S3 Object Lock è abilitato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

A cosa serve Tenant Manager?

Dopo aver creato l'account tenant, gli utenti tenant possono accedere a Tenant Manager per eseguire attività come le seguenti:

- Impostare la federazione delle identità (a meno che l'origine dell'identità non sia condivisa con la griglia)
- Gestisci gruppi e utenti
- Utilizzare la federazione di griglia per la clonazione degli account e la replica tra griglie

- Gestisci le chiavi di accesso S3
- Crea e gestisci bucket S3
- Utilizzare i servizi della piattaforma S3
- Utilizzare S3 Select
- Monitorare l'utilizzo dello spazio di archiviazione



Mentre gli utenti tenant S3 possono creare e gestire bucket e chiavi di accesso S3 con Tenant Manager, devono utilizzare un'applicazione client S3 per acquisire e gestire gli oggetti. Vedere ["Utilizzare l'API REST S3"](#) per i dettagli.

Crea un account inquilino

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 a seconda che ["federazione di identità"](#) E ["accesso unico"](#) sono configurati e se l'account Grid Manager utilizzato per creare l'account tenant appartiene a un gruppo di amministratori con autorizzazione di accesso Root.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Accesso root o autorizzazione account tenant"](#) .
- Se l'account tenant utilizzerà l'origine identità configurata per Grid Manager e si desidera concedere l'autorizzazione di accesso Root per l'account tenant a un gruppo federato, è stato importato tale gruppo federato in Grid Manager. Non è necessario assegnare alcuna autorizzazione Grid Manager a questo gruppo di amministratori. Vedere ["Gestisci gruppi di amministratori"](#) .
- Se si desidera consentire a un tenant S3 di clonare i dati dell'account e replicare gli oggetti bucket su un'altra griglia utilizzando una connessione di federazione della griglia:
 - Hai ["configurato la connessione della federazione di griglia"](#) .
 - Lo stato della connessione è **Connesso**.
 - Hai i permessi di accesso Root.
 - Hai esaminato le considerazioni per ["gestione degli inquilini autorizzati per la federazione della rete"](#) .
 - Se l'account tenant utilizzerà l'origine identità configurata per Grid Manager, significa che hai importato lo stesso gruppo federato in Grid Manager su entrambe le griglie.

Quando si crea il tenant, si selezionerà questo gruppo per avere l'autorizzazione di accesso Root iniziale sia per l'account tenant di origine che per quello di destinazione.



Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non verrà replicato nella destinazione.

Accedi alla procedura guidata

Passi

1. Selezionare **INQUILINI**.

2. Seleziona **Crea**.

Inserisci i dettagli

Passi

1. Inserisci i dettagli dell'inquilino.

Campo	Descrizione
Nome	Un nome per l'account dell'inquilino. I nomi degli inquilini non devono essere univoci. Quando viene creato l'account tenant, questo riceve un ID account univoco di 20 cifre.
Descrizione (facoltativa)	Una descrizione che aiuti a identificare l'inquilino. Se si sta creando un tenant che utilizzerà una connessione di federazione di griglia, è possibile utilizzare questo campo per identificare il tenant di origine e quello di destinazione. Ad esempio, questa descrizione per un tenant creato sulla Griglia 1 apparirà anche per il tenant replicato sulla Griglia 2: "Questo tenant è stato creato sulla Griglia 1".
Tipo di cliente	Il tipo di protocollo client che questo tenant utilizzerà, S3 o Swift . Nota: il supporto per le applicazioni client Swift è stato deprecato e verrà rimosso in una versione futura.
Quota di archiviazione (facoltativa)	Se si desidera che questo tenant disponga di una quota di archiviazione, specificare un valore numerico per la quota e le unità.

2. Selezionare **Continua**.

Seleziona autorizzazioni

Passi

1. Facoltativamente, seleziona le autorizzazioni di base che desideri assegnare a questo tenant.



Alcune di queste autorizzazioni prevedono requisiti aggiuntivi. Per maggiori dettagli, seleziona l'icona della guida per ogni autorizzazione.

Permesso	Se selezionato...
Consenti i servizi della piattaforma	Il tenant può utilizzare i servizi della piattaforma S3 come CloudMirror. Vedere "Gestire i servizi della piattaforma per gli account tenant S3" .
Utilizzare la propria fonte di identità	Il tenant può configurare e gestire la propria fonte di identità per gruppi e utenti federati. Questa opzione è disabilitata se hai "SSO configurato" per il tuo sistema StorageGRID.

Permesso	Se selezionato...
Consenti selezione S3	Il tenant può inviare richieste API S3 SelectObjectContent per filtrare e recuperare i dati degli oggetti. Vedere "Gestisci S3 Select per gli account tenant" . Importante: le richieste SelectObjectContent possono ridurre le prestazioni del bilanciamento del carico per tutti i client S3 e tutti i tenant. Abilitare questa funzionalità solo quando necessario e solo per i tenant attendibili.

2. Facoltativamente, seleziona le autorizzazioni avanzate che desideri assegnare a questo tenant.

Permesso	Se selezionato...
Collegamento della federazione di rete	L'inquilino può utilizzare una connessione di federazione di rete, che: • Fa sì che questo tenant e tutti i gruppi e gli utenti tenant aggiunti all'account vengano clonati da questa griglia (la <i>griglia di origine</i>) all'altra griglia nella connessione selezionata (la <i>griglia di destinazione</i>). • Consente a questo tenant di configurare la replica tra griglie tra i bucket corrispondenti su ciascuna griglia. Vedere "Gestire gli inquilini autorizzati per la federazione della rete" .
Blocco oggetto S3	Consentire al tenant di utilizzare funzionalità specifiche di S3 Object Lock: • Imposta periodo massimo di conservazione definisce per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. • Consenti modalità di conformità impedisce agli utenti di sovrascrivere o eliminare versioni di oggetti protetti durante il periodo di conservazione.

3. Selezionare **Continua**.

Definisci l'accesso root e crea il tenant

Passi

1. Definisci l'accesso root per l'account tenant, a seconda che il tuo sistema StorageGRID utilizzi la federazione delle identità, il Single Sign-On (SSO) o entrambi.

Opzione	Fai questo
Se la federazione delle identità non è abilitata	Specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se la federazione delle identità è abilitata	a. Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si accede al tenant come utente root locale.

Opzione	Fai questo
Se sono abilitati sia la federazione delle identità che il Single Sign-On (SSO)	Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. Nessun utente locale può effettuare l'accesso.

2. Selezionare **Crea tenant**.

Viene visualizzato un messaggio di conferma e il nuovo inquilino viene elencato nella pagina Inquilini. Per informazioni su come visualizzare i dettagli degli inquilini e monitorarne l'attività, vedere ["Monitorare l'attività degli inquilini"](#).



L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato del nodo e delle operazioni di Cassandra.

3. Se hai selezionato l'autorizzazione **Usa connessione federata alla griglia** per il tenant:

- Verificare che un tenant identico sia stato replicato sull'altra griglia nella connessione. Gli inquilini su entrambe le griglie avranno lo stesso ID account di 20 cifre, nome, descrizione, quota e autorizzazioni.



Se viene visualizzato il messaggio di errore "Tenant creato senza un clone", fare riferimento alle istruzioni in ["Risolvere gli errori di federazione della griglia"](#).

- Se hai fornito una password utente root locale quando hai definito l'accesso root, ["cambiare la password per l'utente root locale"](#) per l'inquilino replicato.



Un utente root locale non può accedere a Tenant Manager sulla griglia di destinazione finché non viene modificata la password.

Sign in al tenant (facoltativo)

Se necessario, puoi accedere subito al nuovo tenant per completare la configurazione oppure puoi accedere al tenant in un secondo momento. I passaggi per l'accesso variano a seconda che tu abbia effettuato l'accesso a Grid Manager tramite la porta predefinita (443) o una porta con restrizioni. Vedere ["Controllare l'accesso al firewall esterno"](#).

Sign in ora

Se stai utilizzando...	Fai questo...
Porta 443 e si imposta una password per l'utente root locale	- Seleziona * Sign in come root*. Quando effettui l'accesso, vengono visualizzati i link per configurare bucket, federazione delle identità, gruppi e utenti. - Selezionare i link per configurare l'account tenant. Ogni collegamento apre la pagina corrispondente in Tenant Manager. Per completare la pagina, vedere il "istruzioni per l'utilizzo degli account degli inquilini".

Se stai utilizzando...	Fai questo...
Porta 443 e non hai impostato una password per l'utente root locale	Selezionare * Sign in* e immettere le credenziali di un utente nel gruppo federato con accesso root.
Un porto limitato	1. Seleziona Fine 2. Selezionare Limitato nella tabella Tenant per saperne di più sull'accesso a questo account tenant. L'URL per Tenant Manager ha questo formato: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ◦ `FQDN_or_Admin_Node_IP` è un nome di dominio completamente qualificato o l'indirizzo IP di un nodo di amministrazione ◦ `port` è la porta riservata al tenant ◦ `20-digit-account-id` è l'ID account univoco del tenant

Sign in più tardi

Se stai utilizzando...	Fai una di queste cose...
Porta 443	• Da Grid Manager, seleziona TENANT e seleziona * Sign in* a destra del nome del tenant. • Inserisci l'URL del tenant in un browser web: <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ◦ `FQDN_or_Admin_Node_IP` è un nome di dominio completamente qualificato o l'indirizzo IP di un nodo di amministrazione ◦ `20-digit-account-id` è l'ID account univoco del tenant
Un porto limitato	• Da Grid Manager, seleziona TENANTS e seleziona Restricted. • Inserisci l'URL del tenant in un browser web: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ `FQDN_or_Admin_Node_IP` è un nome di dominio completamente qualificato o l'indirizzo IP di un nodo di amministrazione ◦ `port` è la porta riservata solo al tenant ◦ `20-digit-account-id` è l'ID account univoco del tenant

Configurare il tenant

Seguire le istruzioni in ["Utilizzare un account tenant"](#) per gestire gruppi di tenant e utenti, chiavi di accesso S3, bucket, servizi di piattaforma, clonazione di account e replica tra griglie.

Modifica account inquilino

È possibile modificare un account tenant per cambiare il nome visualizzato, la quota di archiviazione o le autorizzazioni del tenant.



Se un tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile modificare i dettagli del tenant da entrambe le griglie nella connessione. Tuttavia, tutte le modifiche apportate a una griglia nella connessione non verranno copiate nell'altra griglia. Se si desidera che i dettagli degli inquilini siano perfettamente sincronizzati tra le griglie, apportare le stesse modifiche su entrambe le griglie. Vedere ["Gestire gli inquilini autorizzati per la connessione alla federazione di rete"](#).

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Accesso root o autorizzazione account tenant"](#).



L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato del nodo e delle operazioni di Cassandra.

Passi

1. Selezionare **INQUILINI**.

Tenants							
View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.							
Create	Export to CSV	Actions ▾	Search tenants by name or ID		Displaying 5 results		
☐	Name ?	Logical space used ?	Quota utilization ?	Quota ?	Object count ?	Sign in/Copy URL ?	
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄	
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄	
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄	
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄	
☐	Tenant 05	5.00 GB	—	—	500	→ 📄	

2. Individua l'account tenant che desideri modificare.

Utilizzare la casella di ricerca per cercare un inquilino per nome o ID inquilino.

3. Selezionare l'inquilino. Puoi procedere in uno dei seguenti modi:

- Selezionare la casella di controllo per il tenant e selezionare **Azioni > Modifica**.
 - Selezionare il nome del tenant per visualizzare la pagina dei dettagli e selezionare **Modifica**.
4. Facoltativamente, modifica i valori per questi campi:
- **Nome**
 - **Descrizione**
 - **Quota di archiviazione**
5. Selezionare **Continua**.
6. Selezionare o deselezionare le autorizzazioni per l'account tenant.
- Se disabiliti i **Servizi di piattaforma** per un tenant che li sta già utilizzando, i servizi che ha configurato per i suoi 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 archiviare oggetti nel bucket, ma le copie di tali oggetti non verranno più create nel bucket S3 esterno che ha configurato come endpoint. Vedere ["Gestire i servizi della piattaforma per gli account tenant S3"](#).
 - Modificare l'impostazione **Usa la propria origine identità** per determinare se l'account tenant utilizzerà la propria origine identità o l'origine identità configurata per Grid Manager.

Se **Utilizza la propria fonte di identità** è:

- Disabilitato e selezionato, il tenant ha già abilitato la propria fonte di identità. Un tenant deve disabilitare la propria origine identità prima di poter utilizzare l'origine identità configurata per Grid Manager.
 - Disabilitato e non selezionato, SSO è abilitato per il sistema StorageGRID . Il tenant deve utilizzare l'origine identità configurata per Grid Manager.
- Selezionare o deselezionare l'autorizzazione **Consenti selezione S3** in base alle esigenze. Vedere ["Gestisci S3 Select per gli account tenant"](#) .
 - Per rimuovere l'autorizzazione **Usa connessione federazione griglia**:
 - i. Selezionare la scheda **Federazione di griglia**.
 - ii. Seleziona **Rimuovi autorizzazione**.
 - Per aggiungere l'autorizzazione **Usa connessione federata griglia**:
 - i. Selezionare la scheda **Federazione di griglia**.
 - ii. Selezionare la casella di controllo **Usa connessione federata alla griglia**.
 - iii. Facoltativamente, seleziona **Clona utenti e gruppi locali esistenti** per clonarli nella griglia remota. Se lo desideri, puoi interrompere la clonazione in corso o riprovare se alcuni utenti o gruppi locali non sono riusciti a essere clonati dopo il completamento dell'ultima operazione di clonazione.
 - Per impostare un periodo di conservazione massimo o consentire la modalità di conformità:



Prima di poter utilizzare queste impostazioni, è necessario abilitare il blocco oggetti S3 sulla griglia.

- i. Selezionare la scheda **Blocco oggetto S3**.
- ii. Per **Imposta periodo massimo di conservazione**, immettere un valore e selezionare il periodo di tempo dal menu a discesa.
- iii. Per **Consenti modalità conformità**, seleziona la casella di controllo.

Cambia 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 fuori dall'account.

Prima di iniziare

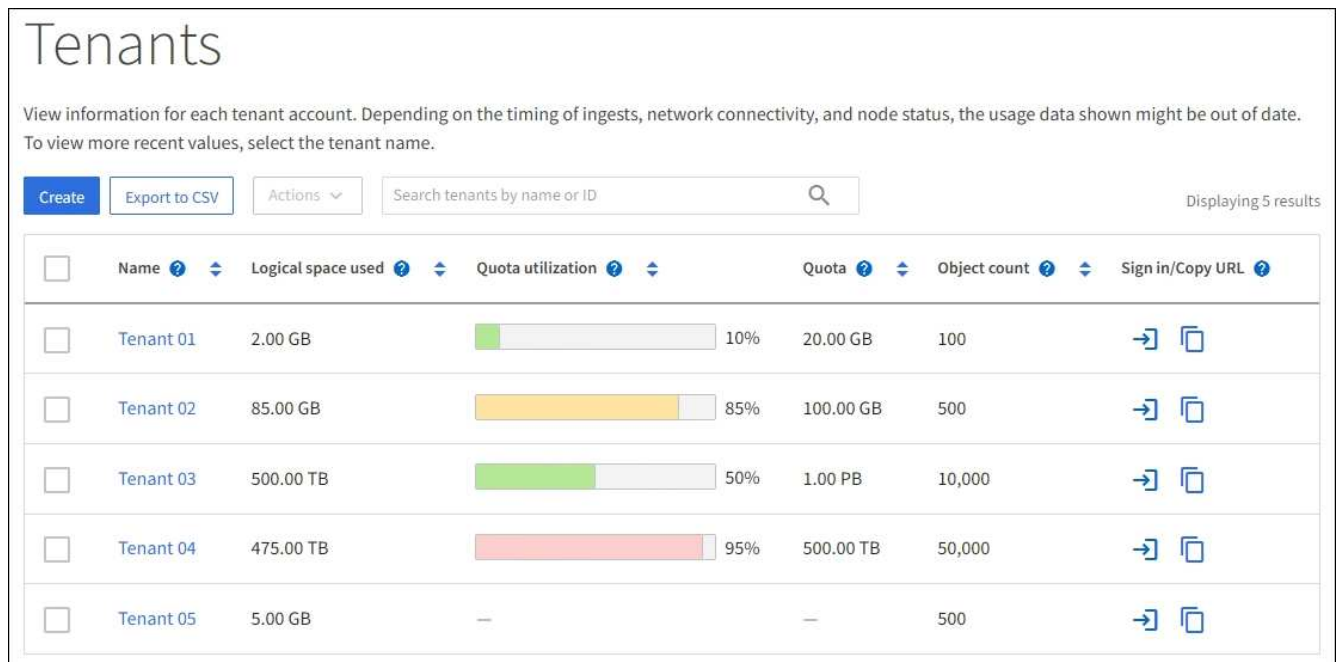
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Informazioni su questo compito

Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), l'utente root locale non può accedere all'account tenant. Per eseguire attività come utente root, gli utenti devono appartenere a un gruppo federato che dispone dell'autorizzazione di accesso root per il tenant.

Passi

1. Selezionare **INQUILINI**.



☐	Name ?	Logical space used ?	Quota utilization ?	Quota ?	Object count ?	Sign in/Copy URL ?
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Selezionare l'account dell'inquilino. Puoi procedere in uno dei seguenti modi:
 - Selezionare la casella di controllo per il tenant e selezionare **Azioni > Cambia password di root**.
 - Selezionare il nome del tenant per visualizzare la pagina dei dettagli e selezionare **Azioni > Modifica password root**.
3. Inserisci la nuova password per l'account tenant.
4. Seleziona **Salva**.

Elimina account inquilino

È possibile eliminare un account tenant se si desidera rimuovere definitivamente l'accesso del tenant al sistema.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Sono stati rimossi tutti i bucket e gli oggetti S3 associati all'account tenant.
- Se all'inquilino è consentito utilizzare una connessione di federazione di rete, hai esaminato le considerazioni per ["eliminazione di un tenant con l'autorizzazione Usa connessione federazione griglia"](#) .

Passi

1. Selezionare **INQUILINI**.
2. Individua l'account o gli account tenant che desideri eliminare.

Utilizzare la casella di ricerca per cercare un inquilino per nome o ID inquilino.
3. Per eliminare più tenant, seleziona le caselle di controllo e seleziona **Azioni > Elimina**.
4. Per eliminare un singolo tenant, procedere in uno dei seguenti modi:
 - 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

Cosa sono i servizi di piattaforma?

I servizi della piattaforma includono la replica CloudMirror, le notifiche degli eventi e il servizio di integrazione della ricerca.

Se si abilitano i servizi della piattaforma per gli account tenant S3, è necessario configurare la griglia in modo che i tenant possano accedere alle risorse esterne necessarie per utilizzare questi servizi.

Replica CloudMirror

Il servizio di replica StorageGRID CloudMirror viene utilizzato per eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.

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



La replica di CloudMirror presenta alcune importanti somiglianze e differenze con la funzionalità di replica tra griglie. Per saperne di più, vedere ["Confronta la replicazione cross-grid e la replicazione CloudMirror"](#) .



La replica CloudMirror non è supportata se nel bucket di origine è abilitato S3 Object Lock.

Notifiche

Le notifiche degli eventi per bucket vengono utilizzate per inviare notifiche su azioni specifiche eseguite sugli oggetti a un cluster Kafka esterno specificato o ad Amazon Simple Notification Service.

Ad esempio, è possibile configurare l'invio di avvisi agli amministratori per ogni oggetto aggiunto a un bucket,

dove gli oggetti rappresentano file di registro associati a un evento di sistema critico.



Sebbene la notifica degli eventi possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Conserva 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 metadati di oggetti S3 a un indice Elasticsearch specificato, dove è possibile ricercare o analizzare i metadati utilizzando il servizio esterno.

Ad esempio, puoi configurare i tuoi bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. Potresti quindi utilizzare Elasticsearch per effettuare ricerche tra i bucket e realizzare analisi sofisticate dei modelli presenti nei metadati degli oggetti.



Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Retain Until Date e Legal Hold) degli oggetti non saranno inclusi nei messaggi di notifica.

I servizi della piattaforma offrono agli inquilini la possibilità di utilizzare risorse di archiviazione esterne, servizi di notifica e servizi di ricerca o analisi con i propri dati. Poiché la posizione di destinazione per i servizi della piattaforma è in genere esterna alla distribuzione StorageGRID, è necessario decidere se si desidera consentire ai tenant di utilizzare questi servizi. In tal caso, è necessario abilitare l'utilizzo dei servizi della piattaforma quando si creano o si 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 loro destinazioni.

Raccomandazioni per l'utilizzo dei servizi della piattaforma

Prima di utilizzare i servizi della piattaforma, tieni presente i seguenti consigli:

- Se in un bucket S3 del sistema StorageGRID sono abilitati sia il controllo delle versioni sia la replica CloudMirror, è necessario abilitare anche il controllo delle versioni del bucket S3 per l'endpoint di destinazione. Ciò consente alla replica CloudMirror di generare versioni di oggetti simili sull'endpoint.
- Non dovresti utilizzare più di 100 tenant attivi con richieste S3 che richiedono la replica, le notifiche e l'integrazione della ricerca di CloudMirror. Avere più di 100 tenant attivi può comportare prestazioni più lente del client S3.
- Le richieste a un endpoint che non possono essere completate verranno messe in coda fino a un massimo di 500.000 richieste. Questo limite è equamente ripartito tra gli inquilini attivi. Ai nuovi inquilini è consentito superare temporaneamente questo limite di 500.000 unità, in modo che i nuovi inquilini non vengano ingiustamente penalizzati.

Informazioni correlate

- ["Gestire i servizi della piattaforma"](#)
- ["Configurare le impostazioni del proxy di archiviazione"](#)
- ["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 abilitati, il tenant può creare endpoint che fungono da destinazione per la replica di CloudMirror, le notifiche degli eventi o i messaggi di integrazione della ricerca dai suoi bucket S3. Questi messaggi dei servizi di piattaforma vengono inviati dai nodi di archiviazione che eseguono il servizio ADC agli endpoint di destinazione.

Ad esempio, i tenant potrebbero configurare i seguenti tipi di endpoint di destinazione:

- Un 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 recapitati, è necessario configurare la rete o le reti contenenti i nodi di archiviazione ADC. È necessario assicurarsi che le seguenti porte possano essere utilizzate per inviare messaggi di servizi di piattaforma agli endpoint di destinazione.

Per impostazione predefinita, i messaggi dei servizi della piattaforma vengono inviati sulle seguenti porte:

- **80**: Per gli URI degli endpoint che iniziano con http (la maggior parte degli endpoint)
- **443**: Per gli URI degli endpoint che iniziano con https (la maggior parte degli endpoint)
- **9092**: Per gli URI degli endpoint che iniziano con http o https (solo endpoint Kafka)

Gli inquilini possono specificare una porta diversa quando creano o modificano un endpoint.



Se si utilizza una distribuzione StorageGRID come destinazione per la 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 dalla distribuzione StorageGRID di destinazione sia specificata nell'endpoint.

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

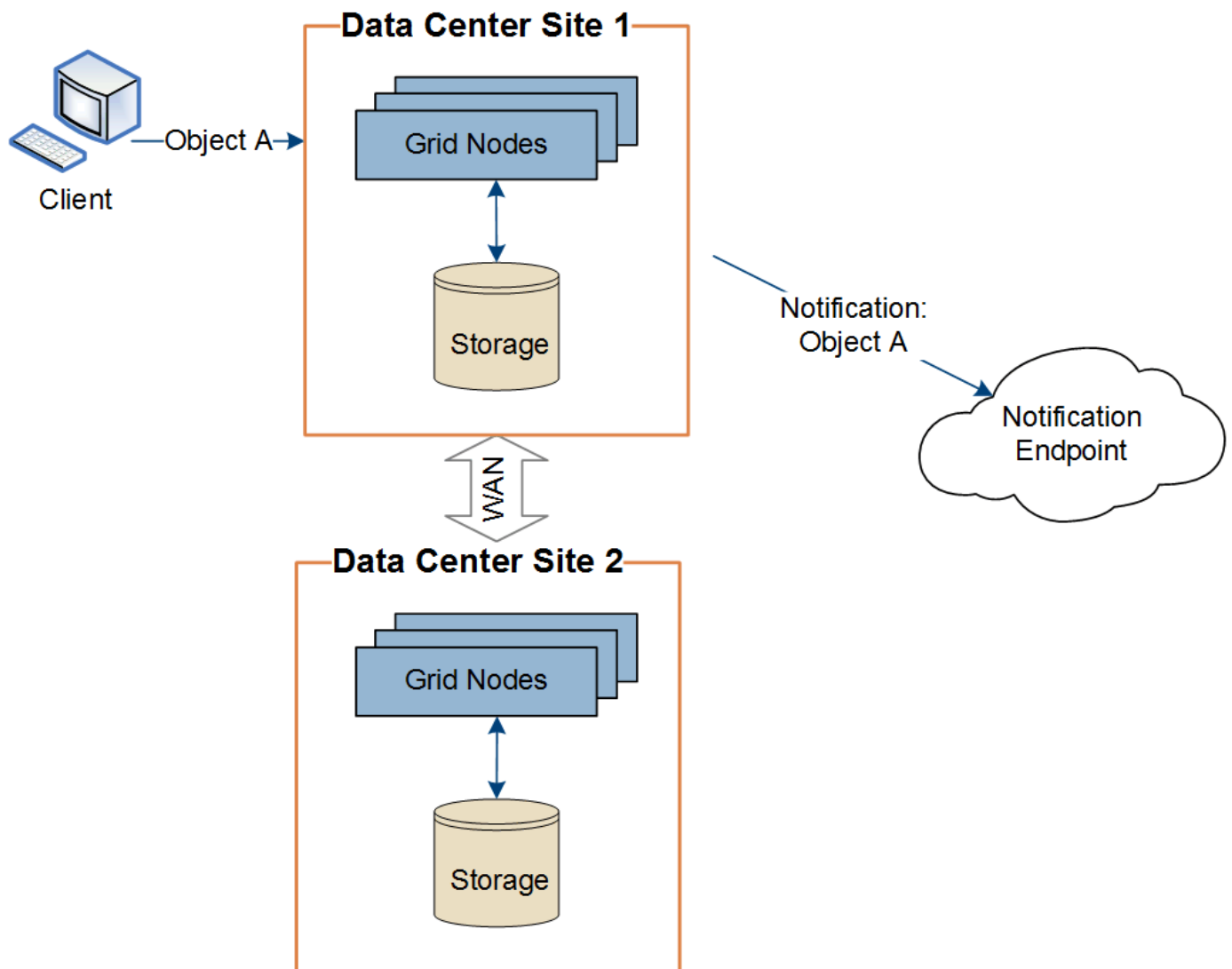
Informazioni correlate

["Utilizzare un account tenant"](#)

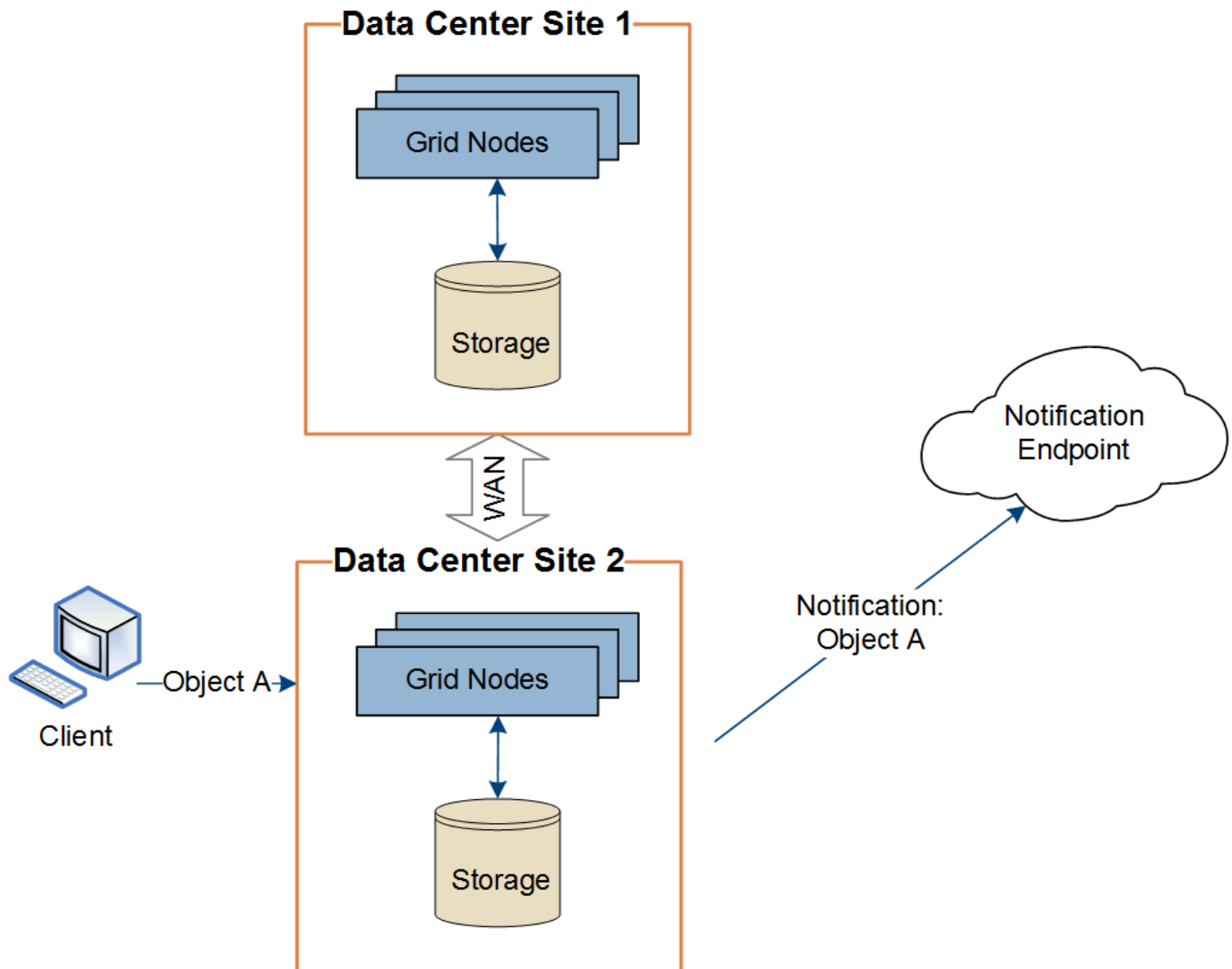
Consegna per sito di messaggi di servizi di piattaforma

Tutte le operazioni dei servizi della piattaforma vengono eseguite per ogni sito.

Ciò significa che se un tenant utilizza un client per eseguire un'operazione di creazione API S3 su un oggetto connettendosi a un nodo gateway nel sito del data center 1, la notifica relativa a tale azione viene attivata e inviata dal sito del data center 1.



Se successivamente il client esegue un'operazione di eliminazione dell'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 in ogni sito sia configurata in modo tale che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

Risolvere i problemi dei servizi della piattaforma

Gli endpoint utilizzati nei servizi della piattaforma vengono creati e gestiti dagli utenti tenant in Tenant Manager; tuttavia, se un tenant riscontra problemi nella configurazione o nell'utilizzo dei servizi della piattaforma, è 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 Tenant Manager. Ogni endpoint rappresenta una destinazione esterna per un servizio di piattaforma, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento Amazon Simple Notification Service, un argomento Kafka o un cluster Elasticsearch ospitato localmente o su AWS. Ogni endpoint include sia la posizione della risorsa esterna sia le credenziali necessarie per accedere a tale risorsa.

Quando un tenant crea un endpoint, il sistema StorageGRID verifica che l'endpoint esista e che possa essere raggiunto utilizzando le credenziali specificate. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Se la convalida dell'endpoint fallisce, un messaggio di errore ne spiega il motivo. L'utente tenant dovrebbe risolvere il problema, quindi provare a creare nuovamente l'endpoint.



La creazione dell'endpoint non riuscirà 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 nella dashboard di Tenant Manager.



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 tenant possono andare alla pagina 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 da quanto tempo si è verificato l'errore. Errori che includono il  l'icona si è verificata negli ultimi 7 giorni.

Platform services endpoints

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



One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

Create endpoint

Delete endpoint

☐	Display name  	Last error  	Type  	URI  	URN  
☐	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
☐	my-endpoint-3	 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



Alcuni messaggi di errore nella colonna **Ultimo errore** potrebbero includere un logID tra parentesi. Un amministratore di rete o il supporto tecnico possono utilizzare questo ID per individuare informazioni più dettagliate sull'errore nel file bycast.log.

Problemi relativi ai server proxy

Se hai configurato un "[proxy di archiviazione](#)" tra i nodi di archiviazione e gli endpoint del servizio di piattaforma, potrebbero verificarsi errori se il servizio proxy non consente messaggi da StorageGRID. Per risolvere questi problemi, controlla le impostazioni del tuo server proxy per assicurarti che i messaggi relativi ai servizi della piattaforma non siano bloccati.

Determina se si è verificato un errore

Se si sono verificati errori dell'endpoint negli ultimi 7 giorni, la dashboard in Tenant Manager visualizza un messaggio di avviso. Puoi andare alla pagina Endpoint per vedere maggiori dettagli sull'errore.

Le operazioni del client falliscono

Alcuni problemi relativi ai servizi della piattaforma potrebbero causare il fallimento delle operazioni client sul bucket S3. Ad esempio, le operazioni del client S3 non riusciranno se il servizio RSM (Replicated State Machine) interno si arresta o se sono presenti troppi messaggi dei servizi della piattaforma in coda per la consegna.

Per verificare lo stato dei servizi:

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **sito > Nodo di archiviazione > SSM > Servizi**.

Errori di endpoint recuperabili e irrecuperabili

Dopo la creazione degli endpoint, possono verificarsi errori nella richiesta del servizio di piattaforma per vari motivi. Alcuni errori sono recuperabili con l'intervento dell'utente. Ad esempio, gli errori recuperabili potrebbero verificarsi per i seguenti motivi:

- Le credenziali dell'utente sono state eliminate o sono scadute.
- Il bucket di destinazione non esiste.
- La notifica non può essere recapitata.

Se StorageGRID riscontra un errore recuperabile, la richiesta del servizio di piattaforma verrà ripetuta finché non avrà esito positivo.

Altri errori non sono recuperabili. Ad esempio, se l'endpoint viene eliminato, si verifica un errore irrecuperabile.

Se StorageGRID riscontra un errore di endpoint irreversibile:

- In Grid Manager, vai su **Supporto > Strumenti > Metriche > Grafana > Panoramica dei servizi della piattaforma** per visualizzare i dettagli dell'errore.
- In Tenant Manager, vai su **STORAGE (S3) > Platform Services Endpoints** per visualizzare i dettagli dell'errore.
- Controlla il `/var/local/log/bycast-err.log` per errori correlati. I nodi di archiviazione dotati del servizio ADC contengono questo file di registro.

I messaggi dei servizi della piattaforma non possono essere recapitati

Se la destinazione riscontra un problema che le impedisce di accettare i 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

tale che StorageGRID non possa più autenticarsi al servizio di destinazione.

Controlla gli avvisi correlati.

Prestazioni più lente per le richieste di servizi della piattaforma

Il software StorageGRID potrebbe limitare le richieste S3 in arrivo per un bucket se la velocità con cui vengono inviate le richieste supera la velocità con cui l'endpoint di destinazione può riceverle. La limitazione si verifica solo quando è presente un arretrato di richieste in attesa di essere inviate all'endpoint di destinazione.

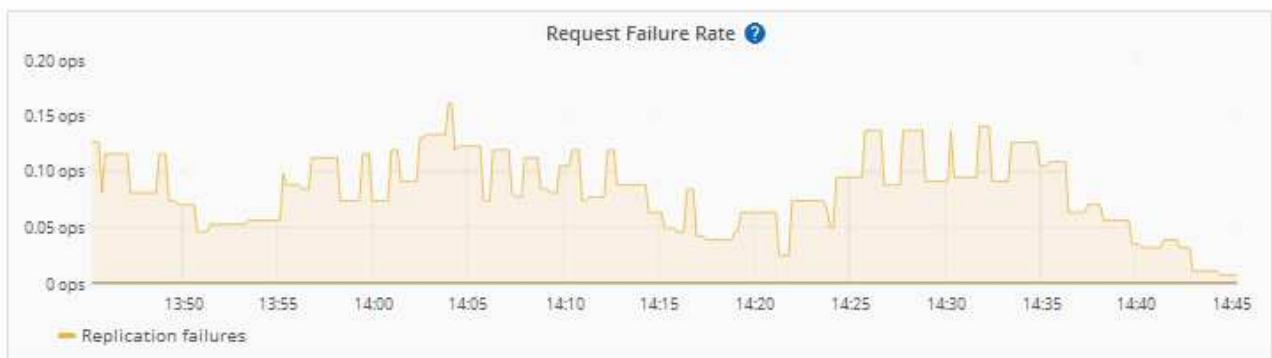
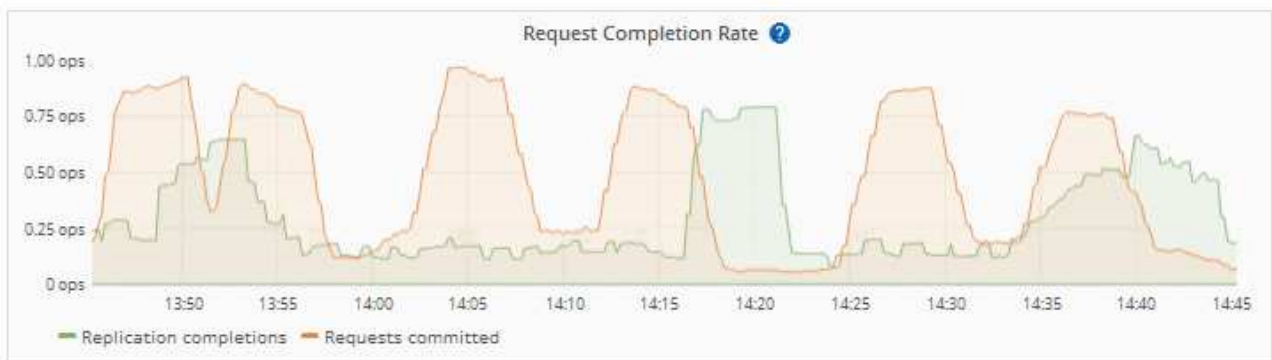
L'unico effetto visibile è che le richieste S3 in arrivo impiegheranno più tempo per essere eseguite. Se si inizia a rilevare un rallentamento significativo delle prestazioni, è opportuno ridurre la velocità di acquisizione o utilizzare un endpoint con capacità maggiore. Se l'arretrato di richieste continua ad aumentare, le operazioni S3 del client (come le richieste PUT) alla fine falliranno.

Le richieste CloudMirror hanno maggiori probabilità di essere influenzate dalle prestazioni dell'endpoint di destinazione, perché in genere comportano un trasferimento di dati maggiore rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Le richieste di servizio della piattaforma falliscono

Per visualizzare il tasso di errore delle richieste per i servizi della piattaforma:

1. Selezionare **NODES**.
2. Seleziona **site > Servizi piattaforma**.
3. Visualizza il grafico del tasso di errore delle richieste.



Avviso di servizi di piattaforma non disponibili

L'avviso **Servizi di piattaforma non disponibili** indica che non è possibile eseguire alcuna operazione di servizio di piattaforma in un sito perché sono in esecuzione o disponibili troppi pochi nodi di archiviazione 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 archiviazione nel sito includono il servizio RSM. (Il servizio RSM è presente sui nodi di archiviazione che includono anche il servizio ADC.) Quindi, assicurarsi che la maggioranza semplice di tali nodi di archiviazione sia in esecuzione e disponibile.



Se più di un nodo di archiviazione contenente il servizio RSM si guasta in un sito, si perdono tutte le richieste di servizio della piattaforma in sospeso per quel sito.

Ulteriori indicazioni per la risoluzione dei problemi per gli endpoint dei servizi della piattaforma

Per ulteriori informazioni vedere [Utilizzare un account tenant](#) › [Risoluzione dei problemi degli endpoint dei servizi della piattaforma](#).

Informazioni correlate

["Risoluzione dei problemi del sistema StorageGRID"](#)

Gestisci S3 Select per gli account tenant

È possibile consentire a determinati tenant S3 di utilizzare S3 Select per inviare richieste `SelectObjectContent` su singoli oggetti.

S3 Select offre un modo efficiente per effettuare ricerche in grandi quantità di dati senza dover implementare un database e le risorse associate per abilitare le ricerche. Riduce inoltre 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 di S3 Select.

Considerazioni e requisiti per l'utilizzo di S3 Select

Requisiti di amministrazione della rete

L'amministratore della rete deve concedere ai tenant la capacità S3 Select. Seleziona **Consenti selezione S3** quando ["creazione di un inquilino"](#) o ["modifica di un inquilino"](#).

Requisiti del formato dell'oggetto

L'oggetto che si desidera interrogare 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 Parquet:
 - S3 Select supporta solo la compressione colonnare tramite GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti Parquet.
 - S3 Select non supporta l'output Parquet. È necessario specificare il formato di output come CSV o JSON.
 - La dimensione massima del gruppo di righe non compresso è 512 MB.
 - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
 - Non è possibile utilizzare i tipi logici INTERVAL, JSON, LIST, TIME o UUID.

Requisiti dell'endpoint

La richiesta `SelectObjectContent` deve essere inviata a un ["Endpoint del bilanciamento del carico StorageGRID"](#).

I nodi Admin e Gateway utilizzati dall'endpoint devono essere uno dei seguenti:

- Un nodo di appliance di servizi
- Un nodo software basato su VMware
- Un nodo bare metal che esegue un kernel con cgroup v2 abilitato

Considerazioni generali

Le query non possono essere inviate direttamente ai nodi di archiviazione.



Le richieste SelectObjectContent possono ridurre le prestazioni del bilanciatore del carico per tutti i client S3 e tutti i tenant. Abilitare questa funzionalità solo quando necessario e solo per i tenant attendibili.

Vedi il ["istruzioni per l'uso di S3 Select"](#).

Per visualizzare ["Grafici Grafana"](#) per le operazioni di selezione S3 nel tempo, selezionare **SUPPORTO > Strumenti > Metriche** in Grid Manager.

Configurare le connessioni client

Configurare le connessioni client S3

In qualità di amministratore della griglia, gestisci le opzioni di configurazione che controllano il modo in cui le applicazioni client S3 si connettono al tuo sistema StorageGRID per archiviare e recuperare i dati.



I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere ["StorageGRID 11.8: configurazione delle connessioni client S3 e Swift"](#).

Attività di configurazione

1. Eseguire le attività prerequisite in StorageGRID, in base al modo in cui l'applicazione client si conatterà a StorageGRID.

Compiti richiesti

È necessario ottenere:

- indirizzi IP
- Nomi di dominio
- Certificato SSL

Attività facoltative

Facoltativamente, configurare:

- Federazione delle identità
- SSO

1. Utilizzare StorageGRID per ottenere i valori di cui l'applicazione ha bisogno per connettersi alla griglia. È possibile utilizzare la procedura guidata di configurazione di S3 oppure configurare manualmente ciascuna entità StorageGRID . +

Utilizzare la procedura guidata di configurazione S3

Seguire i passaggi della procedura guidata di configurazione S3.

Configurare manualmente

1. Crea un gruppo ad alta disponibilità
2. Crea endpoint del bilanciatore del carico
3. Crea un account inquilino
4. Crea bucket e chiavi di accesso
5. Configurare la regola e la politica ILM

1. Utilizzare l'applicazione S3 per completare la connessione a StorageGRID. Crea voci DNS per associare gli indirizzi IP a tutti i nomi di dominio che intendi utilizzare.

Se necessario, eseguire ulteriori configurazioni dell'applicazione.

2. Eseguire attività continue nell'applicazione e in StorageGRID per gestire e monitorare l'archiviazione degli oggetti nel tempo.

Informazioni necessarie per collegare StorageGRID a un'applicazione client

Prima di poter collegare StorageGRID a un'applicazione client S3, è necessario eseguire i passaggi di configurazione in StorageGRID e ottenere un determinato valore.

Di quali valori ho bisogno?

Nella tabella seguente vengono mostrati i valori che è necessario configurare in StorageGRID e dove tali valori vengono utilizzati dall'applicazione S3 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 bilanciatore del carico	Applicazione client
Certificato SSL	StorageGRID > Endpoint del bilanciatore del carico	Applicazione client
Nome del server (FQDN)	StorageGRID > Endpoint del bilanciatore del carico	• Applicazione client • voce DNS
ID chiave di accesso S3 e chiave di accesso segreta	StorageGRID > Tenant e bucket	Applicazione client

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Nome del bucket/contenitore	StorageGRID > Tenant e bucket	Applicazione client

Come posso ottenere questi valori?

A seconda delle tue esigenze, puoi procedere in uno dei seguenti modi per ottenere le informazioni di cui hai bisogno:

- *Usa il "[Procedura guidata di configurazione S3](#)" *. La procedura guidata di configurazione di S3 consente di configurare rapidamente i valori richiesti in StorageGRID e genera uno o due file che è possibile utilizzare durante la configurazione dell'applicazione S3. La procedura guidata ti guida attraverso i passaggi necessari e ti aiuta a verificare che le tue impostazioni siano conformi alle best practice StorageGRID .



Se si sta configurando un'applicazione S3, si consiglia di utilizzare la procedura guidata di configurazione S3, a meno che non si abbiano requisiti particolari o che l'implementazione non richieda una personalizzazione significativa.

- *Usa il "[Procedura guidata di configurazione FabricPool](#)" *. Simile alla procedura guidata di configurazione di S3, la procedura guidata di configurazione FabricPool consente di configurare rapidamente i valori richiesti e genera un file che è possibile utilizzare quando si configura un livello cloud FabricPool in ONTAP.



Se si prevede di utilizzare StorageGRID come sistema di archiviazione degli oggetti per un livello cloud FabricPool , si consiglia di utilizzare la procedura guidata di configurazione FabricPool , a meno che non si abbiano requisiti speciali o che l'implementazione non richieda una personalizzazione significativa.

- **Configurare gli elementi manualmente.** Se ci si connette a un'applicazione S3 e si preferisce non utilizzare la procedura guidata di configurazione S3, è possibile ottenere i valori richiesti eseguendo manualmente la configurazione. Segui questi passaggi:
 - a. Configurare il gruppo ad alta disponibilità (HA) che si desidera utilizzare per l'applicazione S3. Vedere "[Configurare gruppi ad alta disponibilità](#)" .
 - b. Creare l'endpoint del bilanciatore del carico che verrà utilizzato dall'applicazione S3. Vedere "[Configurare gli endpoint del bilanciatore del carico](#)" .
 - c. Creare l'account tenant che verrà utilizzato dall'applicazione S3. Vedere "[Crea un account inquilino](#)" .
 - d. Per un tenant S3, accedi all'account del tenant e genera un ID chiave di accesso e una chiave di accesso segreta per ogni utente che accederà all'applicazione. Vedere "[Crea le tue chiavi di accesso](#)" .
 - e. Creare uno o più bucket S3 all'interno dell'account tenant. Per S3, vedere "[Crea bucket S3](#)" .
 - f. Per aggiungere istruzioni di posizionamento specifiche per gli oggetti appartenenti al nuovo tenant o bucket/contenitore, creare una nuova regola ILM e attivare una nuova policy ILM per utilizzare tale regola. Vedere "[Crea regola ILM](#)" E "[Crea policy ILM](#)" .

Sicurezza per i client S3

Gli account tenant StorageGRID utilizzano applicazioni client S3 per salvare i dati degli oggetti in StorageGRID. Dovresti rivedere le misure di sicurezza implementate per le applicazioni client.

Riepilogo

L'elenco seguente riassume come viene implementata la sicurezza per l'API REST S3:

Sicurezza della connessione

TLS

Autenticazione del server

Certificato del server X.509 firmato dalla CA di sistema o certificato del server personalizzato fornito dall'amministratore

Autenticazione del client

ID chiave di accesso all'account S3 e chiave di accesso segreta

Autorizzazione del cliente

Proprietà del bucket e tutte le policy di controllo degli accessi applicabili

Come StorageGRID fornisce sicurezza per le applicazioni client

Le applicazioni client S3 possono connettersi al servizio Load Balancer sui nodi gateway o sui nodi amministrativi oppure direttamente sui nodi di archiviazione.

- I client che si connettono al servizio Load Balancer possono utilizzare HTTPS o HTTP, a seconda di come ["configurare l'endpoint del bilanciatore del carico"](#).

HTTPS garantisce una comunicazione sicura e crittografata tramite TLS ed è consigliato. È necessario allegare un certificato di sicurezza all'endpoint.

HTTP fornisce una comunicazione meno sicura e non crittografata e dovrebbe essere utilizzato solo per griglie non di produzione o di prova.

- I client che si connettono ai nodi di archiviazione possono anche utilizzare HTTPS o HTTP.

HTTPS è il protocollo predefinito ed è consigliato.

HTTP fornisce una comunicazione meno sicura e non crittografata, ma può essere facoltativamente ["abilitato"](#) per griglie non di produzione o di prova.

- Le comunicazioni tra StorageGRID e il client sono crittografate tramite TLS.
- Le comunicazioni tra il servizio Load Balancer e i nodi di archiviazione all'interno della griglia sono crittografate indipendentemente dal fatto che l'endpoint del load balancer sia configurato per accettare connessioni HTTP o HTTPS.
- I clienti devono fornire ["Intestazioni di autenticazione HTTP"](#) a StorageGRID per eseguire operazioni REST API.

Certificati di sicurezza e applicazioni client

In tutti i casi, le applicazioni client possono effettuare 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 load balancer. Ogni endpoint del bilanciatore del carico ha il 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 sul bilanciamento del carico"](#) .

- Quando le applicazioni client si connettono direttamente a un nodo di archiviazione, utilizzano i certificati server generati dal sistema per i nodi di archiviazione 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 ["aggiungi un certificato API S3 personalizzato"](#) .

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

Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un set di suite di cifratura che le applicazioni client possono utilizzare quando stabiliscono una sessione TLS. Per configurare i cifrari, vai su **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza** e seleziona **Criteri TLS e SSH**.

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 la procedura guidata di configurazione S3

Utilizzare la procedura guidata di configurazione S3: considerazioni e requisiti

È possibile utilizzare la procedura guidata di configurazione S3 per configurare StorageGRID come sistema di archiviazione degli oggetti per un'applicazione S3.

Quando utilizzare la procedura guidata di configurazione S3

La procedura guidata di configurazione di S3 ti guida attraverso ogni fase della configurazione di StorageGRID per l'utilizzo con un'applicazione S3. Durante il completamento della procedura guidata, scaricherai i file che potrai utilizzare per immettere valori nell'applicazione S3. Utilizza la procedura guidata per configurare il sistema più rapidamente e per assicurarti che le impostazioni siano conformi alle best practice StorageGRID .

Se hai il ["Permesso di accesso root"](#) , puoi completare la procedura guidata di configurazione di S3 quando inizi a utilizzare StorageGRID Grid Manager oppure puoi accedere e completare la procedura guidata in qualsiasi momento successivo. A seconda delle esigenze, è anche possibile configurare manualmente alcuni o tutti gli elementi richiesti e quindi utilizzare la procedura guidata per assemblare i valori necessari a un'applicazione S3.

Prima di utilizzare la procedura guidata

Prima di utilizzare la procedura guidata, verificare di aver completato questi prerequisiti.

Ottenere indirizzi IP e configurare le interfacce VLAN

Se si configura un gruppo ad alta disponibilità (HA), si sa a quali nodi si conatterà l'applicazione S3 e quale rete StorageGRID verrà utilizzata. Si sa anche quali valori immettere per il CIDR della subnet, l'indirizzo IP del gateway e gli indirizzi IP virtuali (VIP).

Se si prevede di utilizzare una LAN virtuale per separare il traffico dall'applicazione S3, è già stata configurata l'interfaccia VLAN. Vedere ["Configurare le interfacce VLAN"](#) .

Configurare la federazione delle identità e SSO

Se intendi utilizzare la federazione delle identità o l'accesso singolo (SSO) per il tuo sistema StorageGRID , hai abilitato queste funzionalità. Si sa anche quale gruppo federato deve avere accesso root per l'account tenant che verrà utilizzato dall'applicazione S3. Vedere ["Utilizzare la federazione delle identità"](#) E ["Configurare l'accesso singolo"](#) .

Ottieni e configura i nomi di dominio

Sai quale nome di dominio completo (FQDN) utilizzare per StorageGRID. Le voci del server dei nomi di dominio (DNS) mapperanno questo FQDN agli indirizzi IP virtuali (VIP) del gruppo HA creato tramite la procedura guidata.

Se si prevede di utilizzare richieste in stile host virtuale S3, è necessario disporre ["nomi di dominio endpoint S3 configurati"](#) . Si consiglia di utilizzare richieste in stile virtual hosted.

Esaminare i requisiti del bilanciatore del carico e del certificato di sicurezza

Se si prevede di utilizzare il bilanciatore del carico StorageGRID , è necessario aver esaminato le considerazioni generali sul bilanciamento del carico. Hai i certificati che caricherai o i valori necessari per generare un certificato.

Se si prevede di utilizzare un endpoint di bilanciamento del carico esterno (di terze parti), è necessario disporre del nome di dominio completo (FQDN), della porta e del certificato per tale bilanciatore del carico.

Configurare tutte le connessioni della federazione di griglia

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 di federazione della griglia, confermare quanto segue prima di avviare la procedura guidata:

- Hai ["configurato la connessione della federazione di griglia"](#) .
- Lo stato della connessione è **Connesso**.
- Hai i permessi di accesso Root.

Accedi e completa la procedura guidata di configurazione S3

È possibile utilizzare la procedura guidata di configurazione S3 per configurare StorageGRID per l'utilizzo con un'applicazione S3. La procedura guidata di configurazione fornisce i valori necessari all'applicazione per accedere a un bucket StorageGRID e salvare gli oggetti.

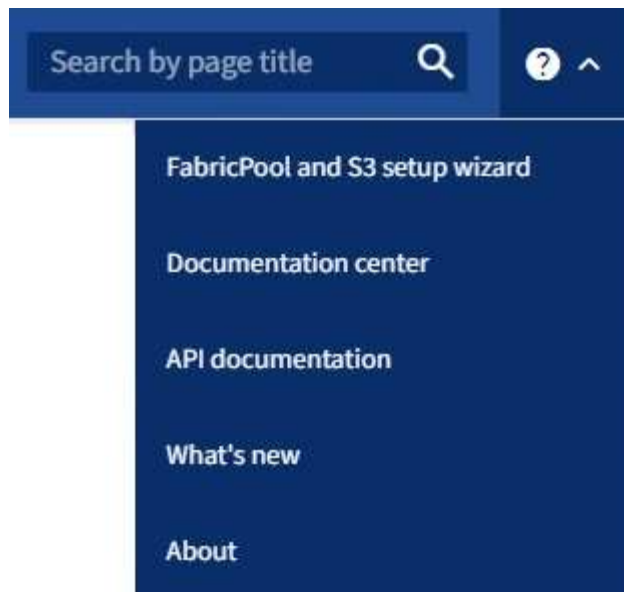
Prima di iniziare

- Tu hai il ["Permesso di accesso root"](#) .
- Hai esaminato il ["considerazioni e requisiti"](#) per utilizzare la procedura guidata.

Accedi alla procedura guidata

Passi

1. Sign in a Grid Manager utilizzando un ["browser web supportato"](#) .
2. Se nella dashboard viene visualizzato il banner **Procedura guidata di configurazione FabricPool e S3**, selezionare il collegamento nel banner. Se il banner non viene più visualizzato, seleziona l'icona della guida dalla barra dell'interfaccia in Grid Manager e seleziona **Procedura guidata di configurazione di FabricPool e S3**.



3. Nella sezione Applicazione S3 della pagina della procedura guidata di configurazione FabricPool e S3, seleziona **Configura ora**.

Passaggio 1 di 6: configurare il gruppo HA

Un gruppo HA è una raccolta di nodi, ognuno dei quali contiene il servizio StorageGRID Load Balancer. Un gruppo HA può contenere nodi gateway, nodi amministrativi o entrambi.

È possibile utilizzare un gruppo HA per mantenere disponibili le connessioni dati S3. Se l'interfaccia attiva nel gruppo HA fallisce, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni S3.

Per i dettagli su questa attività, vedere "[Gestire gruppi ad alta disponibilità](#)".

Passi

1. Se si prevede di utilizzare un bilanciatore del carico esterno, non è necessario creare un gruppo HA. Seleziona **Salta questo passaggio** e vai a [Passaggio 2 di 6: configurare l'endpoint del bilanciatore del carico](#).
2. Per utilizzare il bilanciatore del carico StorageGRID, è possibile creare un nuovo gruppo HA o utilizzare un gruppo HA esistente.

Crea gruppo HA

- a. Per creare un nuovo gruppo HA, seleziona **Crea gruppo HA**.
- b. Per la fase **Inserisci dettagli**, compila i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome visualizzato univoco per questo gruppo HA.
Descrizione (facoltativa)	Descrizione di questo gruppo HA.

- c. Per il passaggio **Aggiungi interfacce**, seleziona le interfacce del nodo che desideri utilizzare in questo gruppo HA.

Utilizzare le intestazioni di colonna per ordinare le righe oppure immettere un termine di ricerca per individuare più rapidamente le interfacce.

È possibile selezionare uno o più nodi, ma è possibile selezionare solo un'interfaccia per ciascun nodo.

- d. Per il passaggio **Assegna priorità alle interfacce**, determinare l'interfaccia primaria e tutte 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 primaria 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 funziona, gli indirizzi IP virtuali (VIP) vengono spostati sulla prima interfaccia di backup in ordine di priorità. Se tale interfaccia non funziona, gli indirizzi VIP vengono spostati alla successiva interfaccia di backup e così via. Una volta risolti i guasti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

- e. Per il passaggio **Inserisci indirizzi IP**, compila i seguenti campi.

Campo	Descrizione
CIDR di sottorete	L'indirizzo della subnet VIP in notazione CIDR: un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere alcun bit host impostato. Ad esempio, 192.16.0.0/22.
Indirizzo IP del gateway (facoltativo)	Se gli indirizzi IP S3 utilizzati per accedere a StorageGRID non si trovano sulla stessa subnet degli indirizzi VIP StorageGRID, immettere l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve essere all'interno della subnet VIP.

Campo	Descrizione
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. Facoltativamente, è possibile specificare indirizzi IPv4 e IPv6 aggiuntivi.

f. Selezionare **Crea gruppo HA** e quindi **Fine** per tornare alla procedura guidata di configurazione di 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 da **Seleziona un gruppo HA**.

b. Selezionare **Continua** per passare alla fase di bilanciamento del carico.

Passaggio 2 di 6: configurare l'endpoint del bilanciatore del carico

StorageGRID utilizza un bilanciatore del carico per gestire il carico di lavoro delle applicazioni client. Il bilanciamento del carico massimizza la velocità e la capacità di connessione su più nodi di archiviazione.

È possibile utilizzare il servizio StorageGRID Load Balancer, presente su tutti i nodi gateway e amministrativi, oppure connettersi a un bilanciatore del carico esterno (di terze parti). Si consiglia di utilizzare il bilanciatore del carico StorageGRID .

Per i dettagli su questa attività, vedere "[Considerazioni sul bilanciamento del carico](#)".

Per utilizzare il servizio StorageGRID Load Balancer, seleziona la scheda * StorageGRID load balancer* e quindi crea o seleziona l'endpoint del load balancer che desideri utilizzare. Per utilizzare un bilanciatore del carico esterno, seleziona la scheda **Bilanciatore del carico esterno** e fornisci i dettagli sul sistema che hai già configurato.

Crea endpoint

Passi

1. Per creare un endpoint del bilanciatore del carico, seleziona **Crea endpoint**.
2. Per il passaggio **Inserisci i dettagli dell'endpoint**, compila 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 impostato su 10433 per il primo endpoint creato, ma è possibile immettere qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, perché queste porte sono riservate sui nodi amministrativi. Nota: non sono consentite le porte utilizzate da altri servizi di rete. Vedi il "Riferimento porta di rete".
Tipo di cliente	Deve essere S3 .
Protocollo di rete	Selezionare HTTPS. Nota: la comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

3. Per il passaggio **Seleziona modalità di associazione**, specificare la modalità di associazione. La modalità di associazione controlla il modo in cui si accede all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (predefinito)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo HA su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione Globale (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 il corrispondente FQDN) di un gruppo HA. Gli endpoint con questa modalità di associazione possono utilizzare tutti lo stesso numero di porta, purché i gruppi HA selezionati per gli endpoint non si sovrappongano.
Interfacce dei nodi	Per accedere a questo endpoint, i client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionati.

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 oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway per accedere a questo endpoint.

4. Per il passaggio **Accesso tenant**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai propri bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

5. Per il passaggio **Allega certificato**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Carica il certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato da una CA, una chiave privata del certificato e un bundle CA facoltativo.
Genera certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere " Configurare gli endpoint del bilanciatore del carico " per i dettagli su cosa inserire.
Utilizzare il certificato StorageGRID S3	Utilizzare questa opzione solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID . Vedere " Configurare i certificati API S3 " per i dettagli.

6. Selezionare **Fine** per tornare alla procedura guidata di configurazione S3.

7. Selezionare **Continua** per passare alla fase tenant e bucket.



Le modifiche al certificato di un endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Utilizzare l'endpoint del bilanciatore del carico esistente

Passi

1. Per utilizzare un endpoint esistente, selezionarne il nome da **Seleziona un endpoint del bilanciatore del carico**.
2. Selezionare **Continua** per passare alla fase tenant e bucket.

Utilizzare un bilanciatore di carico esterno

Passi

1. Per utilizzare un bilanciatore del carico esterno, compilare i seguenti campi.

Campo	Descrizione
Nome di dominio completo	Nome di dominio completo (FQDN) del bilanciatore del carico esterno.
Porta	Numero di porta che l'applicazione S3 utilizzerà per connettersi al bilanciatore del carico esterno.
Certificato	Copiare il certificato del server per il bilanciatore del carico esterno e incollarlo in questo campo.

2. Selezionare **Continua** per passare alla fase tenant e bucket.

Passaggio 3 di 6: creare tenant e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per archiviare e recuperare oggetti in StorageGRID. Ogni tenant ha i propri utenti, chiavi di accesso, bucket, oggetti e un set specifico di funzionalità.

Un bucket è un contenitore utilizzato per archiviare gli oggetti e i metadati degli oggetti di un tenant. Anche se i tenant potrebbero avere molti bucket, la procedura guidata ti aiuta a creare un tenant e un bucket nel modo più rapido e semplice. Se in un secondo momento è necessario aggiungere bucket o impostare opzioni, è possibile utilizzare Tenant Manager.

Per i dettagli su questa attività, vedere ["Crea un account inquilino"](#) e ["Crea bucket S3"](#).

Passi

1. Inserisci un nome per l'account tenant.

I nomi degli inquilini non devono essere univoci. Quando viene creato l'account tenant, questo riceve un ID account numerico univoco.

2. Definisci l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del sistema StorageGRID ["federazione di identità"](#), ["accesso unico \(SSO\)"](#), o entrambi.

Opzione	Fai questo
Se la federazione delle identità non è abilitata	Specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se la federazione delle identità è abilitata	a. Seleziona un gruppo federato esistente da avere "Permesso di accesso root" per l'inquilino. b. Facoltativamente, specificare la password da utilizzare quando si accede al tenant come utente root locale.

Opzione	Fai questo
Se sono abilitati sia la federazione delle identità che il Single Sign-On (SSO)	Seleziona un gruppo federato esistente da avere "Permesso di accesso root" per l'inquilino. Nessun utente locale può effettuare l'accesso.

- 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 del tenant sarà l'utente root. Se altri utenti utilizzeranno questo tenant, ["utilizzare Tenant Manager"](#) per configurare chiavi e permessi.

- Se desideri creare subito un bucket per questo tenant, seleziona **Crea bucket per questo tenant**.



Se il blocco oggetti S3 è abilitato per la griglia, il bucket creato in questo passaggio non ha il blocco oggetti S3 abilitato. Se è necessario utilizzare un bucket S3 Object Lock per questa applicazione S3, non selezionare l'opzione per creare un bucket ora. Invece, usa Tenant Manager per ["creare il secchio"](#) Dopo.

- Immettere il nome del bucket che verrà utilizzato dall'applicazione S3. Ad esempio, `s3-bucket`.

Non è possibile modificare il nome del bucket dopo averlo creato.

- Seleziona la **Regione** per questo bucket.

Utilizza la regione predefinita (`us-east-1`) a meno che non si preveda di utilizzare ILM in futuro per filtrare gli oggetti in base alla regione del bucket.

- Seleziona **Crea e continua**.

Passaggio 4 di 6: Scarica i dati

Nella fase di download dei dati, puoi scaricare uno o due file per salvare i dettagli di ciò che hai appena configurato.

Passi

- Se hai selezionato **Crea automaticamente la chiave di accesso S3 dell'utente root**, esegui una o entrambe le seguenti operazioni:
 - Seleziona **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.
- Selezionare **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.
- Salvare queste informazioni in un luogo sicuro.



Non chiudere questa pagina finché non hai copiato entrambe le chiavi di accesso. Le chiavi non saranno più disponibili dopo aver chiuso questa pagina. Assicuratevi di salvare queste informazioni in un luogo sicuro, perché possono essere utilizzate per ottenere dati dal vostro sistema StorageGRID.

4. Se richiesto, seleziona la casella di controllo per confermare di aver scaricato o copiato le chiavi.
5. Selezionare **Continua** per passare alla fase relativa alle regole e ai criteri ILM.

Passaggio 5 di 6: rivedere la regola ILM e la policy ILM per S3

Le regole di gestione del ciclo di vita delle informazioni (ILM) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel sistema StorageGRID . La policy ILM inclusa in StorageGRID crea due copie replicate di tutti gli oggetti. Questa politica è valida finché non attivi almeno una nuova politica.

Passi

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 un nuovo criterio. Vedere ["Crea regola ILM"](#) E ["Utilizzare le policy ILM"](#) .
3. Seleziona **Ho esaminato questi passaggi e ho capito cosa devo fare**.
4. Seleziona la casella di controllo per indicare che hai capito cosa fare dopo.
5. Selezionare **Continua** per andare a **Riepilogo**.

Fase 6 di 6: Riepilogo della revisione

Passi

1. Rivedi 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 * Sign in come root* si accede a Tenant Manager, dove è possibile aggiungere utenti tenant, creare bucket aggiuntivi e aggiornare le impostazioni dei bucket.
3. Selezionare **Fine**.
4. Configurare l'applicazione utilizzando il file scaricato da StorageGRID o i valori ottenuti manualmente.

Gestire i gruppi HA

Cosa sono i gruppi ad alta disponibilità (HA)?

I gruppi ad alta disponibilità (HA) forniscono connessioni dati ad alta disponibilità per i client S3 e connessioni ad alta disponibilità per Grid Manager e Tenant Manager.

È possibile raggruppare le interfacce di rete di più nodi di amministrazione e gateway in un gruppo ad alta disponibilità (HA). Se l'interfaccia attiva nel gruppo HA non funziona, un'interfaccia di backup può gestire il carico di lavoro.

Ogni gruppo HA fornisce l'accesso ai servizi condivisi sui nodi selezionati.

- I gruppi HA che includono nodi gateway, nodi amministrativi o entrambi forniscono connessioni dati ad alta disponibilità per i client S3.
- I gruppi HA che includono solo nodi amministrativi forniscono connessioni ad alta disponibilità al Grid Manager e al Tenant Manager.
- Un gruppo HA che include solo appliance di servizi e nodi software basati su VMware può fornire connessioni ad alta disponibilità per ["Tenant S3 che utilizzano S3 Select"](#) . I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono obbligatori.

Come si crea un gruppo HA?

1. Selezionare un'interfaccia di rete per uno o più nodi amministrativi o nodi 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 ha un indirizzo IP assegnato tramite DHCP.

2. Si specifica un'interfaccia come interfaccia primaria. L'interfaccia primaria è l'interfaccia attiva, a meno che non si verifichi un errore.
3. È possibile determinare l'ordine di priorità per tutte le interfacce di backup.
4. Assegna al gruppo da uno a 10 indirizzi IP virtuali (VIP). Le applicazioni client possono utilizzare uno qualsiasi di questi indirizzi VIP per connettersi a StorageGRID.

Per le istruzioni, vedere ["Configurare gruppi ad alta disponibilità"](#).

Qual 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 in ordine di priorità. Finché l'interfaccia primaria rimane disponibile, viene utilizzata quando i client si connettono a qualsiasi indirizzo VIP del gruppo. Ciò significa che durante il normale funzionamento, l'interfaccia primaria è l'interfaccia "attiva" per il gruppo.

Allo stesso modo, durante il normale funzionamento, tutte le interfacce con priorità inferiore per il gruppo HA fungono da interfacce di "backup". Queste interfacce di backup non vengono utilizzate a meno che l'interfaccia primaria (attualmente attiva) non diventi più disponibile.

Visualizza lo stato attuale del gruppo HA di un nodo

Per verificare se un nodo è assegnato a un gruppo HA e determinarne lo stato attuale, selezionare **NODI > nodo**.

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 è lo 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; questa è un'interfaccia di backup.
- **Arrestato:** il gruppo HA non può essere ospitato su questo nodo perché il servizio High Availability (keepalived) è stato arrestato manualmente.
- **Errore:** il gruppo HA non può essere ospitato su questo nodo a causa di uno o più dei seguenti motivi:
 - Il servizio Load Balancer (nginx-gw) non è in esecuzione sul nodo.
 - L'interfaccia eth0 o VIP del nodo è inattiva.
 - Il nodo è inattivo.

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 Admin e un'interfaccia di backup per il gruppo di client FabricPool.

DC1-ADM1 (Primary Admin Node)

Overview
Hardware
Network
Storage
Load balancer
Tasks

Node information

Name: DC1-ADM1
Type: Primary Admin Node
ID: ce00d9c8-8a79-4742-bdef-c9c658db5315
Connection state: Connected
Software version: 11.6.0 (build 20211207.1804.614bc17)
HA groups:

Admin clients (Active)
FabricPool clients (Backup)

IP addresses: 172.16.1.225 - eth0 (Grid Network)
10.224.1.225 - eth1 (Admin Network)
47.47.0.2, 47.47.1.225 - eth2 (Client Network)
Show additional IP addresses

Cosa succede quando l'interfaccia attiva fallisce?

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 funziona, gli indirizzi VIP vengono spostati sulla prima interfaccia di backup disponibile in ordine di priorità. Se tale interfaccia non funziona, gli indirizzi VIP vengono spostati alla successiva interfaccia di backup disponibile e così via.

Il failover può essere attivato per uno qualsiasi di questi motivi:

- Il nodo su cui è configurata l'interfaccia si interrompe.
- Il nodo su cui è configurata l'interfaccia perde la connettività con tutti gli altri nodi per almeno 2 minuti.
- L'interfaccia attiva si disattiva.
- Il servizio Load Balancer si arresta.
- Il servizio di alta disponibilità si arresta.



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 sufficientemente veloce da non avere un impatto significativo sulle applicazioni client e da consentire loro di continuare a funzionare con i normali comportamenti di ripetizione.

Quando l'errore viene risolto e un'interfaccia con priorità più alta diventa nuovamente disponibile, gli indirizzi VIP vengono automaticamente spostati sull'interfaccia con priorità più alta disponibile.

Come vengono utilizzati i gruppi HA?

È possibile utilizzare gruppi ad alta disponibilità (HA) per fornire connessioni ad alta disponibilità a StorageGRID per i dati degli oggetti e per uso amministrativo.

- Un gruppo HA può fornire connessioni amministrative ad alta disponibilità al Grid Manager o al Tenant Manager.
- Un gruppo HA può fornire connessioni dati ad alta disponibilità per i client S3.
- Un gruppo HA che contiene una sola interfaccia consente di fornire molti indirizzi VIP e di impostare esplicitamente indirizzi IPv6.

Un gruppo HA può garantire un'elevata disponibilità solo se tutti i nodi inclusi nel gruppo forniscono gli stessi servizi. Quando si crea un gruppo HA, aggiungere le interfacce dai tipi di nodi che forniscono i servizi richiesti.

- **Nodi amministrativi:** includono il servizio Load Balancer e consentono l'accesso al Grid Manager o al Tenant Manager.
- **Nodi gateway:** includono il servizio Load Balancer.

Scopo del gruppo HA	Aggiungi nodi di questo tipo al gruppo HA
Accesso a Grid Manager	• Nodo amministratore primario (Primario) • Nodi amministrativi non primari Nota: il nodo di amministrazione 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 amministrativi primari o non primari
Accesso client S3 - Servizio Load Balancer	• Nodi amministrativi • Nodi gateway
Accesso client S3 per "S3 Seleziona"	• Servizi elettrodomestici • Nodi software basati su VMware Nota: i gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono obbligatori.

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.

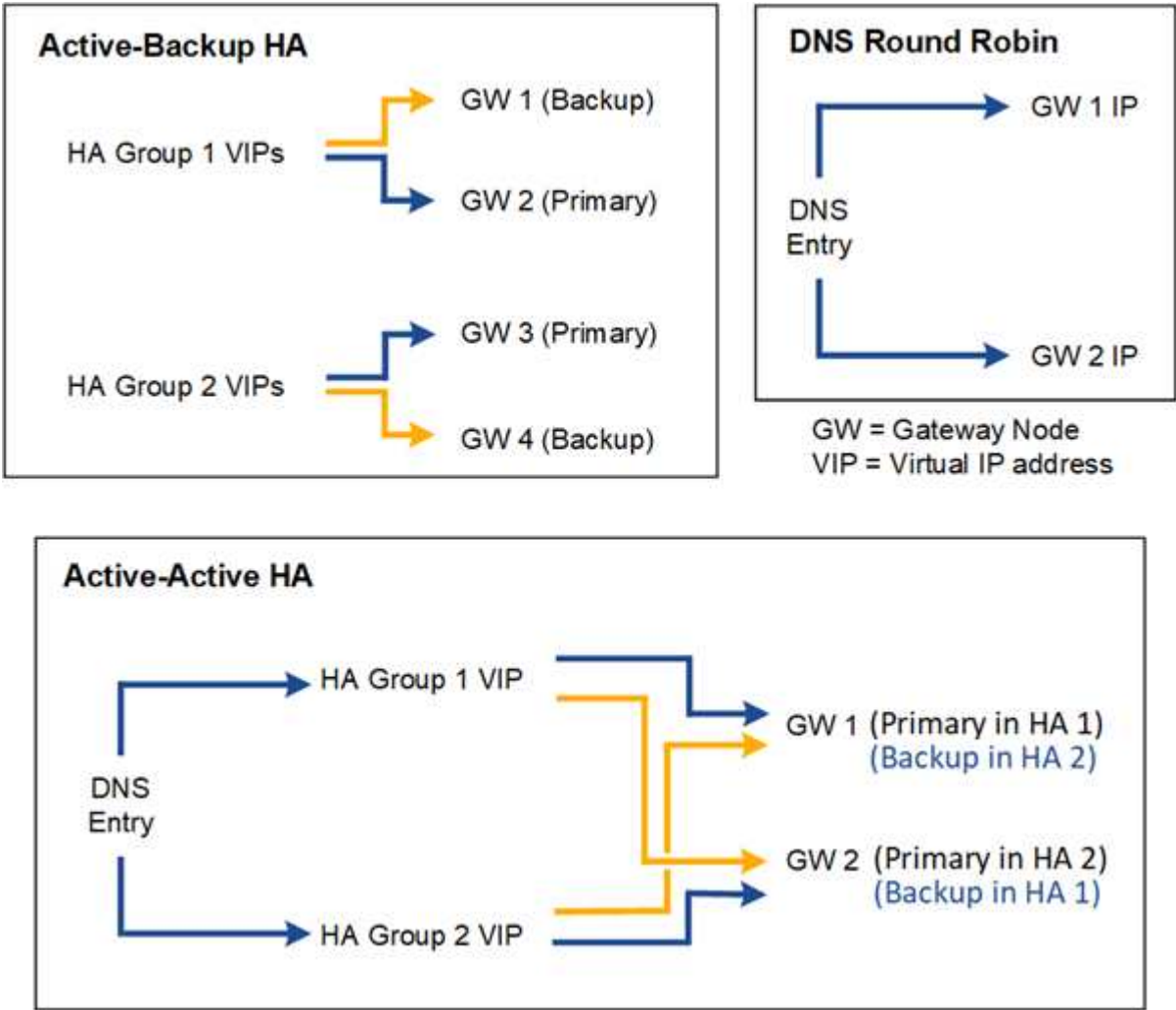
Se hai effettuato l'accesso a Grid Manager o Tenant Manager quando si verifica il failover, verrai disconnesso e dovrai effettuare nuovamente l'accesso per riprendere l'attività.

Alcune procedure di manutenzione non possono essere eseguite 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 diagrammi seguenti forniscono esempi di diversi modi in cui è possibile configurare i gruppi HA. Ogni opzione presenta vantaggi e svantaggi.

Nei diagrammi, il blu indica l'interfaccia primaria 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 con backup attivo	• Gestito da StorageGRID senza dipendenze esterne. • Failover rapido.	• In un gruppo HA è attivo solo un nodo. Almeno un nodo per gruppo HA sarà inattivo.

Configurazione	Vantaggi	Svantaggi
DNS Round Robin	• Aumento della produttività aggregata. • Nessun host inattivo.	• Failover lento, che potrebbe dipendere dal comportamento del client. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Richiede un controllo sanitario implementato dal cliente.
HA attivo-attivo	• Il traffico è distribuito su più gruppi HA. • Elevata produttività aggregata che aumenta con il numero di gruppi HA. • Failover rapido.	• Più complesso da configurare. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Richiede un controllo sanitario implementato dal cliente.

Configurare gruppi ad alta disponibilità

È possibile configurare gruppi ad alta disponibilità (HA) per fornire un accesso altamente disponibile ai servizi sui nodi di amministrazione o sui nodi gateway.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .
- Se si prevede di utilizzare un'interfaccia VLAN in un gruppo HA, è stata creata l'interfaccia VLAN. Vedere ["Configurare le interfacce VLAN"](#) .
- Se si prevede di utilizzare un'interfaccia di accesso per un nodo in un gruppo HA, è stata creata l'interfaccia:
 - **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 aver installato il nodo):** ["Linux: aggiungere interfacce trunk o di accesso a un nodo"](#)
 - **VMware (dopo l'installazione del nodo):** ["VMware: aggiungi trunk o interfacce di accesso a un nodo"](#)

Creare un gruppo ad alta disponibilità

Quando si crea un gruppo ad alta disponibilità, si seleziona una o più interfacce e le si organizza in ordine di priorità. Quindi, assegna uno o più indirizzi VIP al gruppo.

Per includere un nodo gateway o un nodo amministrativo in un gruppo HA, è necessaria un'interfaccia. Un gruppo HA può utilizzare una sola interfaccia per ogni nodo; tuttavia, altre interfacce per lo stesso nodo possono essere utilizzate in altri gruppi HA.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Gruppi ad alta disponibilità**.

2. Seleziona **Crea**.

Inserisci i dettagli per il gruppo HA

Passi

1. Fornire un nome univoco per il gruppo HA.
2. Facoltativamente, immettere una descrizione per il gruppo HA.
3. Selezionare **Continua**.

Aggiungere interfacce al gruppo HA

Passi

1. Selezionare una o più interfacce da aggiungere a questo gruppo HA.

Utilizzare le intestazioni di colonna per ordinare le righe oppure immettere un termine di ricerca per individuare più rapidamente le interfacce.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

Total interface count: 4

	Node	Interface	Site	IPv4 subnet	Node type
☐	DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
☐	DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
☐	DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
☐	DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected



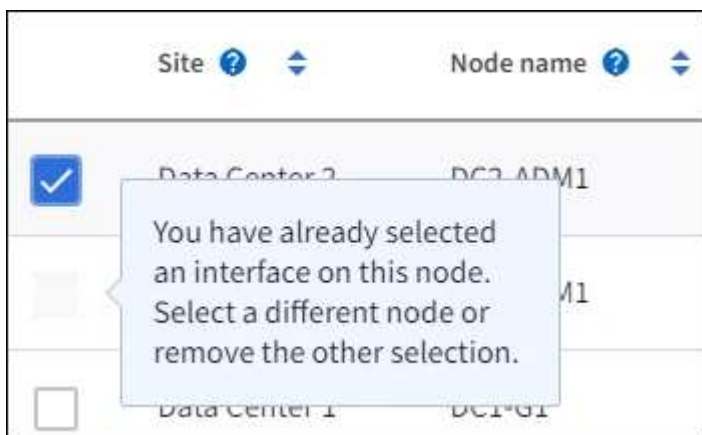
Dopo aver creato un'interfaccia VLAN, attendere fino a 5 minuti affinché la nuova interfaccia venga visualizzata nella tabella.

Linee guida per la selezione delle interfacce

- È necessario selezionare almeno un'interfaccia.
- È possibile selezionare una sola interfaccia per un nodo.
- Se il gruppo HA è destinato alla protezione HA dei servizi del nodo amministrativo, che includono Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi amministrativi.
- Se il gruppo HA è destinato alla protezione HA del traffico client S3, 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 se si verifica un failover, i servizi forniti dal nodo precedentemente attivo potrebbero non essere disponibili sul nodo nuovamente attivo. Ad esempio, un nodo gateway di backup non può fornire protezione HA dei servizi del nodo amministrativo. Allo stesso modo, un Admin Node di backup non può eseguire tutte le procedure di manutenzione che può fornire il Admin Node primario.

- Se non è possibile selezionare un'interfaccia, la relativa casella di controllo è disattivata. La descrizione comandi fornisce ulteriori informazioni.



- Non è possibile selezionare un'interfaccia se il suo valore di subnet o 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 primaria non funziona, gli indirizzi VIP vengono spostati sull'interfaccia con la priorità più alta disponibile. Se tale interfaccia non funziona, gli indirizzi VIP vengono spostati all'interfaccia con priorità più alta disponibile, e così via.

Passi

1. Trascinare le righe nella colonna **Ordine di priorità** per determinare l'interfaccia primaria e le eventuali interfacce di backup.

La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia primaria è l'interfaccia attiva, a meno che non si verifichi un errore.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	DC1-ADM1-104-96	eth2	Primary Admin Node
2	DC2-ADM1-104-103	eth2	Admin Node



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**.

Inserisci gli indirizzi IP

Passi

1. Nel campo **Subnet CIDR**, specificare la subnet VIP in notazione CIDR, ovvero un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32).

L'indirizzo di rete non deve avere alcun bit host impostato. Ad esempio, 192.16.0.0/22.



Se si utilizza un prefisso a 32 bit, l'indirizzo di rete VIP funge anche da indirizzo gateway e indirizzo VIP.

Enter details for the HA group

Subnet CIDR ⓘ
Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional) ⓘ
Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address ⓘ
Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

2. Facoltativamente, se un client amministrativo o tenant S3 accederà a questi indirizzi VIP da una subnet diversa, immettere l'**indirizzo IP del gateway**. L'indirizzo del gateway deve essere all'interno della subnet VIP.

Gli utenti client e amministratori 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 saranno tutti attivi contemporaneamente sull'interfaccia attiva.

È necessario fornire almeno un indirizzo IPv4. Facoltativamente, è possibile specificare indirizzi IPv4 e IPv6 aggiuntivi.

4. Selezionare **Crea gruppo HA** e selezionare **Fine**.

Il gruppo HA è stato creato ed è ora possibile utilizzare gli indirizzi IP virtuali configurati.

Prossimi passi

Se si intende utilizzare questo gruppo HA per il bilanciamento del carico, creare un endpoint del bilanciatore del carico per determinare la porta e il protocollo di rete e per allegare eventuali certificati richiesti. Vedere ["Configurare gli endpoint del bilanciatore del carico"](#).

Modifica un gruppo ad alta disponibilità

È possibile modificare un gruppo ad alta disponibilità (HA) per cambiarne il nome e la descrizione, aggiungere o rimuovere interfacce, cambiare 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 dismissione di un sito o di un nodo.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Gruppi ad alta disponibilità**.

La pagina Gruppi ad alta disponibilità mostra tutti i gruppi HA esistenti.

2. Selezionare la casella di controllo per il gruppo HA che si desidera modificare.

3. A seconda di cosa vuoi aggiornare, procedi in uno dei seguenti modi:

- 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 hai selezionato **Modifica indirizzo IP virtuale**:

- a. Aggiornare gli indirizzi IP virtuali per il gruppo HA.
- b. Seleziona **Salva**.
- c. Selezionare **Fine**.

5. Se hai selezionato **Modifica gruppo HA**:

- a. Facoltativamente, aggiorna il nome o la descrizione del gruppo.
- b. Facoltativamente, seleziona o deseleziona le caselle di controllo per aggiungere o rimuovere le 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 di tutte le interfacce di backup per questo gruppo HA.
- d. Facoltativamente, aggiornare gli indirizzi IP virtuali.
- e. Selezionare **Salva** e poi **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 del bilanciatore del carico. Per eliminare un gruppo HA, è necessario rimuoverlo da tutti gli endpoint del bilanciatore del carico che lo utilizzano.

Per evitare interruzioni del client, aggiornare tutte le applicazioni client S3 interessate prima di rimuovere un gruppo HA. Aggiornare ciascun client in modo che si connetta 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.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Gruppi ad alta disponibilità**.
2. Esaminare la colonna **Endpoint del bilanciatore del carico** per ogni gruppo HA che si desidera rimuovere. Se sono elencati degli endpoint del bilanciatore del carico:
 - a. Vai a **CONFIGURAZIONE > Rete > Endpoint del bilanciatore del carico**.
 - b. Selezionare la casella di controllo per l'endpoint.
 - c. Selezionare **Azioni > Modifica modalità di associazione endpoint**.
 - d. Aggiornare la modalità di associazione per rimuovere il gruppo HA.
 - e. Seleziona **Salva modifiche**.
3. Se non sono elencati endpoint del bilanciatore del carico, selezionare la casella di controllo per ciascun gruppo HA che si desidera rimuovere.
4. Selezionare **Azioni > Rimuovi gruppo HA**.
5. Rivedi il messaggio e seleziona **Elimina gruppo HA** per confermare la selezione.

Tutti i gruppi HA selezionati verranno rimossi. Nella pagina Gruppi ad alta disponibilità viene visualizzato un banner verde di successo.

Gestire il bilanciamento del carico

Considerazioni sul bilanciamento del carico

È possibile utilizzare il bilanciamento del carico per gestire i carichi di lavoro di acquisizione e recupero dai client S3.

Che cos'è il bilanciamento del carico?

Quando un'applicazione client salva o recupera dati da un sistema StorageGRID, StorageGRID utilizza un bilanciatore 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 su più nodi di archiviazione.

Il servizio StorageGRID Load Balancer è installato su tutti i nodi amministrativi e su tutti i nodi gateway e fornisce il bilanciamento del carico di livello 7. Esegue la terminazione Transport Layer Security (TLS) delle richieste client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di archiviazione.

Il servizio Load Balancer su ciascun nodo funziona in modo indipendente quando inoltra il traffico client ai nodi di archiviazione. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai

nodi di archiviazione con maggiore disponibilità della CPU.



Sebbene il servizio StorageGRID Load Balancer sia il meccanismo di bilanciamento del carico consigliato, potrebbe essere opportuno integrare un bilanciatore del carico di terze parti. Per informazioni, contattare il rappresentante dell'account NetApp o fare riferimento a ["TR-4626: Bilanciatori di carico globali e di terze parti StorageGRID"](#).

Di quanti nodi di bilanciamento del carico ho bisogno?

Come buona pratica generale, ogni sito nel sistema StorageGRID dovrebbe includere due o più nodi con il servizio Load Balancer. Ad esempio, un sito potrebbe includere due nodi gateway oppure sia un nodo amministrativo che un nodo gateway. Assicurarsi che vi sia un'adeguata infrastruttura di rete, hardware o virtualizzazione per ciascun nodo di bilanciamento del carico, indipendentemente dal fatto che si utilizzino appliance di servizi, nodi bare metal o nodi basati su macchine virtuali (VM).

Che cos'è un endpoint di bilanciamento del carico?

Un endpoint del bilanciatore del carico definisce la porta e il protocollo di rete (HTTPS o HTTP) che le richieste delle applicazioni client in entrata e in uscita utilizzeranno per accedere ai nodi che contengono il servizio di bilanciamento del carico. L'endpoint definisce anche il tipo di client (S3), la modalità di associazione e, facoltativamente, un elenco di tenant consentiti o bloccati.

Per creare un endpoint del bilanciatore del carico, seleziona **CONFIGURAZIONE > Rete > Endpoint del bilanciatore del carico** oppure completa la procedura guidata di configurazione FabricPool e S3. Per istruzioni:

- ["Configurare gli endpoint del bilanciatore del carico"](#)
- ["Utilizzare la procedura guidata di configurazione S3"](#)
- ["Utilizzare la procedura guidata di configurazione FabricPool"](#)

Considerazioni per il porto

Per impostazione predefinita, la porta per un endpoint del bilanciatore del carico è 10433 per il primo endpoint creato, ma è possibile specificare qualsiasi porta esterna non utilizzata 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 amministrativi. Se si utilizza la stessa porta per più endpoint, è necessario specificare una modalità di associazione diversa per ciascun endpoint.

Non sono consentite le porte utilizzate da altri servizi di rete. Vedi il ["Riferimento porta di rete"](#).

Considerazioni sul protocollo di rete

Nella maggior parte dei casi, le connessioni tra le applicazioni client e StorageGRID dovrebbero utilizzare la crittografia Transport Layer Security (TLS). 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 bilanciatore del carico StorageGRID, è necessario selezionare **HTTPS**.

Considerazioni sui certificati degli endpoint del bilanciatore del carico

Se selezioni **HTTPS** come protocollo di rete per l'endpoint del bilanciatore del carico, devi fornire un certificato di sicurezza. Quando si crea l'endpoint del bilanciatore del carico, è possibile utilizzare una qualsiasi di queste tre opzioni:

- **Carica un certificato firmato (consigliato).** Questo certificato può essere firmato da un'autorità di certificazione (CA) pubblica o privata. La procedura consigliata per proteggere la connessione è quella di utilizzare un certificato del server CA pubblicamente attendibile. A differenza dei certificati generati, i certificati firmati da una CA possono essere ruotati senza interruzioni, il che può aiutare a evitare problemi di scadenza.

Prima di creare l'endpoint del bilanciatore del carico, è necessario ottenere i seguenti file:

- Il file del certificato del server personalizzato.
 - File della chiave privata del certificato del server personalizzato.
 - Facoltativamente, un pacchetto CA dei certificati di ciascuna autorità di certificazione emittente intermedia.
- **Genera un certificato autofirmato.**
 - **Utilizzare il certificato globale StorageGRID S3.** È necessario caricare o generare una versione personalizzata di questo certificato prima di poterlo selezionare per l'endpoint del bilanciatore del carico. Vedere "[Configurare i certificati API S3](#)".

Di quali valori ho bisogno?

Per creare il certificato, è necessario conoscere tutti i nomi di dominio e gli indirizzi IP che le applicazioni client S3 utilizzeranno 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. Per esempio:

```
Subject DN:  
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

Se necessario, il certificato può utilizzare caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi amministrativi e dei nodi gateway che eseguono il servizio Load Balancer. Per esempio, *.storagegrid.example.com usa il carattere jolly * per rappresentare adm1.storagegrid.example.com e gn1.storagegrid.example.com.

Se si prevede di utilizzare richieste in stile host virtuale S3, il certificato deve includere anche una voce **Nome alternativo** per ciascuna "[Nome di dominio dell'endpoint S3](#)" che hai configurato, inclusi eventuali nomi jolly. Per esempio:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```



Se si utilizzano caratteri jolly per i nomi di dominio, rivedere il "[Linee guida per il rafforzamento dei certificati del server](#)".

È inoltre necessario definire una voce DNS per ciascun nome nel certificato di sicurezza.

Come posso gestire 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 dei certificati, seguire queste best practice:

- Monitorare attentamente tutti gli avvisi che segnalano l'avvicinarsi della data di scadenza dei certificati, come gli avvisi **Scadenza del certificato dell'endpoint del bilanciatore del carico** e **Scadenza del certificato del server globale per l'API S3**.
- Mantenere sempre sincronizzate le versioni del certificato dell'applicazione StorageGRID e S3. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint del bilanciatore del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato dall'applicazione S3.
- Utilizzare un certificato CA firmato pubblicamente. Se si utilizza un certificato firmato da una CA, è possibile sostituire i certificati prossimi alla scadenza senza interruzioni.
- Se hai generato un certificato StorageGRID autofirmato e tale certificato sta per scadere, devi sostituirlo manualmente sia in StorageGRID che nell'applicazione S3 prima che scada il certificato esistente.

Considerazioni sulla modalità di rilegatura

La modalità di associazione consente di controllare quali indirizzi IP possono essere utilizzati per accedere a un endpoint del bilanciatore del carico. Se un endpoint utilizza una modalità di associazione, le applicazioni client possono accedere all'endpoint solo se utilizzano un indirizzo IP consentito o il corrispondente nome di dominio completo (FQDN). Le applicazioni client che utilizzano un altro indirizzo IP o FQDN non possono accedere all'endpoint.

È possibile specificare una qualsiasi delle seguenti modalità di associazione:

- **Globale** (predefinito): le applicazioni client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo, 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 FQDN corrispondente) di un gruppo HA.
- **Interfacce dei nodi**. I client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionati.
- **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 oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway.

Considerazioni sull'accesso degli inquilini

L'accesso tenant è una funzionalità di sicurezza facoltativa che consente di controllare quali account tenant StorageGRID possono utilizzare un endpoint del bilanciatore del carico per accedere ai propri 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 garantire un migliore isolamento di sicurezza tra i tenant e i loro endpoint. Ad esempio, è possibile utilizzare questa funzionalità per garantire che i materiali top secret o altamente classificati di proprietà di un inquilino rimangano completamente inaccessibili agli altri inquilini.



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 l'accesso anonimo), per determinare il tenant viene utilizzato il proprietario del bucket.

Esempio di accesso dell'inquilino

Per capire come funziona questa funzione di sicurezza, prendiamo in considerazione il seguente esempio:

1. Hai creato due endpoint del bilanciatore del carico, come segue:
 - Endpoint **pubblico**: 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**. A tutti gli altri tenant è impedito l'accesso a questo endpoint.
2. IL `top-secret.pdf` si trova in un bucket di proprietà del tenant **Top secret**.

Per accedere al `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, riceverà immediatamente un messaggio di accesso negato. L'accesso viene negato anche se le credenziali e la firma sono valide.

disponibilità della CPU

Il servizio Load Balancer su ciascun nodo amministrativo e nodo gateway funziona in modo indipendente quando inoltra il traffico S3 ai nodi di archiviazione. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di archiviazione con 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 archiviazione viene assegnato un valore di peso di base minimo, anche se un nodo segnala un utilizzo del 100% o non segnala il proprio 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 bilanciatore del carico

Gli endpoint del bilanciatore del carico determinano le porte e i protocolli di rete che i client S3 possono utilizzare quando si connettono al bilanciatore del carico StorageGRID sui nodi gateway e amministrativi. È anche possibile utilizzare gli endpoint per accedere a Grid Manager, Tenant Manager o entrambi.



I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere ["Configurare le connessioni client S3 e Swift"](#).

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).
- Hai esaminato il ["considerazioni per il bilanciamento del carico"](#).
- Se in precedenza hai rimappato una porta che intendi utilizzare per l'endpoint del bilanciatore del carico, hai ["rimosso il rimappaggio della porta"](#).
- Hai creato tutti i gruppi ad alta disponibilità (HA) che intendi utilizzare. I gruppi HA sono consigliati, ma non obbligatori. Vedere ["Gestire gruppi ad alta disponibilità"](#).
- Se l'endpoint del bilanciatore del carico verrà utilizzato da ["Tenant S3 per S3 Select"](#), non deve utilizzare gli indirizzi IP o i nomi di dominio completi di alcun nodo bare-metal. Per gli endpoint del bilanciatore del carico utilizzati per S3 Select sono consentiti solo appliance di servizi e nodi software basati su VMware.

- Hai configurato tutte le interfacce VLAN che intendi utilizzare. Vedere "[Configurare le interfacce VLAN](#)".
- Se si sta creando un endpoint HTTPS (consigliato), si dispone delle informazioni per il certificato del server.



Le modifiche al certificato di un endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

- Per caricare un certificato, sono necessari il certificato del server, la chiave privata del certificato e, facoltativamente, un bundle CA.
- Per generare un certificato, sono necessari tutti i nomi di dominio e gli indirizzi IP che i client S3 utilizzeranno per accedere all'endpoint. È necessario conoscere anche l'argomento (Nome distinto).
- Se si desidera utilizzare il certificato API StorageGRID S3 (che può essere utilizzato anche per le connessioni dirette ai nodi di archiviazione), è già stato sostituito il certificato predefinito con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere "[Configurare i certificati API S3](#)".

Creare un endpoint del bilanciatore del carico

Ogni endpoint del bilanciatore del carico del client S3 specifica una porta, un tipo di client (S3) e un protocollo di rete (HTTP o HTTPS). Gli endpoint del bilanciatore del carico dell'interfaccia di gestione specificano una porta, un tipo di interfaccia e una rete client non attendibile.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Endpoint del bilanciatore del carico**.
2. Per creare un endpoint per un client S3 o Swift, selezionare la scheda **Client S3 o Swift**.
3. Per creare un endpoint per l'accesso a Grid Manager, Tenant Manager o entrambi, selezionare la scheda **Interfaccia di gestione**.
4. Seleziona **Crea**.

Inserisci i dettagli dell'endpoint

Passi

1. Selezionare le istruzioni appropriate per immettere 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 apparirà nella tabella nella pagina Endpoint del bilanciatore 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 puoi utilizzare la porta 8443 come endpoint S3 e la porta verrà configurata sia sul gateway che sui nodi di amministrazione.
Tipo di cliente	Il tipo di applicazione client che utilizzerà questo endpoint, S3 o Swift .
Protocollo di rete	Protocollo di rete che i client utilizzeranno per connettersi a questo endpoint. • Selezionare HTTPS per comunicazioni sicure e crittografate TLS (consigliato). 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 apparirà nella tabella nella pagina Endpoint del bilanciatore del carico.
Porta	La porta StorageGRID che si desidera utilizzare per accedere a Grid Manager, Tenant Manager o entrambi. • Responsabile della griglia: 8443 • Responsabile dell'affitto: 9443 • Sia il gestore della griglia che il gestore dell'inquilino: 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 accederà tramite questo endpoint.

Campo	Descrizione
Rete client non attendibile	Selezionare Sì se questo endpoint deve essere accessibile alle reti client non attendibili. Altrimenti, seleziona No. Se selezioni Sì, la porta è aperta su tutte le reti client non attendibili. Nota: è possibile configurare una porta in modo che sia aperta o chiusa per reti client non attendibili solo quando si crea l'endpoint del bilanciatore del carico.

1. Selezionare **Continua**.

Seleziona una modalità di rilegatura

Passi

1. Selezionare una modalità di associazione per l'endpoint per controllare il modo in cui si accede all'endpoint tramite qualsiasi indirizzo IP o tramite indirizzi IP e interfacce di rete specifici.

Alcune modalità di associazione sono disponibili sia per gli endpoint client che per gli endpoint dell'interfaccia di gestione. Qui sono elencate tutte le modalità per entrambi i tipi di endpoint.

Modalità	Descrizione
Globale (predefinito per gli endpoint client)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo, 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 il corrispondente FQDN) di un gruppo HA. Gli endpoint con questa modalità di associazione possono utilizzare tutti lo stesso numero di porta, purché i gruppi HA selezionati per gli endpoint non si sovrappongano.
Interfacce dei nodi	Per accedere a questo endpoint, i client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionati.
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 oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway per accedere a questo endpoint.
Tutti i nodi amministrativi (predefiniti per gli endpoint dell'interfaccia di gestione)	Per accedere a questo endpoint, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione.

Se più endpoint utilizzano 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 creano endpoint dell'interfaccia di gestione, sono consentiti solo i nodi amministrativi.

2. Se hai selezionato **IP virtuali dei gruppi HA**, seleziona uno o più gruppi HA.

Se si creano endpoint dell'interfaccia di gestione, selezionare i VIP associati solo ai nodi di amministrazione.

3. Se hai selezionato **Interfacce nodo**, seleziona una o più interfacce nodo per ogni nodo di amministrazione o nodo gateway che desideri associare a questo endpoint.
4. Se hai selezionato **Tipo di nodo**, seleziona Nodi amministrativi, che include sia il nodo amministrativo primario che eventuali nodi amministrativi non primari, oppure Nodi gateway.

Controlla l'accesso degli inquilini



Un endpoint dell'interfaccia di gestione può controllare l'accesso del tenant solo quando l'endpoint ha [tipo di interfaccia di Tenant Manager](#).

Passi

1. Per il passaggio **Accesso tenant**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket. È necessario selezionare questa opzione se non è ancora stato creato alcun account tenant. Dopo aver aggiunto gli account tenant, puoi modificare l'endpoint del bilanciatore del carico per consentire o bloccare account specifici.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai propri bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

2. Se si crea un endpoint **HTTP**, non è necessario allegare un certificato. Selezionare **Crea** per aggiungere il nuovo endpoint del bilanciatore del carico. Poi vai a [Dopo aver finito](#). Altrimenti, seleziona **Continua** per allegare il certificato.

Allega il certificato

Passi

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 il servizio Load Balancer sui nodi di amministrazione o sui nodi gateway.

- **Carica il certificato.** Seleziona questa opzione se hai 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.** Selezionare questa opzione se si desidera utilizzare il certificato API S3 globale, che può essere utilizzato anche per le connessioni dirette ai nodi di archiviazione.

Non è possibile selezionare questa opzione a meno che non si sia sostituito il certificato API S3 predefinito, firmato dalla CA della griglia, con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere ["Configurare i certificati API S3"](#) .

- **Utilizzare il certificato dell'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 di amministrazione.

2. Se non si utilizza il certificato StorageGRID S3, caricare o generare il certificato.

Carica il certificato

- a. Seleziona **Carica certificato**.
- b. Carica i file del certificato del server richiesti:
 - **Certificato del server**: file del certificato del server personalizzato in codifica PEM.
 - **Chiave privata del certificato**: file della chiave privata del certificato del server personalizzato(`.key`).



Le chiavi private EC devono essere di 224 bit o più grandi. Le chiavi private RSA devono essere di 2048 bit o più grandi.

- **Bundle CA**: un singolo file facoltativo contenente i certificati di ciascuna autorità di certificazione (CA) emittente intermedia. Il file dovrebbe contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.
- c. Espandi **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se hai caricato un bundle CA facoltativo, ogni certificato verrà visualizzato in una scheda separata.
 - Selezionare **Scarica certificato** per salvare il file del certificato oppure selezionare **Scarica bundle CA** per salvare il bundle del certificato.

Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM** per copiare il contenuto del certificato e incollarlo altrove.
- d. Seleziona **Crea**. + L'endpoint del bilanciatore del carico è stato creato. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 o l'interfaccia di gestione e l'endpoint.

Genera certificato

- a. Seleziona **Genera certificato**.
- b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completamente qualificati da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
Proprietà intellettuale	Uno o più indirizzi IP da includere nel certificato.
Oggetto (facoltativo)	Soggetto X.509 o nome distinto (DN) del proprietario del certificato. Se non viene immesso alcun valore in questo campo, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.

Campo	Descrizione
Giorni validi	Numero di giorni dopo la creazione in cui scade il certificato.
Aggiungi estensioni di utilizzo delle chiavi	Se selezionata (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e per l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

- Selezionare **Scarica certificato** per salvare il file del certificato.

Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.

e. Seleziona **Crea**.

L'endpoint del bilanciatore del carico è stato creato. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 o l'interfaccia di gestione e questo endpoint.

Dopo aver finito

Passi

1. Se si utilizza un DNS, assicurarsi che includa un record per associare il nome di dominio completo (FQDN) StorageGRID a ciascun indirizzo IP che i client utilizzeranno per effettuare le connessioni.

L'indirizzo IP immesso nel record DNS varia a seconda che si utilizzi un gruppo HA di nodi di bilanciamento del carico:

- Se hai 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 StorageGRID Load Balancer utilizzando l'indirizzo IP di un nodo gateway o di un nodo amministrativo.

È inoltre necessario assicurarsi che il record DNS faccia riferimento a tutti i nomi di dominio degli endpoint richiesti, inclusi eventuali nomi jolly.

2. Fornire ai client S3 le informazioni necessarie per connettersi all'endpoint:

- Numero di porta

- Nome di dominio completo o indirizzo IP
- Eventuali dettagli del certificato richiesti

Visualizza e modifica gli endpoint del bilanciatore del carico

È possibile visualizzare i dettagli degli endpoint del bilanciatore 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 bilanciatore del carico, consultare le tabelle nella pagina Endpoint del bilanciatore del carico.
- Per visualizzare tutti i dettagli su 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.

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

Remove

Binding mode

Certificate

Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode

Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- Per modificare un endpoint, utilizzare il menu **Azioni** nella pagina Endpoint del bilanciatore 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 affinché le modifiche vengano applicate a tutti i nodi.

Compito	Menu Azioni	Pagina dei dettagli
Modifica il nome dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare Azioni > Modifica nome endpoint. c. Inserisci il nuovo nome. d. Seleziona Salva.	a. Selezionare il nome dell'endpoint per visualizzarne i dettagli. b. Seleziona l'icona di modifica  . c. Inserisci il nuovo nome. d. Seleziona Salva.
Modifica la porta dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Seleziona Azioni > Modifica porta endpoint c. Inserisci un numero di porta valido. d. Seleziona Salva.	<i>n / a</i>
Modifica la modalità di associazione dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare Azioni > Modifica modalità di associazione endpoint. c. Aggiornare la modalità di associazione secondo necessità. d. Seleziona Salva modifiche.	a. Selezionare il nome dell'endpoint per visualizzarne i dettagli. b. Selezionare Modifica modalità di rilegatura. c. Aggiornare la modalità di associazione secondo necessità. d. Seleziona Salva modifiche.
Modifica il certificato dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare Azioni > Modifica certificato endpoint. c. Carica o genera un nuovo certificato personalizzato oppure inizia a utilizzare il certificato S3 globale, a seconda delle necessità. d. Seleziona Salva modifiche.	a. Selezionare il nome dell'endpoint per visualizzarne i dettagli. b. Selezionare la scheda Certificato. c. Seleziona Modifica certificato. d. Carica o genera un nuovo certificato personalizzato oppure inizia a utilizzare il certificato S3 globale, a seconda delle necessità. e. Seleziona Salva modifiche.
Modifica l'accesso dell'inquilino	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare Azioni > Modifica accesso tenant. c. Scegli un'opzione di accesso diversa, seleziona o rimuovi gli inquilini dall'elenco oppure fai entrambe le cose. d. Seleziona Salva modifiche.	a. Selezionare il nome dell'endpoint per visualizzarne i dettagli. b. Selezionare la scheda Accesso inquilino. c. Seleziona Modifica accesso tenant. d. Scegli un'opzione di accesso diversa, seleziona o rimuovi gli inquilini dall'elenco oppure fai entrambe le cose. e. Seleziona Salva modifiche.

Rimuovere gli endpoint del bilanciatore del carico

È possibile rimuovere uno o più endpoint utilizzando il menu **Azioni** oppure è possibile rimuovere un singolo endpoint dalla pagina dei dettagli.



Per evitare interruzioni del client, aggiornare tutte le applicazioni client S3 interessate prima di rimuovere un endpoint del bilanciatore del carico. Aggiornare ciascun client per connettersi tramite una porta assegnata a un altro endpoint del bilanciatore del carico. Assicuratevi di aggiornare anche tutte le informazioni richieste sul certificato.



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. Nella pagina Bilanciatore del carico, seleziona la casella di controllo per ogni endpoint che desideri rimuovere.
 - b. Selezionare **Azioni > Rimuovi**.
 - c. Selezionare **OK**.
- Per rimuovere un endpoint dalla pagina dei dettagli:
 - a. Dalla pagina Bilanciatore del carico, seleziona il nome dell'endpoint.
 - b. Seleziona **Rimuovi** nella pagina dei dettagli.
 - c. Selezionare **OK**.

Configurare i nomi di dominio degli endpoint S3

Per supportare le richieste in stile S3 virtual-hosted, 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"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).
- Hai confermato che non è in corso alcun aggiornamento della rete.



Non apportare modifiche alla configurazione del nome di dominio quando è in corso un aggiornamento della griglia.

Informazioni su questo compito

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 cliente.

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 il nome alternativo del soggetto (SAN) 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 facciano riferimento a tutti i nomi di dominio degli endpoint S3 richiesti, inclusi eventuali nomi jolly.



I client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo gateway, di un nodo di amministrazione o di un nodo di archiviazione oppure connettendosi all'indirizzo IP virtuale di un gruppo ad alta disponibilità. È necessario comprendere come 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 di questi certificati:

- I client che si connettono a un endpoint del bilanciatore del carico possono utilizzare un certificato personalizzato per tale endpoint. Ogni endpoint del bilanciatore del carico può essere configurato per riconoscere diversi nomi di dominio degli endpoint S3.
- I client che si connettono a un endpoint del bilanciatore del carico o direttamente a un nodo di archiviazione possono personalizzare il certificato API S3 globale per includere tutti i nomi di dominio dell'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 S3 virtual-hosted è disabilitato.

Aggiungi un nome di dominio dell'endpoint S3

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Nomi di dominio endpoint S3**.
2. Inserisci il nome del dominio nel campo **Nome dominio 1**. Seleziona **Aggiungi un altro nome di dominio** per aggiungere altri nomi di dominio.
3. Seleziona **Salva**.
4. Assicurarsi che i certificati del server utilizzati dai client corrispondano ai nomi di dominio dell'endpoint S3 richiesti.
 - Se i client si connettono a un endpoint del bilanciatore del carico che utilizza il proprio certificato, "[aggiornare il certificato associato all'endpoint](#)".
 - Se i client si connettono a un endpoint del bilanciatore del carico che utilizza il certificato API S3 globale o direttamente ai nodi di archiviazione, "[aggiornare il certificato API S3 globale](#)".
5. Aggiungere i record DNS necessari per garantire che le richieste di 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 dell'endpoint S3

Se si modifica un nome utilizzato dalle applicazioni S3, le richieste in stile virtual-hosted non riusciranno.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Nomi di dominio endpoint S3**.
2. Seleziona il campo del nome di dominio che desideri modificare e apporta le modifiche necessarie.
3. Seleziona **Salva**.
4. Seleziona **Sì** per confermare la modifica.

Elimina un nome di dominio dell'endpoint S3

Se si rimuove un nome utilizzato dalle applicazioni S3, le richieste in stile virtual-hosted non riusciranno.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Nomi di dominio endpoint S3**.
2. Seleziona l'icona Elimina  accanto al nome di dominio.
3. Selezionare **Sì** per confermare l'eliminazione.

Informazioni correlate

- ["Utilizzare l'API REST S3"](#)
- ["Visualizza gli indirizzi IP"](#)
- ["Configurare gruppi ad alta disponibilità"](#)

Riepilogo: indirizzi IP e porte per le connessioni client

Per archiviare o recuperare oggetti, le applicazioni client S3 si connettono al servizio Load Balancer, incluso in tutti i nodi amministrativi e gateway, oppure al servizio Local Distribution Router (LDR), incluso in tutti i nodi di archiviazione.

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo della griglia e il numero di porta del servizio su quel 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) anziché 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 hai già creato endpoint del bilanciatore del carico e gruppi ad alta disponibilità (HA), vedi [Dove trovare gli indirizzi IP](#) per individuare questi valori nel Grid Manager.

Dove avviene la connessione	Servizio a cui il client si connette	indirizzo IP	Porta
gruppo HA	Bilanciatore del carico	Indirizzo IP virtuale di un gruppo HA	Porta assegnata all'endpoint del bilanciatore del carico

Dove avviene la connessione	Servizio a cui il client si connette	Indirizzo IP	Porta
Nodo di amministrazione	Bilanciatore del carico	Indirizzo IP del nodo di amministrazione	Porta assegnata all'endpoint del bilanciatore del carico
Nodo Gateway	Bilanciatore del carico	Indirizzo IP del nodo gateway	Porta assegnata all'endpoint del bilanciatore del carico
Nodo di archiviazione	Relazione a distanza	Indirizzo IP del nodo di archiviazione	Porte S3 predefinite: • HTTPS: 18082 • HTTP: 18084

URL di esempio

Per connettere un'applicazione client all'endpoint del 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 bilanciatore 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. Sign in a Grid Manager utilizzando un ["browser web supportato"](#).
2. Per trovare l'indirizzo IP di un nodo della griglia:
 - a. Selezionare **NODES**.
 - b. Selezionare il nodo di amministrazione, il nodo gateway o il nodo di archiviazione a cui si desidera connettersi.
 - c. Selezionare la scheda **Panoramica**.
 - d. Nella sezione Informazioni sul nodo, annotare gli indirizzi IP del nodo.
 - e. Selezionare **Mostra altro** per visualizzare gli indirizzi IPv6 e le mappature delle interfacce.

È possibile stabilire connessioni dalle applicazioni client a uno qualsiasi degli indirizzi IP nell'elenco:

- **eth0**: Rete di griglia
- **eth1**: Rete di amministrazione (facoltativo)
- **eth2**: Rete client (facoltativo)



Se si visualizza un nodo di amministrazione o un nodo gateway ed è il nodo attivo in 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 **CONFIGURAZIONE > Rete > Gruppi ad alta disponibilità**.
 - b. Nella tabella, annotare l'indirizzo IP virtuale del gruppo HA.
4. Per trovare il numero di porta di un endpoint del Load Balancer:
 - a. Selezionare **CONFIGURAZIONE > Rete > Endpoint del bilanciatore del carico**.
 - 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, perché tali porte sono riservate sui nodi amministrativi. Tutte le altre porte sono configurate sia sui nodi gateway che sui nodi amministrativi.

- c. Selezionare il nome dell'endpoint dalla tabella.
- d. Verificare che il **Tipo di client** (S3) corrisponda all'applicazione client che utilizzerà l'endpoint.

Gestire reti e connessioni

Configurare le impostazioni di rete

È possibile configurare varie impostazioni di rete da Grid Manager per ottimizzare il funzionamento del sistema StorageGRID .

Configurare le interfacce VLAN

Puoi ["creare interfacce LAN virtuali \(VLAN\)"](#) per isolare e partizionare il traffico per garantire sicurezza, flessibilità e prestazioni. Ogni interfaccia VLAN è associata a una o più interfacce padre sui nodi amministrativi e sui nodi gateway. È possibile utilizzare le interfacce VLAN nei gruppi HA e negli endpoint del bilanciatore del carico per separare il traffico client o amministrativo in base all'applicazione o al tenant.

Politiche di classificazione del traffico

Puoi usare ["politiche di classificazione del traffico"](#) per identificare e gestire diversi tipi di traffico di rete, incluso il traffico correlato a bucket, tenant, subnet client o endpoint del bilanciatore del carico specifici. Queste politiche possono aiutare a limitare e monitorare il 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"](#) per imparare a connettere i client S3.

Reti StorageGRID predefinite

Per impostazione predefinita, StorageGRID supporta tre interfacce di rete per nodo della griglia, consentendo di configurare la rete per ogni singolo nodo della griglia in base ai requisiti di sicurezza e accesso.

Per ulteriori informazioni sulla topologia di rete, vedere ["Linee guida per il networking"](#) .

Rete a griglia

Necessario. La rete Grid viene utilizzata per tutto il traffico StorageGRID interno. Fornisce connettività tra tutti i nodi della griglia, in tutti i siti e le sottoreti.

Rete di amministrazione

Opzionale. La rete di amministrazione viene solitamente 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 clienti

Opzionale. La rete client è una rete aperta solitamente utilizzata per fornire accesso alle applicazioni client S3, 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 della griglia non può avere più di un'interfaccia su una rete.
- È supportato un singolo gateway per rete, per nodo della griglia, che deve trovarsi sulla stessa subnet del nodo. Se necessario, è possibile implementare un routing più complesso nel gateway.
- Su ogni nodo, ogni rete è mappata su un'interfaccia di rete specifica.

Rete	Nome dell'interfaccia
Griglia	eth0
Amministratore (facoltativo)	eth1
Cliente (facoltativo)	eth2

- Se il nodo è connesso a un dispositivo StorageGRID , per ogni rete vengono utilizzate porte specifiche. Per maggiori dettagli, consultare le istruzioni di installazione dell'elettrodomestico.
- Il percorso predefinito viene generato automaticamente, per nodo. Se eth2 è abilitato, 0.0.0.0/0 utilizza la rete client su eth2. Se eth2 non è abilitato, 0.0.0.0/0 utilizza la rete Grid su eth0.
- La rete client non diventa operativa finché il nodo della griglia non si è unito alla griglia
- La rete di amministrazione può essere configurata durante la distribuzione del nodo della griglia per consentire l'accesso all'interfaccia utente di installazione prima che la griglia sia completamente installata.

Interfacce opzionali

Facoltativamente, è possibile aggiungere interfacce extra a un nodo. Ad esempio, potresti voler aggiungere un'interfaccia trunk a un nodo di amministrazione o gateway, in modo da poter utilizzare ["Interfacce VLAN"](#) per separare il traffico appartenente a diverse applicazioni o tenant. Oppure, potresti voler aggiungere un'interfaccia di accesso da utilizzare in un ["gruppo ad alta disponibilità \(HA\)"](#) .

Per aggiungere interfacce trunk o di accesso, vedere quanto segue:

- **VMware (dopo l'installazione del nodo):** ["VMware: aggiungi trunk o interfacce di accesso 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: aggiungere interfacce trunk o di accesso a un nodo"](#)

Visualizza 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 della griglia tramite la riga di comando ed eseguire varie procedure di manutenzione.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

Informazioni su questo compito

Per informazioni sulla modifica degli indirizzi IP, vedere ["Configurare gli indirizzi IP"](#) .

Passi

1. Selezionare **NODI > *nodo griglia* > Panoramica**.
2. Selezionare **Mostra altro** a destra del titolo Indirizzi IP.

Gli indirizzi IP per quel nodo della griglia sono elencati in una tabella.

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used:

Object data		7%	?
Object metadata		5%	?

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ⌵	IP address ⌵
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name ⌵	Severity ? ⌵	Time triggered ⌵	Current values
ILM placement unachievable 🔗	 Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

Configurare le interfacce VLAN

È possibile creare interfacce LAN virtuali (VLAN) sui nodi di amministrazione e sui nodi gateway e utilizzarle nei gruppi HA e negli endpoint del bilanciatore del carico per isolare e partizionare il traffico per garantire sicurezza, flessibilità e prestazioni. I nodi selezionati nel gruppo HA possono utilizzare le interfacce VLAN per condividere fino a 10 indirizzi IP virtuali, in modo che se un nodo si guasta, un altro nodo subentri nel traffico da e verso gli indirizzi IP virtuali.

Considerazioni sulle interfacce VLAN

- Per creare un'interfaccia VLAN, immettere un ID VLAN e scegliere un'interfaccia padre su uno o più nodi.
- Un'interfaccia padre deve essere configurata come interfaccia trunk sullo switch.

- Un'interfaccia padre può essere la rete Grid (eth0), la rete client (eth2) o un'interfaccia trunk aggiuntiva per la VM o l'host bare-metal (ad esempio, ens256).
- Per ogni interfaccia VLAN, è possibile selezionare solo un'interfaccia padre per un dato nodo. Ad esempio, non è possibile utilizzare sia l'interfaccia Grid Network che l'interfaccia Client Network sullo stesso Gateway Node come interfaccia padre per la stessa VLAN.
- Se l'interfaccia VLAN è destinata al traffico del nodo amministrativo, che include il traffico relativo al Grid Manager e al Tenant Manager, selezionare le interfacce solo sui nodi amministrativi.
- Se l'interfaccia VLAN è destinata al traffico client S3, selezionare le interfacce sui nodi amministrativi o sui nodi gateway.
- Se è necessario aggiungere interfacce trunk, vedere quanto segue per i dettagli:
 - **VMware (dopo l'installazione del nodo):** ["VMware: aggiungi trunk o interfacce di accesso 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: aggiungere interfacce trunk o di accesso a un nodo"](#)

Creare un'interfaccia VLAN

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).
- Un'interfaccia trunk è stata configurata nella rete e collegata alla VM o al nodo Linux. Conosci il nome dell'interfaccia trunk.
- Conosci l'ID della VLAN che stai configurando.

Informazioni su questo compito

L'amministratore di rete potrebbe aver configurato una o più interfacce trunk e una o più VLAN per separare il traffico client o amministrativo appartenente a diverse applicazioni o tenant. Ogni VLAN è identificata da un ID numerico o 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, si specifica l'ID VLAN e si selezionano le interfacce padre (trunk) su uno o più nodi.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Interfacce VLAN**.
2. Seleziona **Crea**.

Inserisci i dettagli per le interfacce VLAN

Passi

1. Specificare l'ID della VLAN nella rete. È possibile immettere qualsiasi 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, immettere una breve descrizione per l'interfaccia VLAN.
3. Selezionare **Continua**.

Scegli le interfacce padre

Nella tabella sono elencate le interfacce disponibili per tutti i nodi amministrativi e i nodi gateway in ciascun sito della griglia. Le interfacce Admin Network (eth1) non possono essere utilizzate come interfacce padre e non vengono visualizzate.

Passi

1. Selezionare una o più interfacce padre a cui collegare questa VLAN.

Ad esempio, potresti voler collegare una VLAN all'interfaccia Client Network (eth2) per un Gateway Node e un Admin Node.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

	Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?
☐	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
☒	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
☐	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
☒	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
☐	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

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

2. Selezionare **Continua**.

Conferma le impostazioni

Passi

1. Rivedere la configurazione e apportare eventuali modifiche.
 - Se devi modificare l'ID o la descrizione della VLAN, seleziona **Inserisci dettagli VLAN** nella parte superiore della pagina.
 - Se devi modificare un'interfaccia padre, seleziona **Scegli interfacce padre** nella parte superiore della pagina oppure seleziona **Precedente**.

- Se devi rimuovere un'interfaccia padre, seleziona il cestino  .

2. Seleziona **Salva**.

3. Attendere fino a 5 minuti affinché la nuova interfaccia venga visualizzata come selezione nella pagina Gruppi ad alta disponibilità e venga elencata nella tabella **Interfacce di rete** per il nodo (**NODI > nodo interfaccia padre > Rete**).

Modifica 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, potresti voler rimuovere un'interfaccia padre da un'interfaccia VLAN se intendi dismettere il nodo associato.

Notare 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, supponiamo 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.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Interfacce VLAN**.
2. Selezionare la casella di controllo relativa all'interfaccia VLAN che si desidera modificare. Quindi, seleziona **Azioni > Modifica**.
3. Facoltativamente, aggiorna l'ID VLAN o la descrizione. Quindi, seleziona **Continua**.

Non è possibile aggiornare un ID VLAN se la VLAN viene utilizzata in un gruppo HA.

4. Facoltativamente, seleziona o deseleziona le caselle di controllo per aggiungere interfacce padre o per rimuovere interfacce non utilizzate. Quindi, seleziona **Continua**.
5. Rivedere la configurazione e apportare eventuali modifiche.
6. Seleziona **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. Prima di poter rimuovere l'interfaccia VLAN dal gruppo HA, è necessario rimuoverla.

Per evitare interruzioni nel traffico dei clienti, si consiglia di effettuare 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 l'interfaccia 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 primaria, quindi rimuovere la vecchia interfaccia dal gruppo HA. Infine, eliminare l'interfaccia VLAN su quel nodo.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Interfacce VLAN**.
2. Selezionare la casella di controllo per ogni interfaccia VLAN che si desidera rimuovere. Quindi, seleziona **Azioni > Elimina**.
3. Selezionare **Sì** per confermare la selezione.

Tutte le interfacce VLAN selezionate verranno rimosse. Nella pagina delle interfacce VLAN viene visualizzato un banner verde di successo.

Gestire le policy di classificazione del traffico

Quali sono le politiche di classificazione del traffico?

Le policy di classificazione del traffico consentono di identificare e monitorare diversi tipi di traffico di rete. Queste policy possono aiutare a limitare e monitorare il traffico per migliorare le offerte di qualità del servizio (QoS).

I criteri di classificazione del traffico vengono applicati agli endpoint del servizio StorageGRID Load Balancer per i nodi gateway e i nodi amministrativi. Per creare policy di classificazione del traffico, è necessario aver già creato gli endpoint del bilanciatore del carico.

Regole di corrispondenza

Ogni criterio di classificazione del traffico contiene una o più regole di corrispondenza per identificare il traffico di rete correlato a una o più delle seguenti entità:

- Secchi
- Sottorete
- Inquilino
- Endpoint del bilanciatore del carico

StorageGRID monitora il traffico che corrisponde a qualsiasi regola all'interno della policy in base agli obiettivi della regola. Tutto il traffico che corrisponde a una regola di una policy viene gestito da quella policy. Al contrario, è possibile impostare regole in modo che corrispondano a tutto il traffico, ad eccezione di un'entità specificata.

Limitazione del traffico

Facoltativamente, è possibile aggiungere i seguenti tipi di limite a una policy:

- Larghezza di banda aggregata
- Larghezza di banda per richiesta
- Richieste simultanee
- Richiedi tariffa

I valori limite vengono applicati in base al bilanciatore del carico. Se il traffico viene distribuito simultaneamente su più bilanciatori del carico, le tariffe massime totali sono un multiplo dei limiti di tariffa 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 aggregati di larghezza di banda potrebbero avere un impatto minore aggiuntivo sulle prestazioni del traffico non limitato.

Per i limiti di larghezza di banda aggregati o per richiesta, le richieste vengono trasmesse in entrata o in uscita alla velocità impostata. StorageGRID può imporre una sola velocità, quindi viene applicata la corrispondenza più specifica della policy, in base al tipo di matcher. La larghezza di banda consumata dalla richiesta non viene conteggiata in relazione ad altre policy di corrispondenza meno specifiche contenenti policy di limite di larghezza di banda aggregate. Per tutti gli altri tipi di limite, le richieste dei client vengono ritardate di 250 millisecondi e ricevono una risposta 503 Slow Down per le richieste che superano qualsiasi limite di policy corrispondente.

In Grid Manager puoi visualizzare i grafici del traffico e verificare che le policy applichino i limiti di traffico previsti.

Utilizzare criteri di classificazione del traffico con SLA

È possibile utilizzare criteri di classificazione del traffico insieme ai limiti di capacità e alla protezione dei dati per applicare accordi sul livello di servizio (SLA) che forniscono specifiche per capacità, protezione dei dati e prestazioni.

L'esempio seguente mostra tre livelli di un SLA. È possibile creare criteri di classificazione del traffico per raggiungere gli obiettivi prestazionali di ciascun livello SLA.

Livello di servizio	Capacità	Protezione dei dati	Massima prestazione consentita	Costo
Oro	1 PB di spazio di archiviazione consentito	Regola ILM a 3 copie	25 K richieste/sec Larghezza di banda 5 GB/sec (40 Gbps)	\$\$\$ al mese
Argento	250 TB di spazio di archiviazione consentito	Regola ILM a 2 copie	10 K richieste/sec Larghezza di banda 1,25 GB/sec (10 Gbps)	\$\$ al mese
Bronzo	100 TB di spazio di archiviazione consentito	Regola ILM a 2 copie	5 K richieste/sec Larghezza di banda di 1 GB/sec (8 Gbps)	\$ al mese

Creare criteri di classificazione del traffico

È possibile creare criteri di classificazione del traffico se si desidera monitorare e,

facoltativamente, limitare il traffico di rete in base a bucket, espressione regolare del bucket, 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 frequenza delle richieste.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .
- Hai creato tutti gli endpoint del bilanciamento del carico che desideri abbinare.
- Hai creato tutti gli inquilini che desideri abbinare.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.
2. Seleziona **Crea**.
3. Inserisci un nome e una descrizione (facoltativa) per la policy e seleziona **Continua**.

Ad esempio, descrivi a cosa si applica questa politica di classificazione del traffico e cosa limiterà.

4. Selezionare **Aggiungi regola** e specificare i seguenti dettagli per creare una o più regole corrispondenti per il criterio. Ogni policy creata dovrebbe avere almeno una regola corrispondente. Selezionare **Continua**.

Campo	Descrizione
Tipo	Seleziona i tipi di traffico a cui si applica la regola di corrispondenza. I tipi di traffico sono bucket, bucket regex, CIDR, endpoint del bilanciamento del carico e tenant.
Valore della corrispondenza	Immettere il valore corrispondente al tipo selezionato. • Bucket: inserisci uno o più nomi di bucket. • Espressione regolare bucket: inserisci una o più espressioni regolari utilizzate per trovare una corrispondenza con un set di nomi di bucket. L'espressione regolare non è ancorata. Utilizzare l'ancoraggio ^ per la corrispondenza all'inizio del nome del bucket e l'ancoraggio \$ per la corrispondenza alla fine del nome. La corrispondenza delle espressioni regolari supporta un sottoinsieme della sintassi PCRE (espressione regolare compatibile con Perl). • CIDR: immettere una o più subnet IPv4, in notazione CIDR, che corrispondano alla subnet desiderata. • Endpoint del bilanciamento del carico: seleziona un nome per l'endpoint. Questi sono gli endpoint del bilanciamento del carico definiti su "Configurare gli endpoint del bilanciamento del carico" . • Tenant: la corrispondenza del tenant utilizza l'ID della chiave di accesso. Se la richiesta non contiene un ID chiave di accesso (ad esempio, accesso anonimo), la proprietà del bucket a cui si accede viene utilizzata per determinare il tenant.

Campo	Descrizione
Corrispondenza inversa	Se si desidera far corrispondere tutto il traffico di rete <i>eccetto</i> il traffico coerente con il Tipo e il Valore di corrispondenza appena definiti, selezionare la casella di controllo Corrispondenza inversa. In caso contrario, lasciare la casella di controllo deselezionata. Ad esempio, se si desidera che questo criterio venga applicato a tutti gli endpoint del bilanciatore del carico tranne uno, specificare l'endpoint del bilanciatore del carico da escludere e selezionare Corrispondenza inversa. Per una policy contenente più matcher, di cui almeno uno è un matcher inverso, fare attenzione a non creare una policy che corrisponda a tutte le richieste.

5. Facoltativamente, seleziona **Aggiungi un limite** e seleziona i seguenti dettagli per aggiungere uno o più limiti per controllare il traffico di rete corrispondente 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 a cui corrisponde la regola. Ad esempio, è possibile limitare la larghezza di banda o la velocità delle richieste. 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 è in uso la larghezza di banda aggregata, la larghezza di banda per richiesta non è disponibile. Al contrario, quando è in uso la larghezza di banda per richiesta, la larghezza di banda aggregata non è disponibile. I limiti aggregati di larghezza di banda potrebbero avere un impatto minore aggiuntivo sulle prestazioni del 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 è presente traffico che corrisponde a policy aggiuntive che hanno limiti di larghezza di banda. StorageGRID implementa le corrispondenze "migliori" per i limiti di larghezza di banda nel seguente ordine: • Indirizzo IP esatto (maschera /32) • Nome esatto del bucket • Espressione regolare del bucket • Inquilino • Punto finale • Corrispondenze CIDR non esatte (non /32) • Corrispondenze inverse

Campo	Descrizione
Si applica a	Se questo limite si applica alle richieste di lettura del client (GET o HEAD) o alle richieste di scrittura (PUT, POST o DELETE).
Valore	Valore a cui verrà limitato il traffico di rete, in base all'unità selezionata. Ad esempio, immettere 10 e selezionare MiB/s per impedire che il traffico di rete a cui corrisponde questa regola superi i 10 MiB/s. Nota: a seconda delle impostazioni delle unità, le unità disponibili saranno binarie (ad esempio, GiB) o decimali (ad esempio, GB). Per modificare l'impostazione delle unità, seleziona il menu a discesa dell'utente in alto a destra di Grid Manager, quindi seleziona 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 politica di classificazione del traffico. Utilizzare il pulsante **Precedente** per tornare indietro e apportare le modifiche desiderate. Quando sei soddisfatto della policy, seleziona **Salva e continua**.

Il traffico del client S3 viene ora gestito in base alla politica di classificazione del traffico.

Dopo aver finito

["Visualizza le metriche del traffico di rete"](#) per verificare che le norme rispettino i limiti di traffico previsti.

Modifica la politica di classificazione del traffico

È possibile modificare una policy di classificazione del traffico per cambiarne il nome o la descrizione oppure per creare, modificare o eliminare regole o limiti per la policy.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti sono elencati in una tabella.

2. Modifica la policy utilizzando il menu Azioni o la pagina dei dettagli. Vedere ["creare politiche di classificazione del traffico"](#) per cosa inserire.

Menu Azioni

- a. Selezionare la casella di controllo per la policy.
- b. Selezionare **Azioni > Modifica**.

Pagina dei dettagli

- a. Selezionare il nome della policy.
- b. Selezionare il pulsante **Modifica** accanto al nome della policy.

3. Per il passaggio Inserisci nome criterio, modifica facoltativamente il nome o la descrizione del criterio e seleziona **Continua**.
4. Per il passaggio Aggiungi regole di corrispondenza, aggiungere facoltativamente una regola o modificare il **Tipo** e il **Valore di corrispondenza** della regola esistente, quindi selezionare **Continua**.
5. Per il passaggio Imposta limiti, puoi aggiungere, modificare o eliminare un limite e selezionare **Continua**.
6. Rivedi la policy aggiornata e seleziona **Salva e continua**.

Le modifiche apportate alla policy vengono salvate e il traffico di rete viene ora gestito in base alle policy di classificazione del traffico. Puoi visualizzare i grafici del traffico e verificare che le norme rispettino i limiti di traffico previsti.

Eliminare una policy di classificazione del traffico

È possibile eliminare una policy di classificazione del traffico se non ne hai più bisogno. Assicurati di eliminare la policy corretta perché una policy eliminata non può essere recuperata.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[Permesso di accesso root](#)".

Passi

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 la policy utilizzando il menu Azioni o la pagina dei dettagli.

Menu Azioni

- a. Selezionare la casella di controllo per la policy.
- b. Selezionare **Azioni > Rimuovi**.

Pagina dei dettagli della politica

- a. Selezionare il nome della policy.
- b. Selezionare il pulsante **Rimuovi** accanto al nome della policy.

3. Selezionare **Sì** per confermare che si desidera eliminare il criterio.

La politica è stata eliminata.

Visualizza 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"](#).
- Tu hai il ["Accesso root o autorizzazione account tenant"](#).

Informazioni su questo compito

Per qualsiasi policy di classificazione del traffico esistente, è possibile visualizzare le metriche per il servizio di bilanciamento del carico per determinare se la policy sta limitando correttamente il traffico sulla rete. I dati nei grafici possono aiutarti a stabilire se è necessario modificare la polizza.

Anche se non vengono stabiliti limiti per una politica di classificazione del traffico, vengono raccolte metriche e i grafici forniscono informazioni utili per comprendere le tendenze del traffico.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti sono 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 della politica di classificazione del traffico. I grafici mostrano le metriche solo per il traffico che corrisponde alla policy selezionata.

Nella pagina sono inclusi i seguenti grafici.

- Frequenza delle richieste: questo grafico fornisce la quantità di larghezza di banda corrispondente a questa policy gestita da tutti i bilanciatori del carico. I dati ricevuti includono le intestazioni delle richieste per tutte le richieste e le dimensioni dei dati del corpo per le risposte che contengono dati del corpo. Inviato include le intestazioni di risposta per tutte le richieste e le dimensioni dei dati del corpo della risposta per le richieste che includono dati del corpo nella risposta.



Una volta completate le richieste, questo grafico mostra solo l'utilizzo della larghezza di banda. Per 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 frequenza approssimativa con cui le richieste che corrispondono a questa policy restituiscono errori (codice di stato HTTP ≥ 400) ai client.
- Durata media della richiesta (senza errori): questo grafico fornisce la durata media delle richieste riuscite che corrispondono a questa policy.
- Utilizzo della larghezza di banda della policy: questo grafico mostra la quantità di larghezza di banda corrispondente a questa policy gestita da tutti i bilanciatori del carico. I dati ricevuti includono le intestazioni delle richieste per tutte le richieste e le dimensioni dei dati del corpo per le risposte che

contengono dati del corpo. Inviato include le intestazioni di risposta per tutte le richieste e le dimensioni dei dati del corpo della risposta per le richieste che includono dati del corpo nella risposta.

4. Posiziona il cursore su un grafico a linee per visualizzare una finestra pop-up con i valori relativi a una parte specifica del grafico.
5. Selezionare **Dashboard Grafana** subito sotto il titolo Metriche per visualizzare tutti i grafici relativi a una policy. Oltre ai quattro grafici della scheda **Metriche**, puoi visualizzare altri due grafici:
 - Frequenza delle richieste di scrittura in base alle dimensioni dell'oggetto: frequenza delle richieste PUT/POST/DELETE che corrispondono a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le tariffe mostrate nella vista hover vengono troncate a conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
 - Frequenza delle richieste di lettura in base alle dimensioni dell'oggetto: frequenza delle richieste GET/HEAD che corrispondono a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le tariffe mostrate nella vista hover vengono troncate a conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
6. In alternativa, è possibile accedere ai grafici dal menu **SUPPORTO**.
 - a. Selezionare **SUPPORTO > Strumenti > Metriche**.
 - b. Selezionare **Politica di classificazione del traffico** dalla sezione **Grafana**.
 - c. Selezionare la policy dal menu in alto a sinistra della pagina.
 - d. Posiziona il cursore su un grafico per visualizzare un pop-up che mostra la data e l'ora del campione, le dimensioni degli oggetti aggregati nel conteggio e il numero di richieste al secondo durante quel periodo di tempo.

Le policy di classificazione del traffico sono identificate dal loro ID. Gli ID dei criteri sono elencati nella pagina Criteri di classificazione del traffico.
7. Analizza i grafici per determinare la frequenza con cui la policy limita il traffico e se è necessario modificarla.

Cifrature supportate per le connessioni TLS in uscita

Il sistema StorageGRID supporta un set limitato di suite di crittografia per le connessioni Transport Layer Security (TLS) ai sistemi esterni utilizzati per la federazione delle identità e i pool di archiviazione 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 archiviazione cloud.

I cifrari TLS supportati per l'uso con sistemi esterni sono stati selezionati per garantire la compatibilità con una vasta gamma di sistemi esterni. L'elenco è più lungo dell'elenco dei cifrari supportati per l'uso con le applicazioni client S3. Per configurare i cifrari, vai su **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza** e seleziona **Criteri TLS e SSH**.



Le opzioni di configurazione TLS, quali versioni del protocollo, cifrature, algoritmi di scambio di chiavi e algoritmi MAC, non sono configurabili in StorageGRID. Per richieste specifiche su queste impostazioni, contattare il rappresentante dell'account 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 ci siano 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

Vantaggi di mantenere aperte le connessioni HTTP inattive

È opportuno 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, dovresti mantenere aperta una connessione HTTP inattiva per un massimo di 10 minuti. StorageGRID potrebbe chiudere automaticamente una connessione HTTP mantenuta 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 determina di dover eseguire una transazione HTTP al momento in cui il sistema StorageGRID può eseguire la transazione

Il vantaggio principale è la latenza ridotta, soprattutto per quanto riguarda il tempo necessario per stabilire connessioni TCP/IP e TLS.

- Aumento della velocità di trasferimento dati mediante l'attivazione dell'algoritmo di avvio lento TCP/IP con 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 vantaggi 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 archiviazione, è opportuno limitare la durata di una connessione HTTP attiva a un massimo di 10 minuti, anche se la connessione HTTP esegue continuamente transazioni.

Determinare la durata massima per cui una connessione deve rimanere aperta è un compromesso tra i vantaggi della persistenza della connessione e l'allocazione ideale della connessione alle risorse del sistema interno.

Per le connessioni client ai nodi di archiviazione, la limitazione delle connessioni HTTP attive offre i seguenti vantaggi:

- Consente un bilanciamento ottimale del carico nel sistema StorageGRID .

Nel tempo, una connessione HTTP potrebbe non essere più ottimale poiché cambiano i requisiti di bilanciamento del carico. Il sistema ottiene il miglior bilanciamento del carico quando le applicazioni client stabiliscono una connessione HTTP separata per ogni transazione, ma ciò annulla i vantaggi 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 iniziano solo dopo il completamento di tutte le connessioni HTTP in corso.

Per le connessioni client al servizio Load Balancer, limitare la 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 volerci diversi minuti prima che le connessioni attive vengano terminate automaticamente.

Vantaggi delle connessioni HTTP simultanee

È consigliabile mantenere aperte più connessioni TCP/IP al sistema StorageGRID per consentire il parallelismo, che aumenta le prestazioni. 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, senza dover attendere il completamento di altre transazioni.

- Aumento della produttività

Il sistema StorageGRID può eseguire transazioni parallele e aumentare la produttività complessiva delle transazioni.

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 stia elaborando una transazione.

Ogni topologia del sistema StorageGRID presenta un throughput di picco diverso per transazioni e connessioni simultanee prima che le prestazioni inizino a peggiorare. La velocità massima di elaborazione dipende da fattori quali risorse di elaborazione, risorse di rete, risorse di archiviazione e collegamenti WAN. Anche il numero di server e servizi e il numero di applicazioni supportate dal sistema StorageGRID sono fattori da considerare.

I sistemi StorageGRID spesso supportano più applicazioni client. È opportuno tenerlo presente quando si determina il numero massimo di connessioni simultanee utilizzate da un'applicazione client. Se l'applicazione client è composta da più entità software, ciascuna delle quali stabilisce connessioni al sistema StorageGRID, è necessario sommare tutte le connessioni tra le entità. Potrebbe essere necessario modificare il numero massimo di connessioni simultanee nelle seguenti situazioni:

- La topologia del sistema StorageGRID influisce sul numero massimo di transazioni e connessioni simultanee che il sistema può supportare.
- 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 connessioni 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 pool da utilizzare per ciascuna. Pool separati di connessioni HTTP consentono di controllare meglio le transazioni e bilanciare i carichi.

Le applicazioni client possono creare carichi che sono dominanti nel recupero (lettura) o dominanti nello stoccaggio (scrittura). Grazie a pool separati di connessioni HTTP per le transazioni di lettura e scrittura, è possibile definire la quantità di ciascun pool da dedicare alle transazioni di lettura o scrittura.

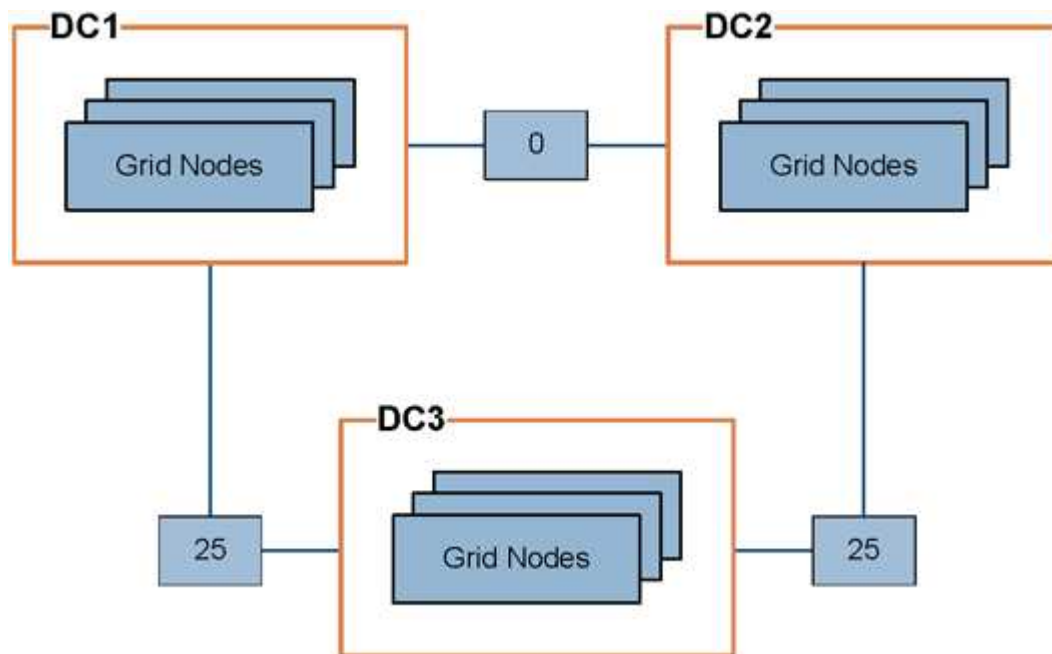
Gestire i costi dei link

I costi di collegamento consentono di stabilire la priorità del sito del data center che fornisce un servizio richiesto quando sono presenti due o più siti del data center. È possibile adattare i costi dei collegamenti in base alla latenza tra i siti.

Quali sono i costi dei link?

- I costi di collegamento vengono utilizzati per stabilire la priorità della copia dell'oggetto da utilizzare per completare i recuperi dell'oggetto.
- I costi dei collegamenti vengono utilizzati dall'API di gestione della griglia e dall'API di gestione dei tenant per determinare quali servizi StorageGRID interni utilizzare.
- I costi di collegamento vengono utilizzati dal servizio Load Balancer sui nodi amministrativi e sui nodi gateway per indirizzare le connessioni client. Vedere ["Considerazioni sul bilanciamento del carico"](#).

Il diagramma mostra una griglia a tre siti in cui sono configurati i costi di collegamento tra i siti:



- Il servizio Load Balancer sui nodi amministrativi e sui nodi gateway distribuisce equamente le connessioni client a tutti i nodi di archiviazione nello stesso sito del data center e a tutti i siti del data center con un costo di collegamento pari a 0.

Nell'esempio, un nodo gateway nel sito del data center 1 (DC1) distribuisce equamente le connessioni

client ai nodi di archiviazione in DC1 e ai nodi di archiviazione in DC2. Un nodo gateway in DC3 invia connessioni client solo ai nodi di archiviazione in DC3.

- Quando si recupera un oggetto che esiste in più copie replicate, StorageGRID recupera la copia nel data center che ha il costo di collegamento più basso.

Nell'esempio, se un'applicazione client su DC2 recupera un oggetto archiviato sia su DC1 che su DC3, l'oggetto viene recuperato da DC1, perché il costo del collegamento da DC1 a DC2 è 0, che è inferiore al costo del collegamento da DC3 a DC2 (25).

I costi dei collegamenti sono numeri relativi arbitrari, senza un'unità di misura specifica. Ad esempio, un costo di collegamento pari a 50 viene utilizzato in modo meno preferenziale rispetto a un costo di collegamento pari a 25. La tabella mostra i costi dei link più comunemente utilizzati.

Collegamento	Costo del collegamento	Note
Tra i siti fisici dei data center	25 (predefinito)	Data center collegati tramite collegamento WAN.
Tra siti di data center logici nella stessa posizione fisica	0	Data center logici nello stesso edificio fisico o campus collegati tramite una LAN.

Aggiorna i costi dei link

È possibile aggiornare i costi di collegamento tra i siti dei data center per riflettere la latenza tra i siti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di configurazione della pagina della topologia della griglia"](#) .

Passi

1. Seleziona **SUPPORTO > Altro > Costo del collegamento**.



Link Cost

Updated: 2023-02-15 18:09:28 MST

Site Names (1 - 3 of 3)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Show Records Per Page

Previous
« 1 » Next

Link Costs

Link Source	Link Destination			Actions
	10	20	30	
Data Center 1	0	25	25	



- Seleziona un sito in **Origine collegamento** e inserisci un valore di costo compreso tra 0 e 100 in **Destinazione collegamento**.

Non è possibile modificare il costo del collegamento se la sorgente è la stessa della destinazione.

Per annullare le modifiche, selezionare  **Ripristina**.

- Selezionare **Applica modifiche**.

Utilizzare AutoSupport

Che cos'è AutoSupport?

La funzionalità AutoSupport consente a StorageGRID di inviare pacchetti di stato e di integrità al supporto tecnico NetApp .

Utilizzando AutoSupport è possibile velocizzare notevolmente la determinazione e la risoluzione dei problemi. Il supporto tecnico può anche monitorare le esigenze di archiviazione del tuo sistema e aiutarti a stabilire se è necessario aggiungere nuovi nodi o siti. Facoltativamente, è possibile configurare i pacchetti AutoSupport in modo che vengano inviati a un'ulteriore destinazione.

StorageGRID ha due tipi di AutoSupport:

- * StorageGRID AutoSupport* segnala problemi software StorageGRID . Abilitato per impostazione predefinita quando si installa per la prima volta StorageGRID. Puoi [modificare la configurazione predefinita AutoSupport](#) se necessario.



Se StorageGRID AutoSupport non è abilitato, viene visualizzato un messaggio nella dashboard di Grid Manager. Il messaggio include un collegamento alla pagina di configurazione AutoSupport . Se chiudi il messaggio, questo non verrà più visualizzato finché la cache del browser non verrà cancellata, anche se AutoSupport rimane disabilitato.

- **Appliance hardware AutoSupport** segnala problemi relativi all'appliance StorageGRID . Devi ["configurare AutoSupport hardware su ogni appliance"](#) .

Che cos'è il Active IQ?

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

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

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

Informazioni incluse nel pacchetto AutoSupport

Un pacchetto AutoSupport contiene i seguenti file e dettagli.

Nome del file	Campi	Descrizione
AUTOSUPPORT-HISTORY.XML	Numero di sequenza AutoSupport + Destinazione per questo AutoSupport + Stato di consegna + Tentativi di consegna + Oggetto AutoSupport + URI di consegna + Ultimo errore + Nome file PUT AutoSupport + Ora di generazione + Dimensione compressa AutoSupport + Dimensione decompressa AutoSupport + Tempo totale di raccolta (ms)	File cronologico AutoSupport .
AUTOSUPPORT.XML	Nodo + Protocollo per contattare l'assistenza + URL di supporto per HTTP/HTTPS + Indirizzo di supporto + Stato di AutoSupport OnDemand + URL del server di AutoSupport OnDemand + Intervallo di polling AutoSupport OnDemand	File di stato AutoSupport . Fornisce dettagli sul protocollo utilizzato, URL e indirizzo del supporto tecnico, intervallo di polling e OnDemand AutoSupport , se abilitato o disabilitato.

Nome del file	Campi	Descrizione
BUCKETS.XML	ID bucket + ID account + versione build + configurazione vincolo posizione + conformità abilitata + configurazione conformità + blocco oggetto S3 abilitato + configurazione blocco oggetto S3 + configurazione coerenza + CORS abilitato + configurazione CORS + ora ultimo accesso abilitata + policy abilitata + configurazione policy + notifiche abilitate + configurazione notifiche + cloud mirror abilitato + configurazione cloud mirror + ricerca abilitata + configurazione ricerca + tag bucket abilitato + configurazione tag bucket + configurazione versioning	Fornisce dettagli di configurazione e statistiche a livello di bucket. Esempi di configurazioni dei bucket includono servizi di piattaforma, conformità e coerenza dei bucket.
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 di griglia, spazio riservato ai metadati, impostazioni di configurazione a livello di griglia (conformità, blocco oggetti S3, compressione oggetti, avvisi, syslog e configurazione ILM), dettagli del profilo di codifica di cancellazione, nome DNS e " Nome NMS ".
GRID-SPEC.XML	Specifiche della griglia, XML grezzo	Utilizzato per configurare e distribuire 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 del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	File di stato delle attività di griglia (procedure di manutenzione). Fornisce dettagli sulle 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.

Nome del file	Campi	Descrizione
ILM-CONFIGURAZIONE.XML	ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	Elenco degli attributi per le configurazioni ILM.
ILM-STATUS.XML	Nodo + Percorso del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	File di informazioni sulle metriche ILM. Contiene i tassi di valutazione ILM per ciascun nodo e le metriche a livello di griglia.
ILM.XML	XML grezzo ILM	File di policy attiva ILM. Contiene dettagli sui criteri ILM attivi, come ID del pool di archiviazione, comportamento di acquisizione, filtri, regole e descrizione.
LOG.TGZ	<i>n / a</i>	File di registro scaricabile. Contiene <code>broadcast-err.log</code> e <code>servermanager.log</code> da ogni nodo.
MANIFEST.XML	Ordine di raccolta + Nome del file del contenuto AutoSupport per questi dati + Descrizione di questo elemento dati + Numero di byte raccolti + Tempo impiegato per la raccolta + Stato di questo elemento dati + Descrizione dell'errore + Tipo di contenuto AutoSupport per questi dati +	Contiene metadati AutoSupport e brevi descrizioni di tutti i file AutoSupport .
NMS-ENTITIES.XML	Indice attributo + OID entità + ID nodo + ID modello dispositivo + Versione modello dispositivo + Nome entità	Entità di gruppo e di servizio nel " Albero NMS ". Fornisce dettagli sulla topologia della griglia. Il nodo può essere determinato in base ai servizi in esecuzione sul nodo.
OGGETTI-STATO.XML	Nodo + Percorso del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	Stato dell'oggetto, tra cui stato della scansione in background, trasferimento attivo, velocità di trasferimento, trasferimenti totali, velocità di eliminazione, frammenti danneggiati, oggetti persi, oggetti mancanti, tentativi di riparazione, velocità di scansione, periodo di scansione stimato e stato di completamento della riparazione.

Nome del file	Campi	Descrizione
STATO-SERVER.XML	Nodo + Percorso del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	Configurazioni del server. Contiene i seguenti dettagli per ciascun nodo: tipo di piattaforma, sistema operativo, memoria installata, memoria disponibile, connettività di archiviazione, numero di serie dello chassis dell'appliance di archiviazione, numero di unità guaste del controller di archiviazione, temperatura dello chassis del controller di elaborazione, hardware di elaborazione, numero di serie del controller di elaborazione, alimentatore, dimensioni dell'unità e tipo di unità.
STATO-SERVIZIO.XML	Nodo + Percorso del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	File di informazioni sul nodo di servizio. Contiene dettagli quali spazio tabella allocato, spazio tabella libero, metriche Reaper del database, durata della riparazione del segmento, durata del processo di riparazione, riavvii automatici del processo e terminazione automatica del processo.
STORAGE-GRADES.XML	ID grado di archiviazione + Nome grado di archiviazione + ID nodo di archiviazione + Percorso nodo di archiviazione	File di definizione del grado di archiviazione per ciascun 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 riepilogano le informazioni sull'utilizzo StorageGRID . Fornisce dettagli quali il nome della griglia, i nomi dei siti, il numero di nodi di archiviazione per griglia e per sito, il tipo di licenza, la capacità e l'utilizzo della licenza, i termini di supporto software e i dettagli delle operazioni S3.
AVVISI DI SISTEMA.XML	Nome + Gravità + Nome nodo + Stato avviso + Nome sito + Ora di attivazione avviso + Ora di risoluzione avviso + ID regola + ID nodo + ID sito + Disattivato + Altre annotazioni + Altre etichette	Avvisi di sistema attuali che indicano potenziali problemi nel sistema StorageGRID .

Nome del file	Campi	Descrizione
USERAGENTS.XML	User agent + Numero di giorni + Richieste HTTP totali + Byte totali ingeriti + Byte totali recuperati + Richieste PUT + Richieste GET + Richieste DELETE + Richieste HEAD + Richieste POST + Richieste OPTIONS + Tempo medio della richiesta (ms) + Tempo medio della richiesta PUT (ms) + Tempo medio della richiesta GET (ms) + Tempo medio della richiesta DELETE (ms) + Tempo medio della richiesta HEAD (ms) + Tempo medio della richiesta POST (ms) + Tempo medio della richiesta OPTIONS (ms)	Statistiche basate sugli user agent dell'applicazione. Ad esempio, il numero di operazioni PUT/GET/DELETE/HEAD per user agent e la dimensione totale in byte di ciascuna operazione.
X-HEADER-DATI	X-Netapp-asup-generato-on + X-Netapp-asup-nome host + X-Netapp-asup-versione-os + X-Netapp-asup-num-seriale + X-Netapp-asup-oggetto + X-Netapp-asup-id-sistema + X-Netapp-asup-nome-modello +	Dati di intestazione AutoSupport .

Configura AutoSupport

Per impostazione predefinita, la funzionalità StorageGRID AutoSupport è abilitata quando si installa StorageGRID per la prima volta. Tuttavia, è necessario configurare AutoSupport hardware su ogni appliance. Se necessario, è possibile modificare la configurazione AutoSupport .

Se si desidera modificare la configurazione di StorageGRID AutoSupport, apportare le modifiche solo sul nodo di amministrazione primario. Devi [configurare l'hardware AutoSupport](#) su ogni elettrodomestico.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .
- Se utilizzerai HTTPS per l'invio di pacchetti AutoSupport , avrai fornito l'accesso Internet in uscita al nodo di amministrazione primario, direttamente o ["utilizzando un server proxy"](#) (non sono richieste connessioni in entrata).
- Se HTTP è selezionato nella pagina StorageGRID AutoSupport , è necessario ["configurato un server proxy"](#) per inoltrare i pacchetti AutoSupport come HTTPS. I server AutoSupport di NetApp rifiuteranno i pacchetti inviati tramite HTTP.
- Se si utilizzerà SMTP come protocollo per i pacchetti AutoSupport , è stato configurato un server di posta SMTP.

Informazioni su questo compito

È possibile utilizzare una 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: Abilitato.
- **Attivato da evento:** invia automaticamente pacchetti AutoSupport ogni ora o quando si verificano eventi di sistema significativi. Impostazione predefinita: Abilitato.
- **Su richiesta:** consente al supporto tecnico di richiedere che il sistema StorageGRID invii automaticamente pacchetti AutoSupport , il che è utile quando stanno lavorando attivamente a un problema (richiede il protocollo di trasmissione HTTPS AutoSupport). Impostazione predefinita: Disabilitato.
- **Attivato dall'utente:** invia manualmente i pacchetti AutoSupport in qualsiasi momento.

Specifica il protocollo per i pacchetti AutoSupport

Per inviare pacchetti AutoSupport è possibile utilizzare uno qualsiasi dei seguenti protocolli:

- **HTTPS:** Questa è l'impostazione predefinita e consigliata per le nuove installazioni. Questo protocollo utilizza la porta 443. Se lo desidera [abilitare la funzionalità AutoSupport on Demand](#) , devi usare 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 tramite HTTP. Questo protocollo utilizza la porta 80.
- **SMTP:** utilizzare questa opzione se si desidera che i pacchetti AutoSupport vengano inviati tramite e-mail.

Il protocollo impostato viene utilizzato per l'invio di tutti i tipi di pacchetti AutoSupport .

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Seleziona il protocollo che desideri utilizzare per inviare i pacchetti AutoSupport .
3. Se hai selezionato **HTTPS**, seleziona se utilizzare un certificato di supporto NetApp (certificato TLS) per proteggere la connessione al server di supporto tecnico.
 - **Verifica certificato** (predefinito): 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:** seleziona questa opzione solo quando hai una buona ragione per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.
4. Seleziona **Salva**. Tutti i pacchetti settimanali, attivati dall'utente e attivati da eventi vengono inviati utilizzando il protocollo selezionato.

Disabilita AutoSupport settimanale

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport al supporto tecnico una volta alla settimana.

Per determinare quando verrà inviato il pacchetto AutoSupport settimanale, vai alla scheda *** AutoSupport* > Risultati**. Nella sezione *** AutoSupport settimanale***, osserva il valore per **Prossimo orario pianificato**.

È possibile disattivare in qualsiasi momento l'invio automatico dei pacchetti AutoSupport settimanali.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Deseleziona la casella di controllo **Abilita AutoSupport settimanale**.
3. Seleziona **Salva**.

Disabilita AutoSupport attivato da eventi

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport al supporto tecnico ogni ora.

È possibile disattivare AutoSupport attivato da eventi in qualsiasi momento.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Deselezionare la casella di controllo **Abilita AutoSupport attivato da evento**.
3. Seleziona **Salva**.

Abilita AutoSupport su richiesta

AutoSupport on Demand può aiutare a risolvere i problemi su cui il supporto tecnico sta lavorando attivamente.

Per impostazione predefinita, AutoSupport on Demand è disabilitato. Abilitando questa funzionalità, il supporto tecnico potrà richiedere al sistema StorageGRID di inviare automaticamente i pacchetti AutoSupport. Il supporto tecnico può anche impostare l'intervallo di polling per le query AutoSupport on Demand.

Il supporto tecnico non può abilitare o disabilitare AutoSupport on Demand.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Selezionare **HTTPS** come protocollo.
3. Selezionare la casella di controllo **Abilita AutoSupport settimanale**.
4. Selezionare la casella di controllo **Abilita AutoSupport su richiesta**.
5. Seleziona **Salva**.

AutoSupport on Demand è abilitato 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 un hotfix o una nuova versione StorageGRID, la nuova versione viene visualizzata nella pagina Aggiornamento StorageGRID.

Se necessario, è possibile disattivare facoltativamente il controllo degli aggiornamenti software. Ad esempio, se il sistema non dispone di accesso WAN, è consigliabile disattivare il controllo per evitare errori di download.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Deseleziona la casella di controllo **Verifica aggiornamenti software**.
3. Seleziona **Salva**.

Aggiungi una destinazione AutoSupport aggiuntiva

Quando si attiva AutoSupport, i pacchetti di salute e stato 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 i pacchetti AutoSupport , vedere le istruzioni per [specificare il protocollo per i pacchetti AutoSupport](#) .



Non è possibile utilizzare il protocollo SMTP per inviare pacchetti AutoSupport a una destinazione aggiuntiva.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Selezionare **Abilita 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. La porta predefinita è 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.
- Seleziona **Non verificare il certificato** per inviare i pacchetti AutoSupport senza convalida del certificato.

Selezionare questa opzione solo quando si ha una buona ragione per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.

4. Se hai selezionato **Verifica certificato**, procedi come segue:
 - a. Passare alla posizione del certificato CA.
 - b. Carica il file del certificato CA.

Vengono visualizzati i metadati del certificato CA.

5. Seleziona **Salva**.

Tutti i futuri pacchetti AutoSupport settimanali, attivati da eventi e attivati dall'utente verranno inviati alla destinazione aggiuntiva.

Configura AutoSupport per gli elettrodomestici

AutoSupport per gli apparecchi segnala problemi hardware StorageGRID , mentre StorageGRID AutoSupport segnala problemi software StorageGRID , con un'eccezione: per SGF6112, StorageGRID AutoSupport

segnala sia problemi hardware che software. È necessario configurare AutoSupport su ogni appliance, ad eccezione di SGF6112, che non richiede alcuna configurazione aggiuntiva. AutoSupport viene implementato in modo diverso per le appliance di servizi e per quelle di storage.

Utilizzare SANtricity per abilitare AutoSupport per ogni appliance di storage. È possibile configurare SANtricity AutoSupport durante la configurazione iniziale dell'appliance o dopo l'installazione dell'appliance:

- Per gli apparecchi SG6000 e SG5700, "[configurare AutoSupport in SANtricity System Manager](#)"

I pacchetti AutoSupport degli appliance E-Series possono essere inclusi in StorageGRID AutoSupport se si configura la distribuzione AutoSupport tramite proxy in "[Gestore del sistema SANtricity](#)".

StorageGRID AutoSupport non segnala problemi hardware, come guasti alla DIMM o alla scheda di interfaccia host (HIC). Tuttavia, alcuni guasti dei componenti potrebbero innescare "[avvisi hardware](#)". Per gli apparecchi StorageGRID dotati di un controller di gestione della scheda base (BMC), è possibile configurare trappole SNMP e e-mail per segnalare guasti hardware:

- "[Imposta notifiche e-mail per gli avvisi BMC](#)"
- "[Configurare le impostazioni SNMP per BMC](#)"

Informazioni correlate

["Supporto NetApp"](#)

Attivare manualmente un pacchetto AutoSupport

Per aiutare il supporto tecnico a risolvere i problemi del sistema StorageGRID, è possibile attivare manualmente l'invio di un pacchetto AutoSupport.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- È necessario disporre dell'autorizzazione di accesso Root o di un'altra configurazione della griglia.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport***.
2. Nella scheda **Azioni**, seleziona **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 **Ultima volta riuscita** nella scheda **Risultati** vengono aggiornati. Se si verifica un problema, il valore **Risultato più recente** viene aggiornato in "Non riuscito" e StorageGRID non tenta più di inviare il pacchetto AutoSupport.



Dopo aver inviato un pacchetto AutoSupport attivato dall'utente, aggiorna la pagina AutoSupport nel browser dopo 1 minuto per accedere ai risultati più recenti.

Risoluzione dei problemi dei pacchetti AutoSupport

Se un tentativo di invio di un pacchetto AutoSupport fallisce, il sistema StorageGRID intraprende azioni diverse a seconda del tipo di pacchetto AutoSupport. È possibile verificare lo stato dei pacchetti AutoSupport selezionando **SUPPORTO > Strumenti > * AutoSupport* > Risultati**.

Se l'invio del pacchetto AutoSupport non riesce, nella scheda **Risultati** della pagina * AutoSupport* viene visualizzato il messaggio "Non riuscito".



Se hai configurato un server proxy per inoltrare i pacchetti AutoSupport a NetApp, dovresti [verificare che le impostazioni di configurazione del server proxy siano corrette](#) .

Errore settimanale del pacchetto AutoSupport

Se un pacchetto AutoSupport settimanale non riesce a essere inviato, il sistema StorageGRID esegue le seguenti azioni:

1. Aggiorna l'attributo Risultato più recente in Nuovo tentativo.
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 Risultato più recente in Non riuscito.
4. Tenta di inviare nuovamente un pacchetto AutoSupport al successivo orario programmato.
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 che siano trascorsi sette giorni.
6. Quando il servizio NMS è nuovamente disponibile, invia immediatamente un pacchetto AutoSupport se un pacchetto non è stato inviato per sette giorni o più.

Errore del pacchetto AutoSupport attivato dall'utente o dall'evento

Se un pacchetto AutoSupport attivato dall'utente o da un evento non riesce a inviare, il sistema StorageGRID esegue le seguenti azioni:

1. Visualizza un messaggio di errore se l'errore è noto. Ad esempio, se un utente seleziona il protocollo SMTP senza fornire le impostazioni di configurazione e-mail corrette, viene visualizzato il seguente 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 pacco.
3. Registra l'errore in `nms.log` .

Se si verifica un errore e SMTP è il protocollo selezionato, verificare che il server di posta elettronica del sistema StorageGRID sia configurato correttamente e che il server di posta elettronica sia in esecuzione (**SUPPORTO > Allarmi (legacy) > Configurazione posta elettronica legacy**). Nella pagina AutoSupport potrebbe apparire 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 SMTP è il protocollo selezionato, verificare che il server di posta elettronica del sistema StorageGRID sia configurato correttamente e che il server di posta elettronica sia in esecuzione. Nella pagina AutoSupport potrebbe apparire il seguente messaggio di errore: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Inviare pacchetti E-Series AutoSupport tramite StorageGRID

È possibile inviare i pacchetti E-Series SANtricity System Manager AutoSupport al

supporto tecnico tramite un nodo di amministrazione StorageGRID anziché tramite la porta di gestione dell'appliance di archiviazione.

Vedere ["AutoSupport hardware serie E"](#) per ulteriori informazioni sull'utilizzo di AutoSupport con gli apparecchi della serie E.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager tramite un ["browser web supportato"](#) .
- Tu hai il ["Amministratore dell'appliance di archiviazione o autorizzazione di accesso root"](#) .
- Hai configurato SANtricity AutoSupport:
 - Per gli apparecchi SG6000 e SG5700, ["configurare AutoSupport in SANtricity System Manager"](#)



Per accedere a SANtricity System Manager tramite Grid Manager è necessario disporre del firmware SANtricity 8.70 o superiore.

Informazioni su questo compito

I pacchetti E-Series AutoSupport contengono dettagli sull'hardware di archiviazione e sono più specifici rispetto ad altri pacchetti AutoSupport inviati dal sistema StorageGRID .

È possibile configurare un indirizzo server proxy speciale in SANtricity System Manager per trasmettere i pacchetti AutoSupport tramite un nodo di amministrazione StorageGRID senza utilizzare la porta di gestione dell'appliance. I pacchetti AutoSupport trasmessi in questo modo vengono inviati dal ["mittente preferito Nodo amministratore"](#) e usano qualsiasi ["impostazioni proxy amministratore"](#) che sono stati configurati in Grid Manager.

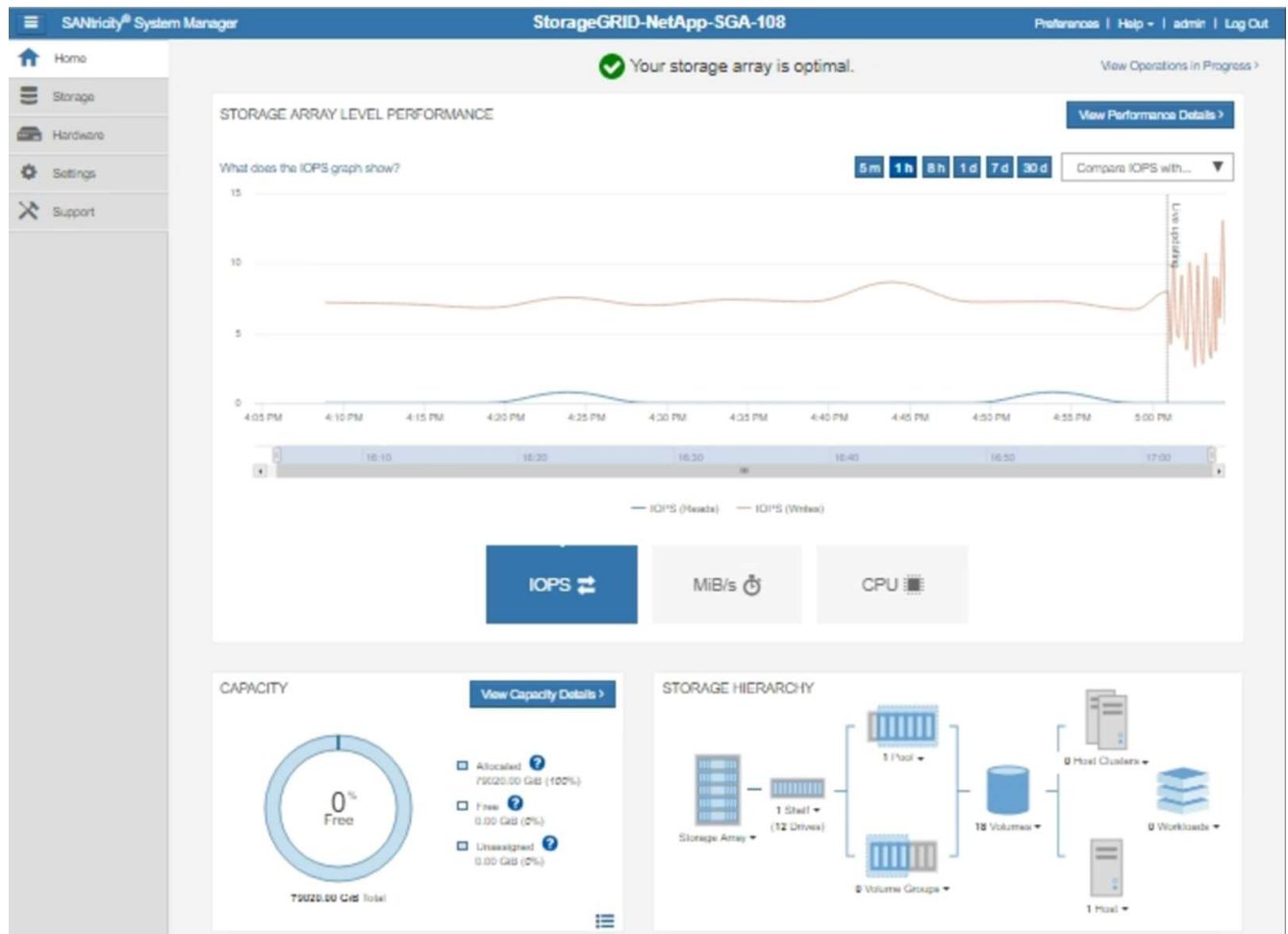


Questa procedura è valida solo per la configurazione di un server proxy StorageGRID per i pacchetti E-Series AutoSupport . Per ulteriori dettagli sulla configurazione di E-Series AutoSupport , vedere ["Documentazione NetApp E-Series e SANtricity"](#) .

Passi

1. Nel Grid Manager, seleziona **NODI**.
2. Dall'elenco dei nodi a sinistra, seleziona il nodo dell'appliance di archiviazione che desideri configurare.
3. Selezionare * SANtricity System Manager*.

Viene visualizzata la home page di SANtricity System Manager.



4. Selezionare **SUPPORTO** > **Centro assistenza** > * AutoSupport*.

Viene visualizzata la pagina delle operazioni di AutoSupport .

Technical Support

Chassis serial number: 031517000693

 [NetApp My Support](#)

US/Canada 888.463.8277

[Other Contacts](#)

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled ?

[Enable/Disable AutoSupport Features](#)
AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

[Configure AutoSupport Delivery Method](#)

Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

[Schedule AutoSupport Dispatches](#)
AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

[Send AutoSupport Dispatch](#)
Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

[View AutoSupport Log](#)
The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

[Enable AutoSupport Maintenance Window](#)
Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[Disable AutoSupport Maintenance Window](#)
Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. Selezionare *Configura metodo di consegna AutoSupport*.

Viene visualizzata la pagina Configura metodo di consegna AutoSupport .

6. Selezionare **HTTPS** come metodo di consegna.



Il certificato che abilita HTTPS è preinstallato.

7. Selezionare **tramite server proxy**.

8. Entra `tunnel-host` per l'**Indirizzo host**.

`tunnel-host` è l'indirizzo speciale per utilizzare un nodo di amministrazione per inviare pacchetti E-Series AutoSupport .

9. Entra `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 nell'appliance.

10. Selezionare **Test configurazione** per testare il routing e la configurazione del server proxy AutoSupport .

Se è corretto, viene visualizzato un messaggio in un banner verde: "La configurazione AutoSupport è stata verificata".

Se il test fallisce, viene visualizzato un messaggio di errore in un banner rosso. Controlla le impostazioni DNS e di rete StorageGRID , assicurati che "[mittente preferito](#) [Nodo amministratore](#)" puoi connetterti al sito di supporto NetApp e riprovare il test.

11. Seleziona **Salva**.

La configurazione viene salvata e viene visualizzato un messaggio di conferma: "Il metodo di consegna AutoSupport è stato configurato".

Gestisci nodi di archiviazione

Gestisci nodi di archiviazione

I nodi di archiviazione forniscono capacità e servizi di archiviazione su disco. La gestione dei nodi di archiviazione comporta quanto segue:

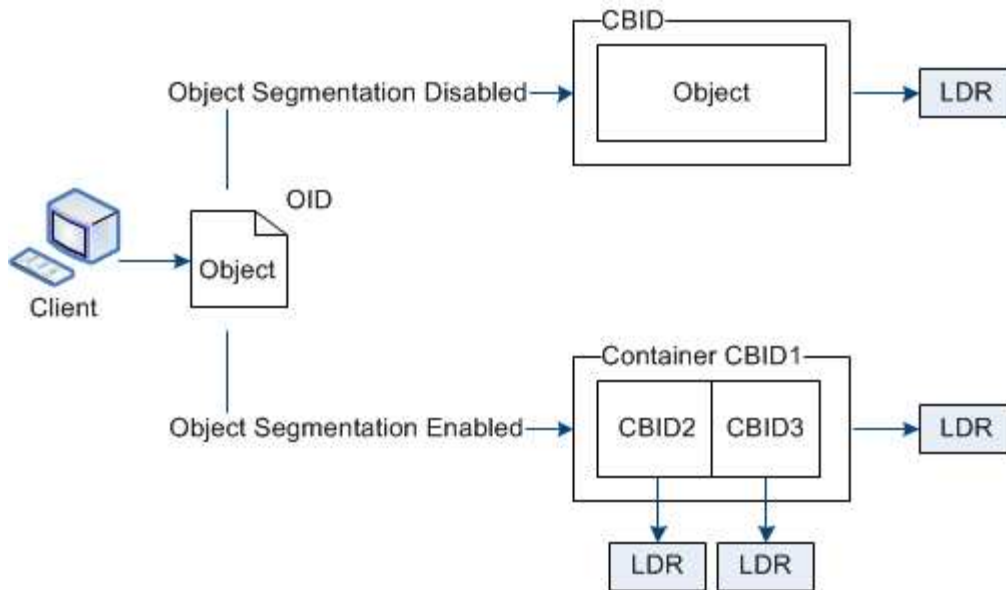
- Gestione delle opzioni di archiviazione
- Comprendere cosa sono le filigrane del volume di archiviazione e come è possibile utilizzare gli override delle filigrane per controllare quando i nodi di archiviazione diventano di sola lettura
- Monitoraggio e gestione dello spazio utilizzato per i metadati degli oggetti
- Configurazione delle impostazioni globali per gli oggetti memorizzati
- Applicazione delle impostazioni di configurazione del nodo di archiviazione
- Gestione di nodi di archiviazione completi

Utilizzare le opzioni di archiviazione

Che cos'è la segmentazione degli oggetti?

La segmentazione degli oggetti è il processo di suddivisione di un oggetto in una raccolta di oggetti più piccoli di dimensioni fisse per ottimizzare l'archiviazione e l'utilizzo delle risorse per oggetti di grandi dimensioni. Il caricamento multiparte di S3 crea anche oggetti segmentati, con un oggetto che rappresenta ogni parte.

Quando un oggetto viene inserito nel sistema StorageGRID , il servizio LDR lo suddivide in segmenti e crea un contenitore di segmenti che elenca le informazioni di intestazione di tutti i segmenti come contenuto.



Al recupero di un contenitore di segmenti, il servizio LDR assembla l'oggetto originale dai suoi segmenti e restituisce l'oggetto al client.

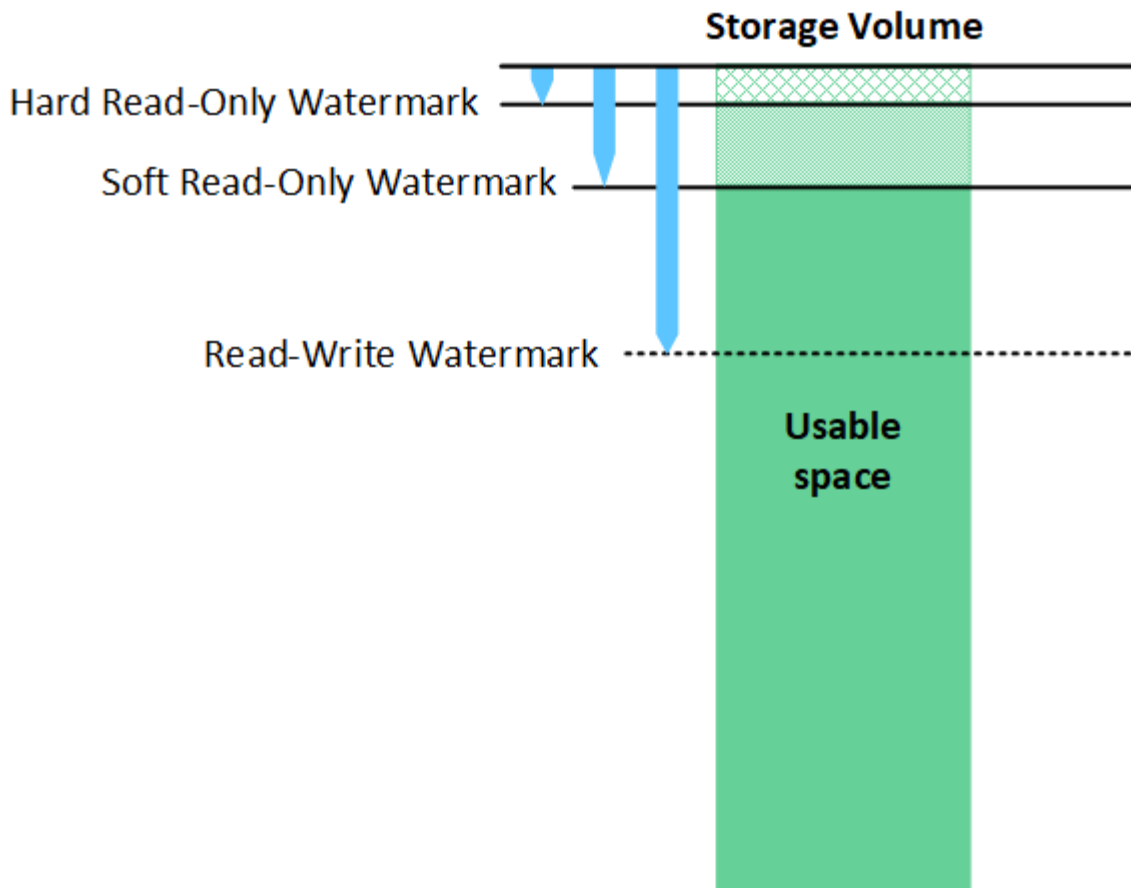
Il contenitore e i segmenti non sono necessariamente archiviati sullo stesso nodo di archiviazione. Il contenitore e i segmenti possono essere archiviati su qualsiasi nodo di archiviazione all'interno del pool di archiviazione specificato nella regola ILM.

Ogni segmento viene trattato in modo indipendente dal sistema StorageGRID e contribuisce al conteggio di attributi quali oggetti gestiti e oggetti archiviati. Ad esempio, se un oggetto archiviato nel sistema StorageGRID viene suddiviso in due segmenti, il valore degli oggetti gestiti aumenta di tre volte al termine dell'acquisizione, come segue:

`segment container + segment 1 + segment 2 = three stored objects`

Cosa sono le filigrane del volume di archiviazione?

StorageGRID utilizza tre filigrane di volume di archiviazione per garantire che i nodi di archiviazione vengano trasferiti in modo sicuro a uno stato di sola lettura prima che lo spazio si esaurisca in modo critico e per consentire ai nodi di archiviazione che sono stati trasferiti a uno stato di sola lettura di tornare allo stato di lettura-scrittura.



Le filigrane del volume di archiviazione si applicano solo allo spazio utilizzato per i dati degli oggetti replicati e codificati per la cancellazione. Per informazioni sullo spazio riservato ai metadati degli oggetti sul volume 0, vai a ["Gestire l'archiviazione dei metadati degli oggetti"](#).

Cos'è la filigrana di sola lettura?

La **filigrana di sola lettura software del volume di archiviazione** è la prima filigrana a indicare che lo spazio utilizzabile di un nodo di archiviazione per i dati degli oggetti si sta esaurendo.

Se ogni volume in un nodo di archiviazione ha meno spazio libero rispetto alla filigrana di sola lettura software di quel volume, il nodo di archiviazione passa alla *modalità di sola lettura*. La modalità di sola lettura significa che il nodo di archiviazione pubblicizza servizi di sola lettura al resto del sistema StorageGRID, ma soddisfa tutte le richieste di scrittura in sospeso.

Ad esempio, supponiamo che ogni volume in un nodo di archiviazione abbia una filigrana di sola lettura software di 10 GB. Non appena ogni volume ha meno di 10 GB di spazio libero, il nodo di archiviazione passa alla modalità di sola lettura software.

Cos'è la filigrana di sola lettura?

La **filigrana di sola lettura fissa del volume di archiviazione** è la filigrana successiva che indica che lo spazio utilizzabile di un nodo per i dati degli oggetti si sta riempiendo.

Se lo spazio libero su un volume è inferiore al limite di sola lettura fisso del volume, le scritture sul volume non riusciranno. Tuttavia, le scritture su altri volumi possono continuare finché lo spazio libero su tali volumi non è inferiore alle relative filigrane di sola lettura.

Ad esempio, supponiamo che ogni volume in un nodo di archiviazione abbia una filigrana di sola lettura fissa di 5 GB. Non appena ogni volume ha meno di 5 GB di spazio libero, il nodo di archiviazione non accetta più richieste di scrittura.

La filigrana di sola lettura fissa è sempre inferiore alla filigrana di sola lettura flessibile.

Cos'è la filigrana di lettura-scrittura?

La **filigrana di lettura-scrittura del volume di archiviazione** si applica solo ai nodi di archiviazione che sono passati alla modalità di sola lettura. Determina quando il nodo può tornare ad essere di lettura-scrittura. Quando lo spazio libero su un volume di archiviazione in un nodo di archiviazione è maggiore del limite di lettura-scrittura del volume, il nodo torna automaticamente allo stato di lettura-scrittura.

Supponiamo, ad esempio, che il nodo di archiviazione sia passato alla modalità di sola lettura. Supponiamo inoltre che ogni volume abbia una filigrana di lettura-scrittura di 30 GB. Non appena lo spazio libero per un volume aumenta a 30 GB, il nodo torna ad essere di lettura-scrittura.

La filigrana di lettura-scrittura è sempre più grande sia della filigrana di sola lettura software che di quella di sola lettura hardware.

Visualizza le filigrane del volume di archiviazione

È possibile visualizzare le impostazioni correnti della filigrana e i valori ottimizzati dal sistema. Se non vengono utilizzate filigrane ottimizzate, puoi valutare se puoi o dovresti modificare le impostazioni.

Prima di iniziare

- Hai completato l'aggiornamento a StorageGRID 11.6 o versione successiva.
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).

Visualizza le impostazioni correnti della filigrana

È possibile visualizzare le impostazioni correnti della filigrana di archiviazione in Grid Manager.

Passi

1. Selezionare **SUPPORTO > Altro > Filigrane di archiviazione**.
2. Nella pagina Filigrane di archiviazione, controlla la casella di controllo Usa valori ottimizzati.
 - Se la casella di controllo è selezionata, tutte e tre le filigrane vengono 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. Facoltativamente, puoi [Visualizza le filigrane di archiviazione ottimizzate](#).
 - Se la casella di controllo Usa valori ottimizzati non è selezionata, vengono utilizzate filigrane personalizzate (non ottimizzate). Si sconsiglia di utilizzare impostazioni di filigrana personalizzate. Utilizzare le istruzioni per ["risoluzione dei problemi avvisi di override della filigrana di sola lettura bassa"](#) per determinare se è possibile o opportuno modificare le impostazioni.

Quando si specificano impostazioni di filigrana personalizzate, è necessario immettere valori maggiori di 0.

Visualizza le filigrane di archiviazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati calcolati per la filigrana di sola lettura software del volume di archiviazione. È possibile visualizzare i valori ottimizzati minimi e massimi per ciascun nodo di archiviazione nella griglia.

1. Selezionare **SUPPORTO > Strumenti > Metriche**.
2. Nella sezione Prometheus, seleziona il collegamento per accedere all'interfaccia utente di Prometheus.
3. Per visualizzare il watermark minimo consigliato per la sola lettura software, 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 software per tutti i volumi di archiviazione su ciascun nodo di archiviazione. Se questo valore è maggiore dell'impostazione personalizzata per la filigrana di sola lettura software del volume di archiviazione, viene attivato l'avviso **Sostituzione filigrana di sola lettura insufficiente** per il nodo di archiviazione.

4. Per visualizzare il limite massimo consigliato per la sola lettura software, 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 software per tutti i volumi di archiviazione su ciascun nodo di archiviazione.

Gestire l'archiviazione dei metadati degli oggetti

La capacità dei metadati degli oggetti di un sistema StorageGRID controlla il numero massimo di oggetti che possono essere archiviati su quel sistema. Per garantire che il sistema StorageGRID disponga di spazio adeguato per archiviare nuovi oggetti, è necessario comprendere dove e come StorageGRID archivia i metadati degli oggetti.

Cosa sono i metadati degli oggetti?

I metadati di un oggetto sono tutte le informazioni che descrivono un oggetto. StorageGRID utilizza i metadati degli oggetti per tracciare le posizioni di tutti gli oggetti nella griglia e per 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:

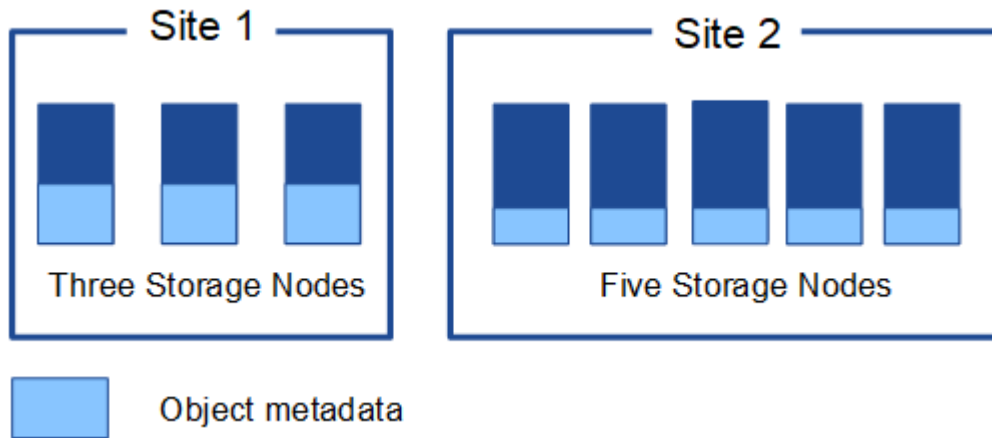
- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora in cui l'oggetto è stato creato per la prima volta e la data e l'ora in cui l'oggetto è stato modificato per l'ultima volta.
- Qualsiasi coppia chiave-valore di metadati utente personalizzati associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore del tag oggetto associata all'oggetto.
- Per le copie di oggetti replicati, la posizione di archiviazione corrente di ciascuna copia.
- Per le copie di oggetti con codice di cancellazione, la posizione di archiviazione 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 oggetti multiparte, identificatori di segmento e dimensioni dei dati.

Come vengono archiviati i metadati degli oggetti?

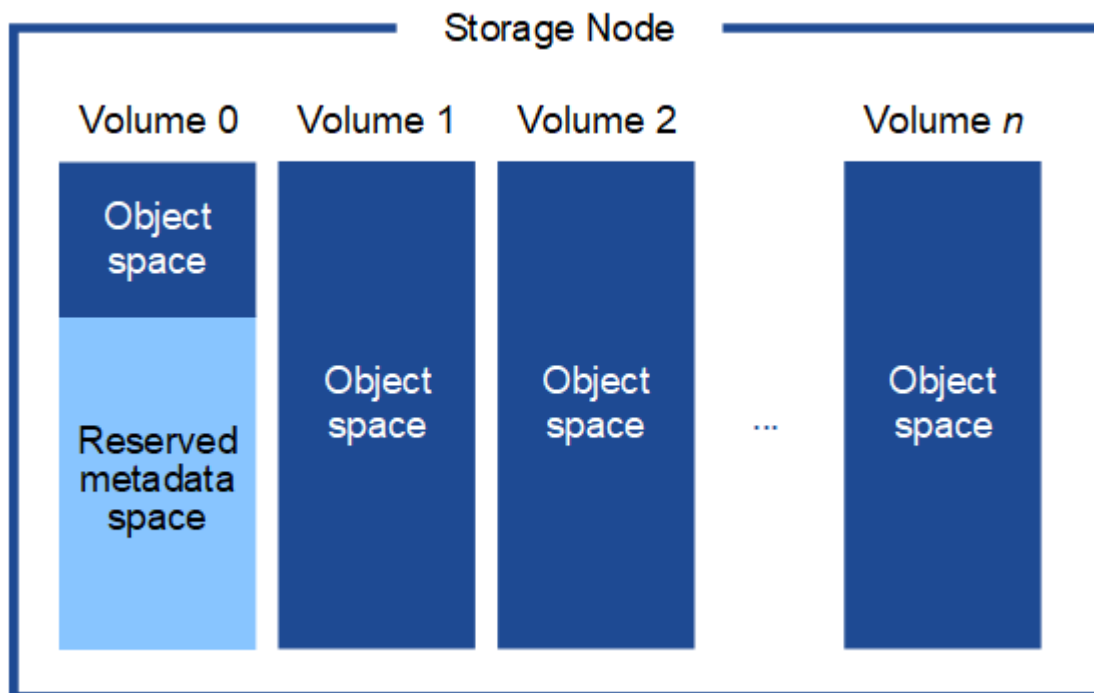
StorageGRID conserva i metadati degli oggetti in un database Cassandra, che viene archiviato indipendentemente dai dati degli oggetti. Per garantire ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti nel sistema in ogni sito.

Questa figura rappresenta i nodi di archiviazione in due siti. Ogni sito ha la stessa quantità di metadati degli oggetti e i metadati di ogni sito sono suddivisi tra tutti i nodi di archiviazione di quel sito.



Dove vengono archiviati i metadati degli oggetti?

Questa cifra rappresenta i volumi di archiviazione per un singolo nodo di archiviazione.



Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di archiviazione 0 di ciascun nodo di archiviazione. Utilizza lo spazio riservato per memorizzare i metadati degli

oggetti e per eseguire operazioni essenziali sul database. Tutto lo spazio rimanente sul volume di archiviazione 0 e su tutti gli altri volumi di archiviazione nel nodo di archiviazione viene utilizzato esclusivamente per i dati degli oggetti (copie replicate e frammenti con codice di cancellazione).

La quantità di spazio riservata ai metadati degli oggetti su un particolare nodo di archiviazione dipende da diversi fattori, descritti di seguito.

Impostazione dello spazio riservato ai metadati

Lo *Spazio riservato ai metadati* è un'impostazione a livello di sistema che rappresenta la quantità di spazio che verrà 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 del software che stavi utilizzando quando hai installato inizialmente StorageGRID.
- La quantità di RAM su ciascun nodo di archiviazione.

Versione utilizzata per l'installazione iniziale StorageGRID	Quantità di RAM sui nodi di archiviazione	Impostazione predefinita dello spazio riservato ai metadati
da 11,5 a 11,9	128 GB o più su ciascun nodo di archiviazione nella griglia	8 TB (8.000 GB)
	Meno di 128 GB su qualsiasi nodo di archiviazione nella griglia	3 TB (3.000 GB)
11.1 a 11.4	128 GB o più su ciascun nodo di archiviazione in qualsiasi sito	4 TB (4.000 GB)
	Meno di 128 GB su qualsiasi nodo di archiviazione in ogni sito	3 TB (3.000 GB)
11.0 o precedente	Qualsiasi importo	2 TB (2.000 GB)

Visualizza l'impostazione dello spazio riservato ai metadati

Seguire questi passaggi per visualizzare l'impostazione dello spazio riservato ai metadati per il sistema StorageGRID .

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Impostazioni di archiviazione**.
2. Nella pagina Impostazioni di archiviazione, espandi la sezione **Spazio riservato metadati**.

Per StorageGRID 11.8 o versioni successive, il valore dello spazio riservato ai metadati deve essere almeno 100 GB e non superiore a 1 PB.

L'impostazione predefinita per una nuova installazione StorageGRID 11.6 o versione successiva in cui ogni nodo di archiviazione ha 128 GB o più di RAM è 8.000 GB (8 TB).

Spazio effettivamente riservato per i metadati

Contrariamente all'impostazione dello spazio riservato ai metadati a livello di sistema, lo *spazio riservato effettivo* per i metadati degli oggetti viene determinato per ciascun nodo di archiviazione. Per ogni nodo di archiviazione, lo spazio effettivamente riservato per i metadati dipende dalla dimensione del volume 0 per il nodo e dall'impostazione dello spazio riservato per i metadati a livello di sistema.

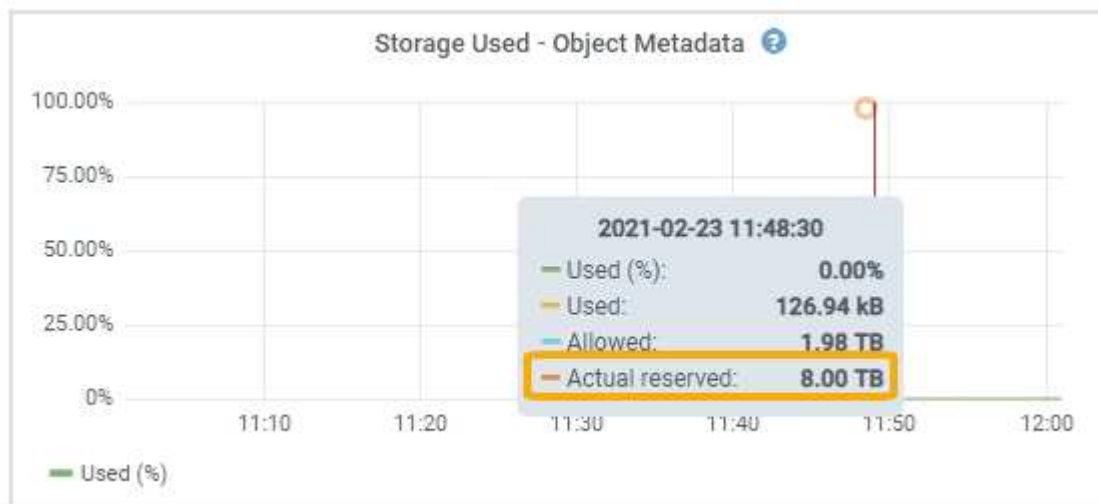
Dimensione del volume 0 per il nodo	Spazio effettivamente riservato per i metadati
Meno di 500 GB (uso non produttivo)	10% del volume 0
500 GB o più + o + Nodi di archiviazione solo metadati	Il più piccolo di questi valori: • Volume 0 • Impostazione dello spazio riservato ai metadati Nota: per i nodi di archiviazione solo metadati è richiesto un solo rangedb.

Visualizza lo spazio effettivamente riservato per i metadati

Per visualizzare lo spazio effettivamente riservato per i metadati su un particolare nodo di archiviazione, seguire questi passaggi.

Passi

1. Da Grid Manager, seleziona **NODI > Nodo di archiviazione**.
2. Selezionare la scheda **Archiviazione**.
3. Posiziona il cursore sul grafico Spazio di archiviazione utilizzato - Metadati oggetto e individua il valore **Riservato effettivo**.



Nello screenshot, il valore **effettivo riservato** è 8 TB. Questa schermata riguarda un nodo di archiviazione di grandi dimensioni in una nuova installazione 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.

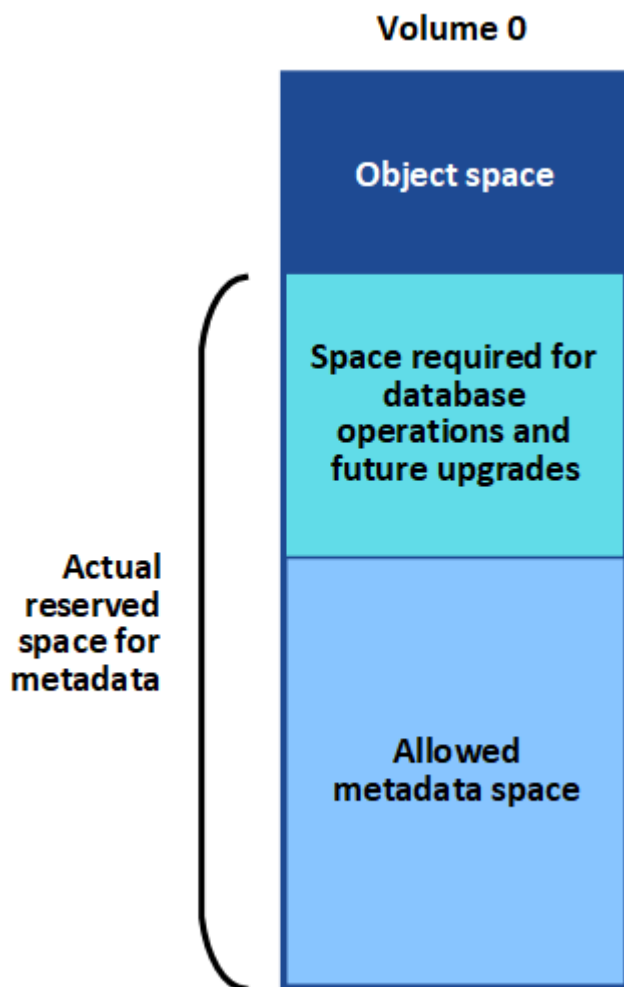
Esempio di spazio metadati effettivamente riservato

Supponiamo di installare un nuovo sistema StorageGRID utilizzando la versione 11.7 o successiva. Per questo esempio, supponiamo che ogni nodo di archiviazione abbia più di 128 GB di RAM e che il volume 0 del nodo di archiviazione 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo **spazio riservato ai metadati** a livello di sistema è impostato su 8 TB. (Questo è il valore predefinito per una nuova installazione StorageGRID 11.6 o versione successiva se ogni nodo di archiviazione ha più di 128 GB di RAM.)
- Lo spazio effettivamente riservato 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 ai metadati**.)

Spazio metadati consentito

Lo spazio effettivamente riservato per i metadati di ciascun nodo di archiviazione è suddiviso nello spazio disponibile per i metadati degli oggetti (lo *spazio metadati consentito*) e nello spazio richiesto per le operazioni essenziali del database (come la compattazione e la riparazione) e per i futuri aggiornamenti hardware e software. Lo spazio dei metadati consentito regola la capacità complessiva dell'oggetto.



La tabella seguente mostra come StorageGRID calcola lo **spazio metadati consentito** per diversi nodi di archiviazione, in base alla quantità di memoria per il nodo e allo spazio effettivamente riservato per i metadati.

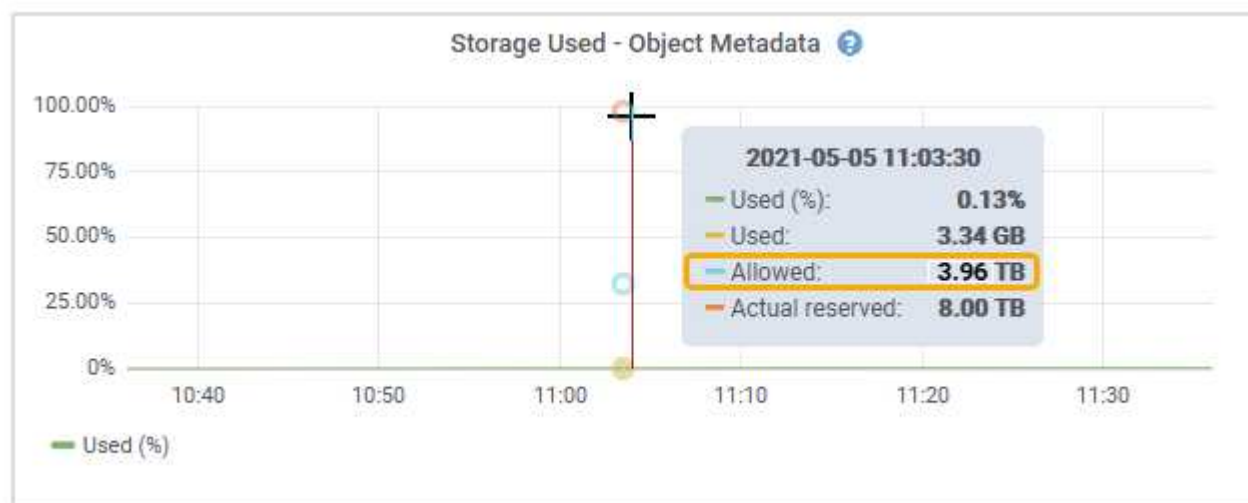
	Quantità di memoria sul nodo di archiviazione		
	< 128 GB	>= 128 GB	Spazio effettivo riservato per i metadati
≤ 4 TB	60% dello spazio effettivamente riservato ai metadati, fino a un massimo di 1,32 TB	60% dello spazio effettivamente riservato ai metadati, fino a un massimo di 1,98 TB	4 TB

Visualizza lo spazio metadati consentito

Per visualizzare lo spazio metadati consentito per un nodo di archiviazione, seguire questi passaggi.

Passi

1. Da Grid Manager, seleziona **NODI**.
2. Selezionare il nodo di archiviazione.
3. Selezionare la scheda **Archiviazione**.
4. Posiziona il cursore sul grafico Metadati oggetto - Spazio di archiviazione utilizzato e individua il valore **Consentito**.



Nello screenshot, il valore **Consentito** è 3,96 TB, che è il valore massimo per un nodo di archiviazione il cui spazio effettivamente riservato per i metadati è superiore a 4 TB.

Il valore **Consentito** corrisponde a questa metrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Esempio di spazio metadati consentito

Supponiamo di installare un sistema StorageGRID utilizzando la versione 11.6. Per questo esempio, supponiamo che ogni nodo di archiviazione abbia più di 128 GB di RAM e che il volume 0 del nodo di archiviazione 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo **spazio riservato ai metadati** a livello di sistema è impostato su 8 TB. (Questo è il valore predefinito per StorageGRID 11.6 o versioni successive quando ogni nodo di archiviazione ha più di 128 GB di RAM.)
- Lo spazio effettivamente riservato 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 ai 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 effettivo riservato per i metadati – 1 TB) × 60%, fino a un massimo di 3,96 TB.

Come i nodi di archiviazione di diverse dimensioni influenzano la capacità degli oggetti

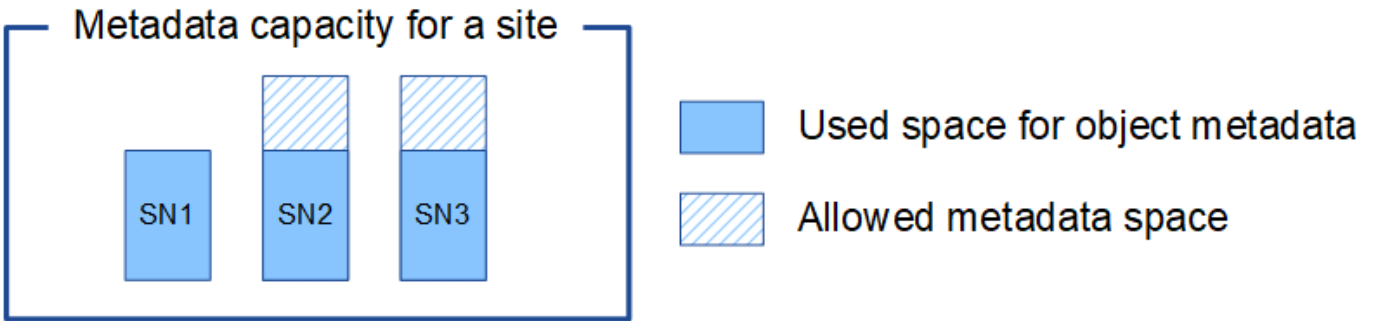
Come descritto sopra, StorageGRID distribuisce uniformemente i metadati degli oggetti tra i nodi di archiviazione in ciascun sito. Per questo motivo, se un sito contiene nodi di archiviazione di dimensioni diverse, il nodo più piccolo del sito determina la capacità dei metadati del sito.

Consideriamo il seguente esempio:

- Si dispone di una griglia a sito singolo contenente tre nodi di archiviazione di dimensioni diverse.
- L'impostazione **Spazio riservato ai metadati** è 4 TB.
- I nodi di archiviazione hanno i seguenti valori per lo spazio metadati effettivamente riservato e lo spazio metadati consentito.

Nodo di archiviazione	Dimensione del volume 0	Spazio metadati effettivamente riservato	Spazio metadati consentito
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 uniformemente tra i nodi di archiviazione di un sito, ogni nodo in questo esempio può contenere solo 1,32 TB di metadati. Non è possibile utilizzare gli ulteriori 0,66 TB di spazio metadati consentito per SN2 e SN3.



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.

E poiché la capacità dei metadati degli oggetti controlla il conteggio massimo degli oggetti, quando un nodo esaurisce la capacità dei metadati, la griglia è di fatto piena.

Informazioni correlate

- Per informazioni su come monitorare la capacità dei metadati degli oggetti per ciascun nodo di archiviazione, consultare le istruzioni per "[Monitoraggio StorageGRID](#)".
- Per aumentare la capacità dei metadati degli oggetti per il tuo sistema, "[espandere una griglia](#)" aggiungendo nuovi nodi di archiviazione.

Aumenta l'impostazione dello spazio riservato ai metadati

Potresti essere in grado di aumentare l'impostazione di sistema Spazio riservato ai metadati se i tuoi nodi di archiviazione soddisfano requisiti specifici per RAM e spazio disponibile.

Cosa ti servirà

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[Autorizzazione di accesso root o configurazione della pagina topologia griglia e altre autorizzazioni di configurazione griglia](#)".



La pagina Topologia griglia è stata deprecata e verrà rimossa in una versione futura.

Informazioni su questo compito

Potresti essere in grado di aumentare manualmente l'impostazione Spazio riservato 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 seguenti affermazioni sono vere:

- Ogni nodo di archiviazione in qualsiasi sito del sistema dispone di almeno 128 GB di RAM.
- Ciascun nodo di archiviazione in qualsiasi sito del sistema dispone di spazio disponibile sufficiente sul volume di archiviazione 0.

Tieni presente che se aumenti questa impostazione, ridurrai contemporaneamente lo spazio disponibile per l'archiviazione degli oggetti sul volume di archiviazione 0 di tutti i nodi di archiviazione. Per questo motivo, potrebbe essere preferibile impostare lo spazio riservato ai metadati su un valore inferiore a 8 TB, in base ai requisiti previsti per i metadati degli oggetti.



In generale, è meglio usare un valore più alto anziché uno più basso. Se l'impostazione Spazio riservato metadati è troppo grande, è possibile ridurla in seguito. 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 degli oggetti su un particolare nodo di archiviazione, vedere "[Gestire l'archiviazione dei metadati degli oggetti](#)".

Passi

1. Determina l'impostazione corrente dello spazio riservato ai metadati.
 - a. Selezionare **CONFIGURAZIONE > Sistema > Opzioni di archiviazione**.
 - b. Nella sezione Filigrane di archiviazione, annotare il valore di **Spazio riservato metadati**.
2. Assicurarsi di avere abbastanza spazio disponibile sul volume di archiviazione 0 di ciascun nodo di archiviazione per aumentare questo valore.
 - a. Selezionare **NODES**.
 - b. Selezionare il primo nodo di archiviazione nella griglia.
 - c. Selezionare la scheda Archiviazione.
 - d. Nella sezione Volumi, individuare la voce **/var/local/rangedb/0**.
 - e. Verificare che il valore Disponibile sia uguale o maggiore della differenza tra il nuovo valore che si desidera utilizzare e il valore corrente dello Spazio riservato ai metadati.

Ad esempio, se l'impostazione Spazio riservato metadati è attualmente pari a 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 archiviazione.
 - Se uno o più nodi di archiviazione non dispongono di spazio disponibile sufficiente, il valore Spazio riservato ai metadati non può essere aumentato. Non continuare con questa procedura.
 - Se ogni nodo di archiviazione dispone di spazio sufficiente sul volume 0, procedere al passaggio successivo.
3. Assicurati di avere almeno 128 GB di RAM su ogni nodo di archiviazione.
 - a. Selezionare **NODES**.
 - b. Selezionare il primo nodo di archiviazione nella griglia.
 - c. Selezionare la scheda **Hardware**.
 - d. Passa il cursore sul grafico Utilizzo memoria. Assicurarsi che la **Memoria totale** sia almeno 128 GB.
 - e. Ripetere questi passaggi per tutti i nodi di archiviazione.
 - Se uno o più nodi di archiviazione non dispongono di memoria totale disponibile sufficiente, il valore dello spazio riservato ai metadati non può essere aumentato. Non continuare con questa procedura.
 - Se ogni nodo di archiviazione ha almeno 128 GB di memoria totale, passare al passaggio successivo.
4. Aggiorna l'impostazione Spazio riservato ai metadati.
 - a. Selezionare **CONFIGURAZIONE > Sistema > Opzioni di archiviazione**.
 - b. Selezionare la scheda Configurazione.
 - c. Nella sezione Filigrane di archiviazione, seleziona **Spazio riservato metadati**.
 - d. Inserisci il nuovo valore.

Ad esempio, per immettere 8 TB, che è il valore massimo supportato, immettere **8000000000000** (8 seguito da 12 zeri)

Storage Options

Overview

Configuration



Configure Storage Options

Updated: 2021-12-10 13:48:23 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1000000000

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0
Storage Volume Soft Read-Only Watermark Override	0
Storage Volume Hard Read-Only Watermark Override	0
Metadata Reserved Space	800000000000

Apply Changes 

a. Selezionare **Applica modifiche**.

Comprimi gli oggetti memorizzati

È possibile abilitare la compressione degli oggetti per ridurre le dimensioni degli oggetti archiviati in StorageGRID, in modo che occupino meno spazio di archiviazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Informazioni su questo compito

Per impostazione predefinita, la compressione degli oggetti è disabilitata. Se si abilita la compressione, StorageGRID tenta di comprimere ogni oggetto durante il salvataggio, utilizzando la compressione senza perdita di dati.



Se si modifica questa impostazione, ci vorrà circa un minuto prima che la nuova impostazione venga applicata. Il valore configurato viene memorizzato nella cache per migliorare le prestazioni e il ridimensionamento.

Prima di abilitare la compressione degli oggetti, tenere presente quanto segue:

- Non selezionare **Comprimi oggetti memorizzati** a meno che non si sia certi che i dati memorizzati siano comprimibili.
- Le applicazioni che salvano oggetti in StorageGRID potrebbero comprimerli prima di salvarli. Se un'applicazione client ha già compresso un oggetto prima di salvarlo in StorageGRID, la selezione di questa opzione non ridurrà ulteriormente le dimensioni dell'oggetto.
- Non selezionare **Comprimi oggetti archiviati** se si utilizza NetApp FabricPool con StorageGRID.
- Se è selezionata l'opzione **Comprimi oggetti archiviati**, le applicazioni client S3 devono evitare di

eseguire operazioni `GetObject` che specificano un intervallo di byte da restituire. Queste operazioni di "lettura di intervallo" sono inefficienti perché StorageGRID deve effettivamente decomprimere gli oggetti per accedere ai byte richiesti. Le operazioni `GetObject` che richiedono un intervallo ridotto 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 potrebbero scadere.



Se è necessario comprimere oggetti e l'applicazione client deve utilizzare letture di intervallo, aumentare il timeout di lettura per l'applicazione.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Impostazioni di archiviazione > Compressione oggetti**.
2. Selezionare la casella di controllo **Comprimi oggetti memorizzati**.
3. Seleziona **Salva**.

Gestisci nodi di archiviazione completi

Quando i nodi di archiviazione raggiungono la capacità massima, è necessario espandere il sistema StorageGRID aggiungendo nuovo spazio di archiviazione. Sono disponibili tre opzioni: aggiunta di volumi di archiviazione, aggiunta di ripiani di espansione dell'archiviazione e aggiunta di nodi di archiviazione.

Aggiungere volumi di archiviazione

Ogni nodo di archiviazione supporta un numero massimo di volumi di archiviazione. Il massimo definito varia a seconda della piattaforma. Se un nodo di archiviazione contiene un numero di volumi di archiviazione inferiore al massimo consentito, è possibile aggiungere volumi per aumentarne la capacità. Vedi le istruzioni per ["espansione di un sistema StorageGRID"](#).

Aggiungere ripiani di espansione per lo stoccaggio

Alcuni nodi di archiviazione dell'appliance StorageGRID, come SG6060 o SG6160, possono supportare ripiani di archiviazione aggiuntivi. Se si dispone di dispositivi StorageGRID con capacità di espansione che non sono ancora stati ampliati alla capacità massima, è possibile aggiungere ripiani di archiviazione per aumentare la capacità. Vedi le istruzioni per ["espansione di un sistema StorageGRID"](#).

Aggiungi nodi di archiviazione

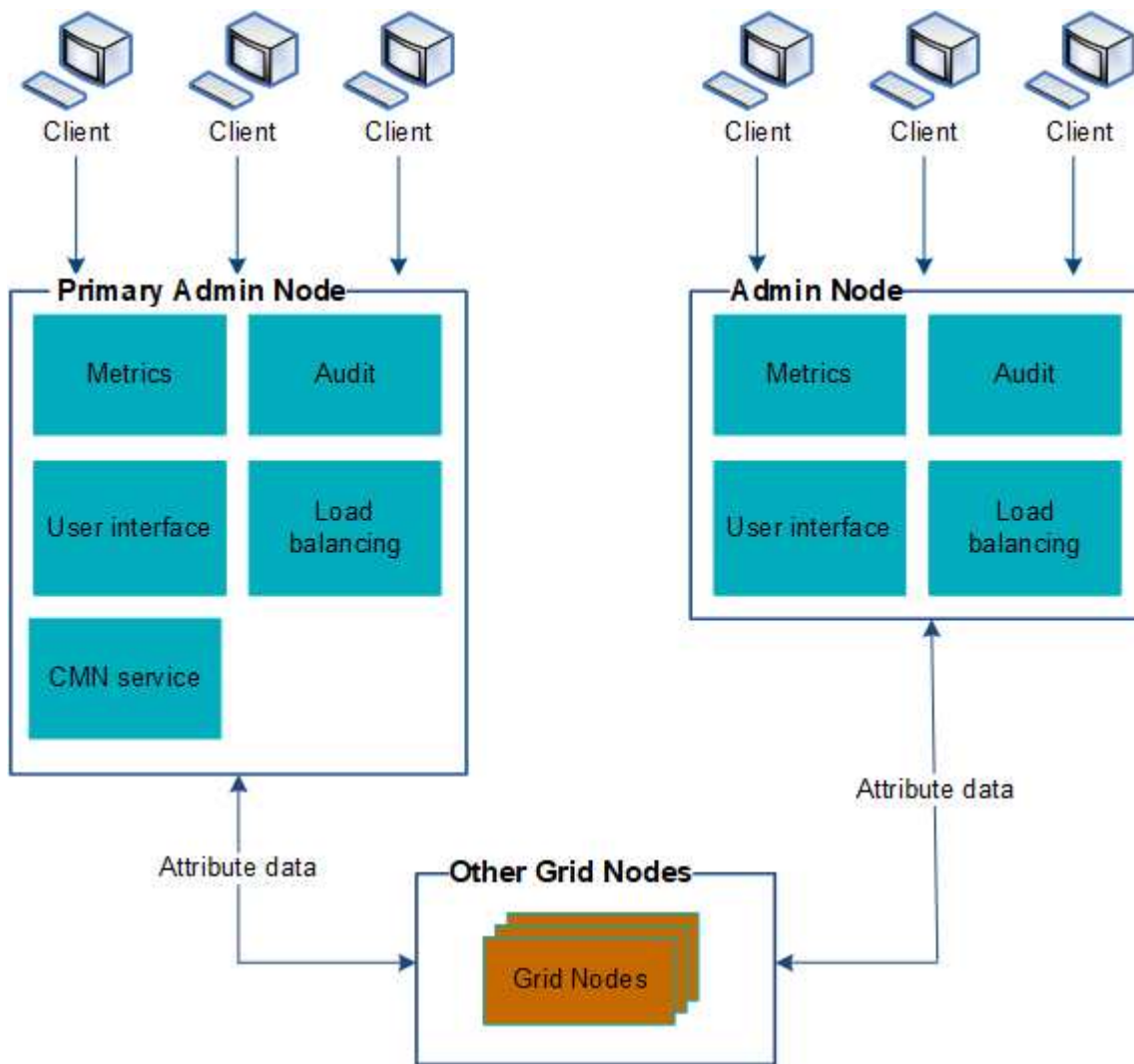
È possibile aumentare la capacità di archiviazione aggiungendo nodi di archiviazione. Quando si aggiunge spazio di archiviazione, è necessario valutare attentamente le regole ILM attualmente attive e i requisiti di capacità. Vedi le istruzioni per ["espansione di un sistema StorageGRID"](#).

Gestisci nodi amministrativi

Utilizzare più nodi di amministrazione

Un sistema StorageGRID può includere più nodi amministrativi per consentirti di monitorare e configurare continuamente il tuo sistema StorageGRID anche in caso di guasto di un nodo amministrativo.

Se un nodo di amministrazione non è più disponibile, l'elaborazione degli attributi continua, gli avvisi vengono comunque attivati e le notifiche e-mail e i pacchetti AutoSupport vengono comunque inviati. Tuttavia, la presenza di più nodi amministrativi non garantisce la protezione dal failover, fatta eccezione per le notifiche e i pacchetti AutoSupport.



Esistono 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 di amministrazione disponibile.
- Se un amministratore di sistema ha configurato un gruppo ad alta disponibilità di nodi amministrativi, i client Web possono continuare ad accedere a Grid Manager o Tenant Manager utilizzando l'indirizzo IP virtuale del gruppo HA. Vedere ["Gestire gruppi ad alta disponibilità"](#).



Quando si utilizza un gruppo HA, l'accesso viene interrotto se il nodo di amministrazione attivo non funziona. Gli utenti devono effettuare nuovamente l'accesso dopo che l'indirizzo IP virtuale del gruppo HA ha eseguito il failover su un altro nodo di amministrazione nel gruppo.

Alcune attività di manutenzione possono essere eseguite solo tramite il nodo di amministrazione primario. Se il nodo di amministrazione primario si guasta, è necessario ripristinarlo prima che il sistema StorageGRID torni a funzionare correttamente.

Identificare il nodo di amministrazione primario

Il nodo amministrativo primario offre più funzionalità rispetto ai nodi amministrativi non primari. Ad esempio, alcune procedure di manutenzione devono essere eseguite utilizzando il nodo di amministrazione primario.

Per ulteriori informazioni sui nodi di amministrazione, vedere ["Che cos'è un nodo di amministrazione"](#).

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Passi

1. Selezionare **NODES**.
2. Inserisci **primario** nella casella di ricerca.

Nei risultati della ricerca, identifica il nodo con "Nodo amministratore primario" visualizzato nella colonna Tipo. Dovrebbe essere elencato un nodo di amministrazione primario.

Visualizza lo stato delle notifiche e le code

Il servizio Network Management System (NMS) sui nodi amministrativi invia notifiche al server di posta. È possibile visualizzare lo stato attuale del servizio NMS e la dimensione della coda delle notifiche nella pagina Interface Engine.

Per accedere alla pagina Interface Engine, selezionare **SUPPORTO > Strumenti > Topologia griglia**. Quindi seleziona **site > Admin Node > NMS > Interface Engine**.

Overview	Alarms	Reports	Configuration
Main			
Overview: NMS (170-176) - Interface Engine Updated: 2009-03-09 10:12:17 PDT			
NMS Interface Engine Status:		Connected	
Connected Services:		15	
E-mail Notification Events			
E-mail Notifications Status:		No Errors	
E-mail Notifications Queued:		0	
Database Connection Pool			
Maximum Supported Capacity:		100	
Remaining Capacity:		95 %	
Active Connections:		5	

Le notifiche vengono elaborate tramite la coda delle notifiche 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, viene effettuato un tentativo di inviare nuovamente la notifica al server di posta per un periodo di 60 secondi. Se la notifica non viene inviata al server di posta entro 60 secondi, viene eliminata dalla coda delle notifiche e viene effettuato un tentativo di inviare la notifica successiva nella coda.

Gestire gli oggetti con ILM

Gestire gli oggetti con ILM

Le regole di gestione del ciclo di vita delle informazioni (ILM) in una policy ILM indicano a StorageGRID come creare e distribuire copie dei dati degli oggetti e come gestire tali copie nel tempo.

Informazioni su queste istruzioni

La progettazione e l'implementazione delle regole e delle 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 stabilire come si desidera che i diversi tipi di oggetti vengano copiati, distribuiti e archiviati.

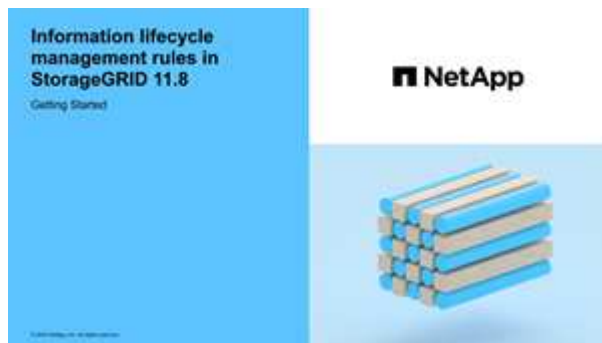
Utilizzare queste istruzioni per:

- Scopri di più su StorageGRID ILM, incluso ["come funziona l'ILM durante tutta la vita di un oggetto"](#).
- Scopri come configurare ["pool di stoccaggio"](#), ["Pool di archiviazione cloud"](#), e ["Regole ILM"](#).
- Impara come ["creare, simulare e attivare una politica ILM"](#) che proteggerà i dati degli oggetti su uno o più siti.
- Impara come ["gestire gli oggetti con S3 Object Lock"](#), che aiuta a garantire che gli oggetti in bucket S3 specifici non vengano eliminati o sovrascritti per un periodo di tempo specificato.

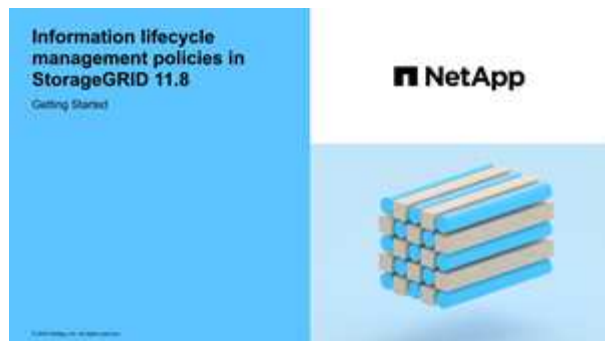
Saperne di più

Per saperne di più, guarda questi video:

- ["Video: panoramica delle regole ILM"](#).



- ["Video: Panoramica delle politiche ILM"](#)



ILM e ciclo di vita degli oggetti

Come funziona l'ILM durante la vita di un oggetto

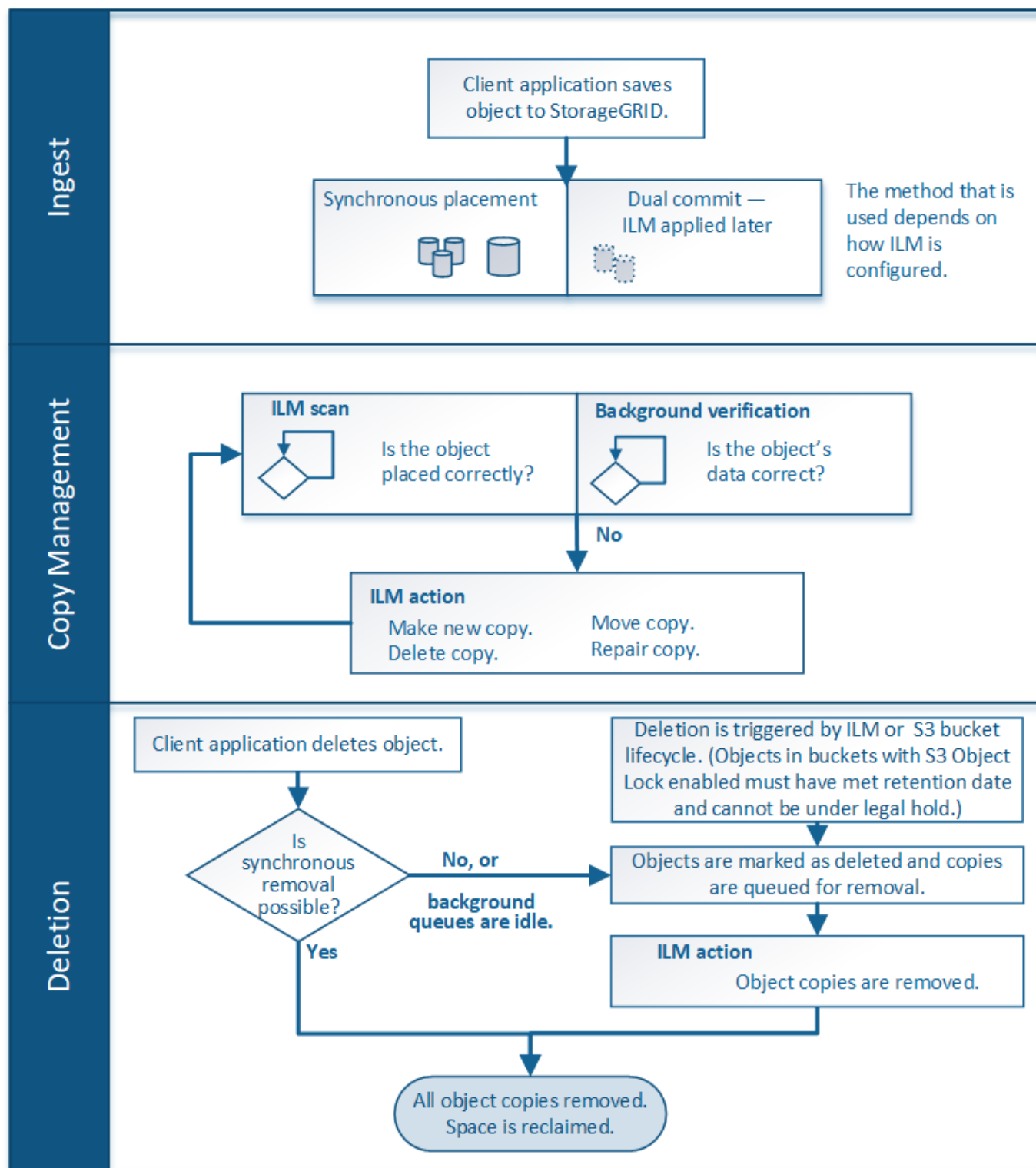
Comprendere come StorageGRID utilizza ILM per gestire gli oggetti in ogni fase del loro ciclo di vita può aiutarti a progettare una policy più efficace.

- **Ingest:** l'ingestione inizia quando un'applicazione client S3 stabilisce una connessione per salvare un oggetto nel sistema StorageGRID e termina quando StorageGRID restituisce al client un messaggio di "ingest riuscito". I dati degli oggetti vengono protetti durante l'acquisizione applicando immediatamente le istruzioni ILM (posizionamento sincrono) oppure creando copie provvisorie e applicando ILM in un secondo momento (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 dell'ILM, StorageGRID gestisce le posizioni degli oggetti e li protegge dalla perdita.
 - **Scansione e valutazione ILM:** StorageGRID esegue continuamente la scansione dell'elenco degli oggetti archiviati nella griglia e verifica se le copie correnti soddisfano i requisiti ILM. Quando sono necessari tipi, numeri o posizioni diverse di copie di oggetti, StorageGRID crea, elimina o sposta le copie in base alle necessità.
 - **Verifica in background:** StorageGRID esegue costantemente la verifica in background per controllare l'integrità dei dati degli oggetti. Se viene rilevato un problema, StorageGRID crea automaticamente una nuova copia dell'oggetto o un frammento di oggetto sostitutivo con codice di cancellazione 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 a seguito di una richiesta di eliminazione da parte di un client, oppure a seguito di un'eliminazione da parte di ILM o causata dalla scadenza del ciclo di vita di un bucket S3.



Gli oggetti in un bucket in cui è abilitato il blocco degli oggetti S3 non possono essere eliminati se sono soggetti a conservazione legale o se è stata specificata una data di conservazione fino a quando non è stata ancora rispettata.

Il diagramma riassume il funzionamento dell'ILM durante l'intero ciclo di vita di un oggetto.



Come vengono ingeriti gli oggetti

Opzioni di acquisizione

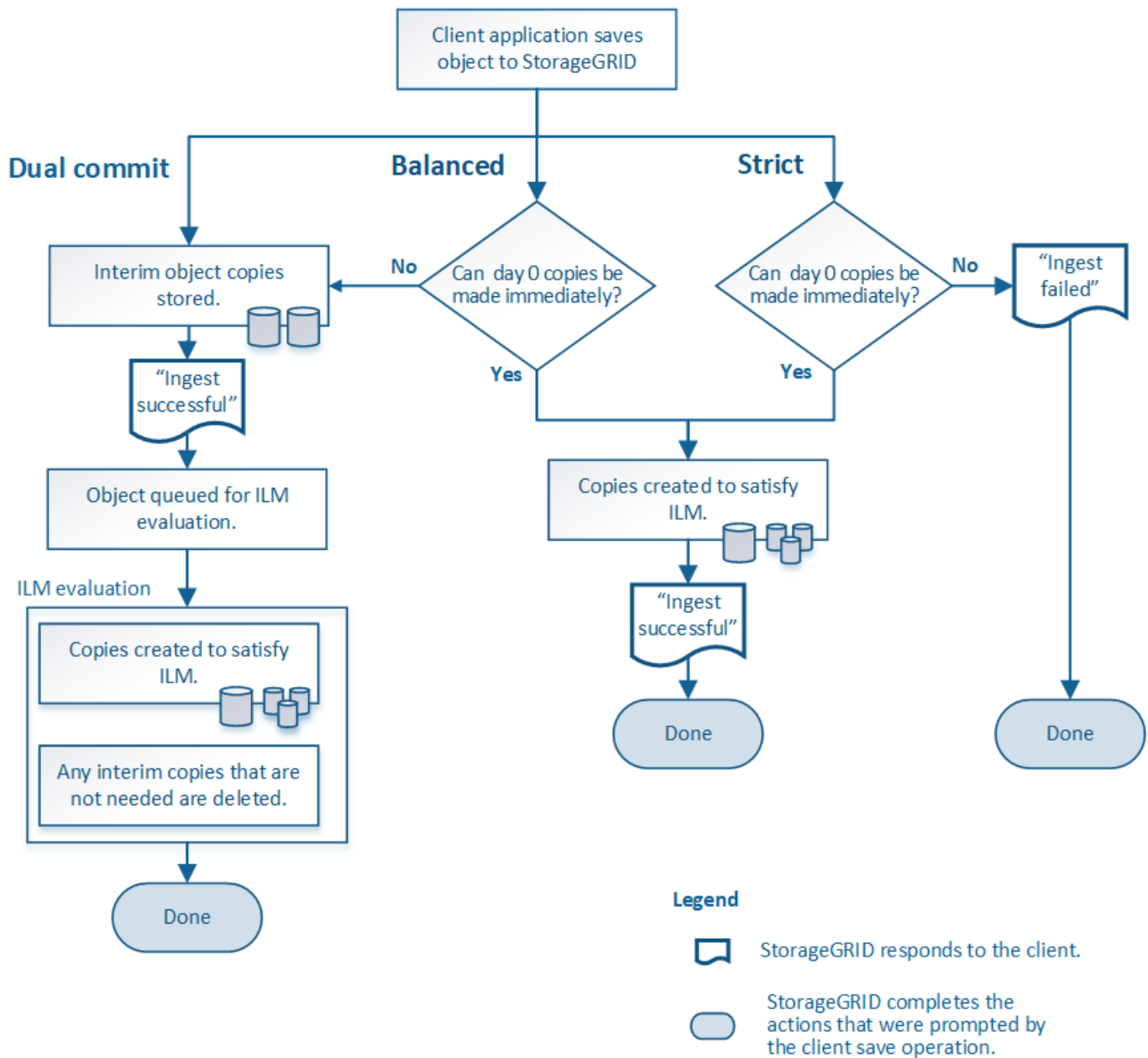
Quando si crea una regola ILM, si specifica una delle tre opzioni per la protezione degli oggetti in fase di acquisizione: Doppio commit, Rigoroso o Bilanciato.

A seconda della scelta, StorageGRID esegue copie provvisorie e mette in coda gli oggetti per una successiva

valutazione ILM, oppure utilizza il posizionamento sincrono ed esegue 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 abbinati da una regola ILM che utilizza ciascuna delle tre opzioni di acquisizione.



Doppio impegno

Quando si seleziona l'opzione Dual commit, StorageGRID esegue immediatamente copie provvisorie degli oggetti su due diversi nodi di archiviazione e restituisce al client un messaggio di "ingest riuscito". L'oggetto viene messo in coda per la valutazione ILM e in seguito vengono create copie che soddisfano le istruzioni di posizionamento della regola. Se la policy ILM non può essere elaborata immediatamente dopo il doppio commit, la protezione contro la perdita del sito potrebbe richiedere del tempo.

Utilizzare l'opzione Dual commit in uno di questi casi:

- Stai utilizzando regole ILM multi-sito e la latenza di acquisizione del client è la tua considerazione principale. Quando si utilizza il Dual commit, è necessario assicurarsi che la griglia possa eseguire il lavoro aggiuntivo di creazione e rimozione delle copie dual-commit se non soddisfano ILM. Nello specifico:
 - Il carico sulla rete deve essere sufficientemente basso da evitare un arretrato ILM.
 - La griglia deve disporre di risorse hardware in eccesso (IOPS, CPU, memoria, larghezza di banda di rete e così via).
- Si utilizzano regole ILM multi-sito e la connessione WAN tra i siti presenta solitamente un'elevata latenza o una larghezza di banda limitata. In questo scenario, l'utilizzo dell'opzione Dual commit può aiutare a prevenire i timeout del client. Prima di scegliere l'opzione Dual commit, è opportuno testare l'applicazione client con carichi di lavoro realistici.

Bilanciato (predefinito)

Quando si seleziona l'opzione Bilanciato, StorageGRID utilizza anche il posizionamento sincrono durante l'acquisizione ed esegue immediatamente tutte le copie specificate nelle istruzioni di posizionamento della regola. A differenza dell'opzione Strict, se StorageGRID non riesce a effettuare immediatamente tutte le copie, utilizza invece Dual commit. Se la policy ILM utilizza posizionamenti su più siti e non è possibile ottenere una protezione immediata contro la perdita del sito, viene attivato l'avviso **Posizionamento ILM non realizzabile**.

Utilizzare l'opzione Bilanciata per ottenere la migliore combinazione di protezione dei dati, prestazioni della griglia e successo dell'acquisizione. Bilanciato è l'opzione predefinita nella procedura guidata Crea regola ILM.

Rigoroso

Quando si seleziona l'opzione Rigorosa, StorageGRID utilizza il posizionamento sincrono durante l'acquisizione ed esegue 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 archiviazione richiesta non è temporaneamente disponibile. Il client deve riprovare l'operazione.

Utilizzare l'opzione Rigorosa se si ha un requisito operativo o normativo che impone di archiviare immediatamente gli oggetti solo nelle posizioni indicate nella regola ILM. Ad esempio, per soddisfare un requisito normativo, potrebbe essere necessario utilizzare l'opzione Rigorosa e un filtro avanzato Vincolo di posizione per garantire che gli oggetti non vengano mai archiviati in determinati data center.

Vedere ["Esempio 5: regole e policy ILM per un comportamento di acquisizione rigoroso"](#).

Vantaggi, svantaggi e limitazioni delle opzioni di ingestione

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 aiutarti a decidere quale selezionare per una regola ILM.

Per una panoramica delle opzioni di acquisizione, vedere ["Opzioni di acquisizione"](#).

Vantaggi delle opzioni Bilanciata e Rigorosa

Rispetto al Dual commit, che crea copie provvisorie durante l'acquisizione, le due opzioni di posizionamento sincrono possono offrire i seguenti vantaggi:

- **Maggiore sicurezza dei dati:** i dati degli oggetti vengono immediatamente protetti come specificato nelle istruzioni di posizionamento della regola ILM, che possono essere configurate per proteggere da un'ampia gamma di condizioni di errore, incluso l'errore di più di una posizione di archiviazione. Il doppio commit può

proteggere solo dalla perdita di una singola copia locale.

- **Funzionamento della griglia più efficiente:** ogni oggetto viene elaborato una sola volta, quando viene acquisito. Poiché il sistema StorageGRID non ha bisogno di tracciare o eliminare copie provvisorie, il carico di elaborazione è inferiore e viene consumato meno spazio nel database.
- **(Bilanciato) Consigliato:** l'opzione Bilanciata garantisce un'efficienza ILM ottimale. Si consiglia di utilizzare l'opzione Bilanciata, a meno che non sia richiesto un comportamento di ingestione rigoroso o che la griglia soddisfi tutti i criteri per l'utilizzo del commit doppio.
- **(Rigorosa) Certezza sulla posizione degli oggetti:** l'opzione Rigorosa garantisce che gli oggetti vengano immediatamente archiviati secondo le istruzioni di posizionamento nella regola ILM.

Svantaggi delle opzioni Bilanciata e Rigorosa

Rispetto al Dual commit, le opzioni Balanced e Strict presentano alcuni svantaggi:

- **Ingestione client più lunga:** le latenze di acquisizione client potrebbero essere più lunghe. Quando si utilizzano le opzioni Bilanciato o Rigoroso, il messaggio "ingest riuscito" non viene restituito al client finché non vengono creati e archiviati tutti i frammenti codificati in modo da essere cancellati o le copie replicate. Tuttavia, è molto probabile che i dati degli oggetti raggiungano la loro collocazione finale molto più rapidamente.
- **(Rigoroso) Maggiori tassi di errore di acquisizione:** con l'opzione Rigorosa, l'acquisizione fallisce ogni volta che StorageGRID non riesce a effettuare immediatamente tutte le copie specificate nella regola ILM. Si potrebbero verificare alti tassi di errore di acquisizione se una posizione di archiviazione richiesta è temporaneamente offline o se problemi di rete causano ritardi nella copia di oggetti tra siti.
- **(Rigoroso) In alcune circostanze, i posizionamenti dei carichi multiparte S3 potrebbero non essere quelli previsti:** con Rigoroso, ci si aspetta che gli oggetti vengano posizionati come descritto dalla regola ILM oppure che l'acquisizione non vada a buon fine. Tuttavia, con un caricamento multiparte S3, l'ILM viene valutato per ogni parte dell'oggetto mentre viene acquisito e per l'oggetto nel suo complesso quando il caricamento multiparte viene completato. Nelle seguenti circostanze, ciò potrebbe comportare posizionamenti diversi da quelli previsti:
 - **Se ILM cambia mentre è in corso un caricamento multiparte S3:** poiché ogni parte viene posizionata in base alla regola attiva al momento dell'acquisizione della parte, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento multiparte. In questi casi l'acquisizione dell'oggetto non fallisce. Invece, qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e successivamente spostata nella posizione corretta.
 - **Quando le regole ILM filtrano in base alle dimensioni:** quando si valuta ILM per una parte, StorageGRID filtra in base alle dimensioni della parte, non in base alle dimensioni dell'oggetto. Ciò significa che parti di un oggetto possono essere archiviate 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 vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, al momento dell'acquisizione ogni parte da 1 GB di un caricamento multiparte da 10 parti viene archiviata in DC2. Quando l'ILM viene valutato per l'oggetto, tutte le parti dell'oggetto vengono spostate in DC1.
- **(Rigoroso) L'inserimento non fallisce quando i tag degli oggetti o i metadati vengono aggiornati e non è possibile effettuare nuovi posizionamenti richiesti:** con Rigoroso, ci si aspetta che gli oggetti vengano posizionati come descritto dalla regola ILM oppure che l'inserimento fallisca. Tuttavia, quando si aggiornano i metadati o i tag per un oggetto già archiviato nella griglia, l'oggetto non viene reinserito. Ciò significa che le modifiche al posizionamento degli oggetti attivate dall'aggiornamento non vengono apportate immediatamente. Le modifiche al posizionamento vengono apportate quando l'ILM viene rivalutato tramite i normali processi ILM in background. Se non è possibile apportare le modifiche di posizionamento richieste (ad esempio perché una posizione appena richiesta non è disponibile), l'oggetto aggiornato mantiene la sua posizione attuale finché non saranno possibili le modifiche di posizionamento.

Limitazioni sul posizionamento degli oggetti con le opzioni Bilanciato e Rigoroso

Le opzioni Bilanciato o Rigoroso non possono essere utilizzate per le regole ILM che hanno una qualsiasi di queste istruzioni di posizionamento:

- Posizionamento in un Cloud Storage Pool al giorno 0.
- Posizionamenti in un pool di archiviazione cloud quando la regola ha un orario di creazione definito dall'utente come orario di riferimento.

Queste restrizioni esistono perché StorageGRID non può creare copie sincrone su un Cloud Storage Pool e un orario di creazione definito dall'utente potrebbe essere risolto nel presente.

Come le regole e la coerenza ILM interagiscono per influenzare la protezione dei dati

Sia la regola ILM che la scelta della coerenza influiscono sul modo in cui gli oggetti vengono protetti. 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 quando un oggetto viene archiviato influisce sul posizionamento iniziale dei metadati degli oggetti. Poiché StorageGRID richiede l'accesso sia ai dati che ai metadati di un oggetto per soddisfare le richieste dei client, la selezione di livelli di protezione corrispondenti per la coerenza e il comportamento di acquisizione può garantire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Ecco un breve riepilogo dei valori di coerenza disponibili in StorageGRID:

- **Tutti:** tutti i nodi ricevono immediatamente i metadati dell'oggetto, altrimenti la richiesta non andrà a buon fine.
- **Strong-global:** i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti. Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti.
- **Strong-site:** i metadati degli oggetti vengono immediatamente distribuiti agli altri nodi del sito. Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito.
- **Lettura dopo nuova scrittura:** garantisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
- **Disponibile:** fornisce 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 letti raramente o per operazioni HEAD o GET su chiavi inesistenti). 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 comprenderne i vantaggi e le limitazioni.

Esempio di come la coerenza e le regole ILM possono interagire

Supponiamo di avere una griglia a due siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM:** creare due copie dell'oggetto, una nel sito locale e una in un sito remoto. Utilizzare un comportamento di acquisizione rigoroso.
- **coerenza:** Strong-global (i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie dell'oggetto e

distribuisce i metadati a entrambi i siti prima di restituire l'esito positivo al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione corretta del messaggio. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, copie sia dei dati dell'oggetto sia dei metadati dell'oggetto sono ancora presenti nel sito remoto. L'oggetto è completamente recuperabile.

Se invece si utilizzasse la stessa regola ILM e la coerenza del sito forte, il client potrebbe ricevere un messaggio di successo dopo che i dati dell'oggetto sono stati replicati sul sito remoto, ma prima che i metadati dell'oggetto vengano distribuiti lì. 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 subito dopo l'acquisizione, anche i metadati dell'oggetto vengono persi. L'oggetto non può essere recuperato.

L'interrelazione tra coerenza e regole ILM può essere complessa. Se hai bisogno di assistenza, contatta NetApp .

Informazioni correlate

["Esempio 5: regole e policy ILM per un comportamento di acquisizione rigoroso"](#)

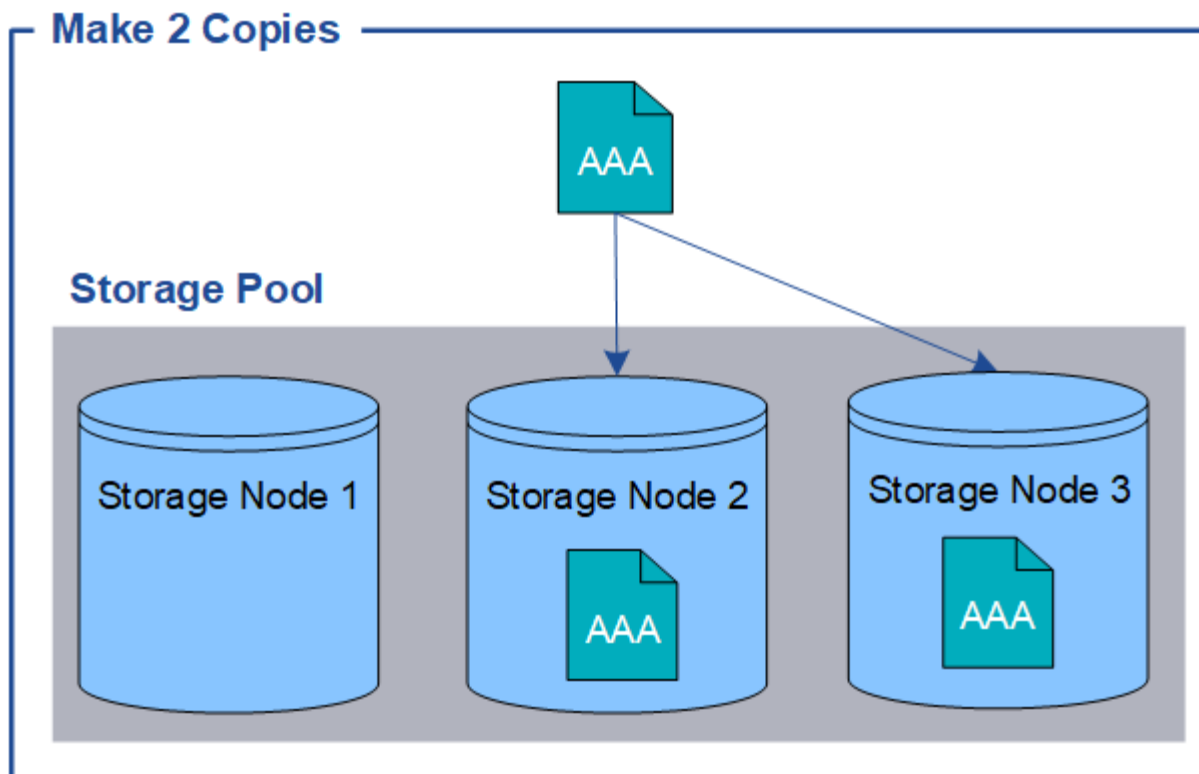
Come vengono memorizzati gli oggetti (codifica di replicazione o cancellazione)

Che cosa è la replicazione?

La replica è uno dei due metodi utilizzati da StorageGRID per archiviare i dati degli oggetti (l'altro metodo è la codifica di cancellazione). Quando gli oggetti corrispondono a una regola ILM che utilizza la replica, il sistema crea copie esatte dei dati dell'oggetto e memorizza le copie sui nodi di archiviazione.

Quando si configura una regola ILM per creare copie replicate, si specifica quante copie devono essere create, dove devono essere posizionate e per quanto tempo devono essere conservate in ogni posizione.

Nell'esempio seguente, la regola ILM specifica che due copie replicate di ciascun oggetto devono essere posizionate in un pool di archiviazione contenente tre nodi di archiviazione.



Quando StorageGRID abbina gli oggetti a questa regola, crea due copie dell'oggetto, posizionando ciascuna copia su un diverso nodo di archiviazione nel pool di archiviazione. Le due copie possono essere posizionate su due qualsiasi dei tre nodi di archiviazione disponibili. In questo caso, la regola ha posizionato copie degli oggetti sui nodi di archiviazione 2 e 3. Poiché sono presenti due copie, l'oggetto può essere recuperato se uno qualsiasi dei nodi nel pool di archiviazione si guasta.



StorageGRID può archiviare solo una copia replicata di un oggetto su un dato nodo di archiviazione. Se la griglia include tre nodi di archiviazione e si crea una regola ILM a 4 copie, verranno create solo tre copie: una copia per ciascun nodo di archiviazione. L'avviso **Posizionamento ILM non realizzabile** viene attivato per indicare che la regola ILM non può essere applicata completamente.

Informazioni correlate

- ["Che cosa è la codifica di cancellazione"](#)
- ["Che cos'è un pool di archiviazione"](#)
- ["Abilita la protezione contro la perdita del sito utilizzando la codifica di replicazione e cancellazione"](#)

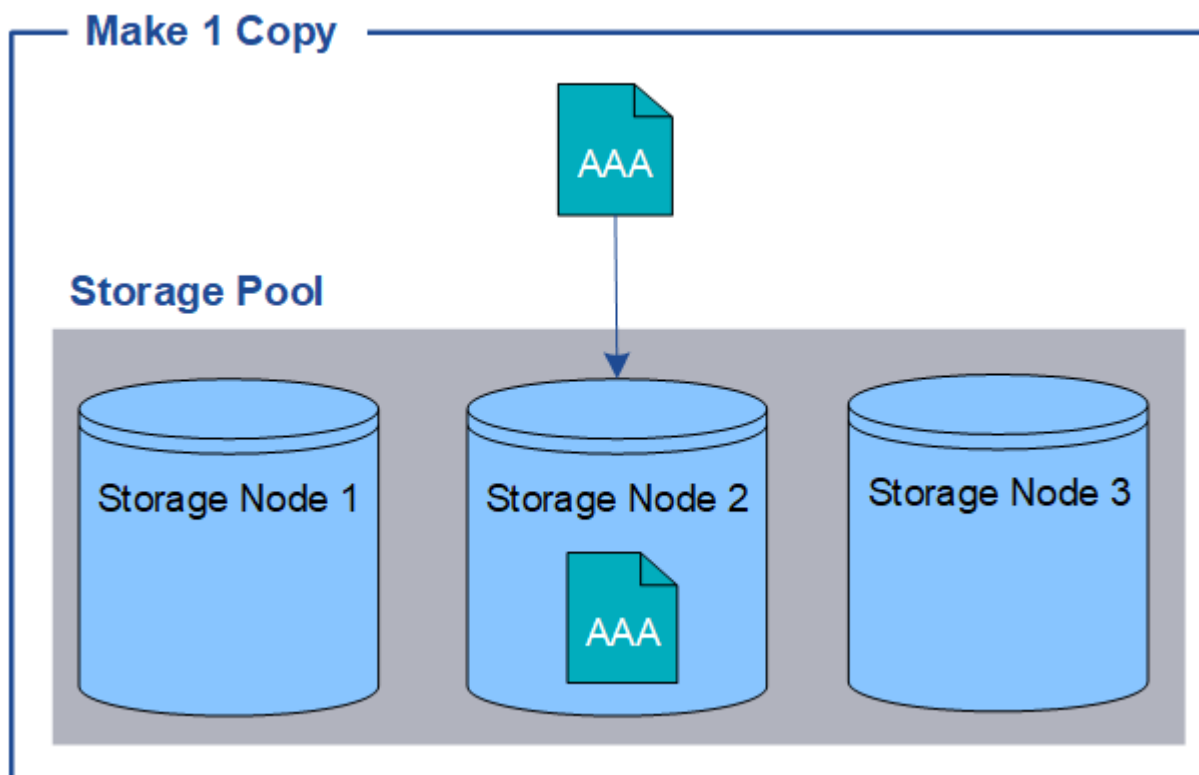
Perché non dovresti usare la replicazione a copia singola

Quando si crea una regola ILM per creare copie replicate, è necessario specificare sempre almeno due copie per qualsiasi periodo di tempo nelle istruzioni di posizionamento.

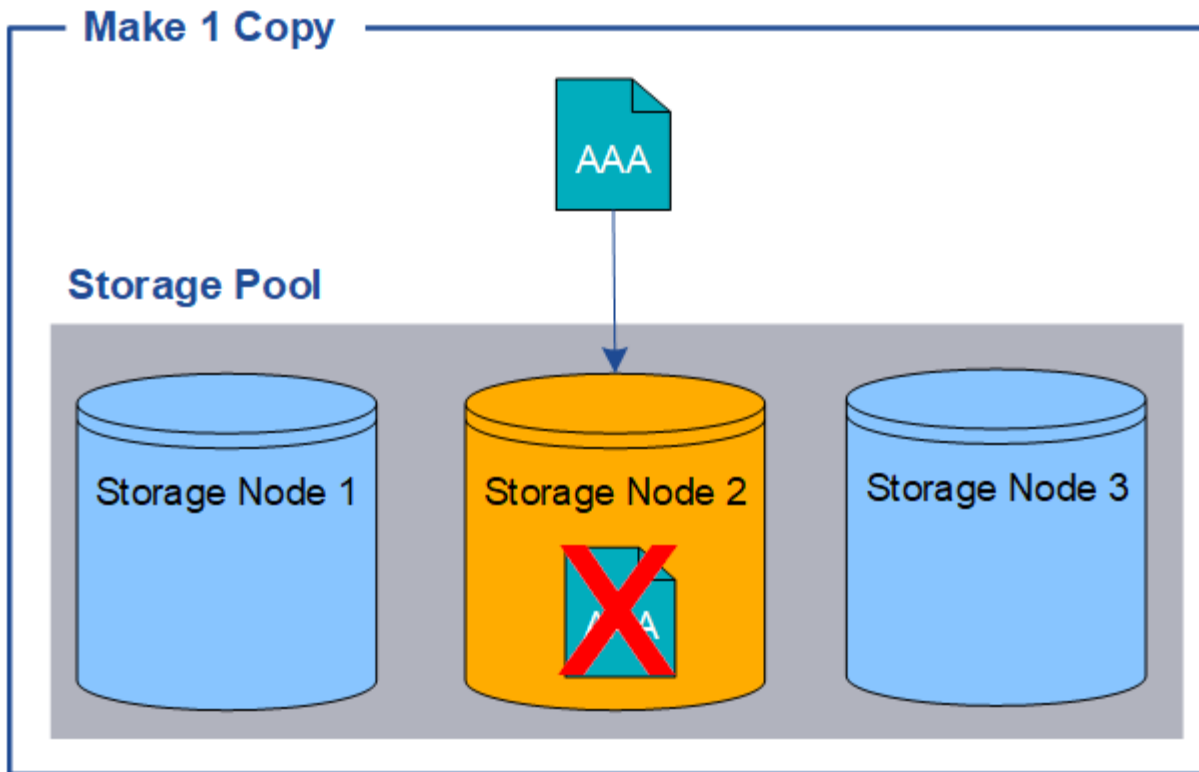


Non utilizzare una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

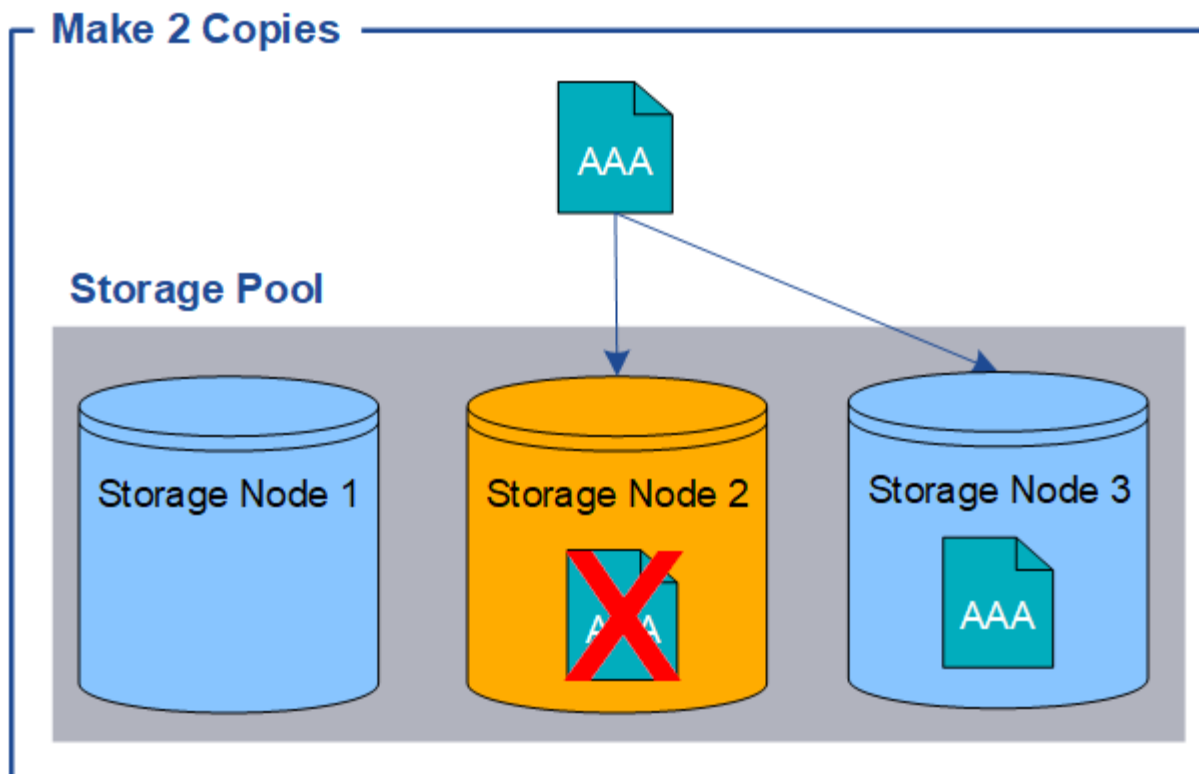
Nell'esempio seguente, la regola ILM Make 1 Copy specifica che una copia replicata di un oggetto venga inserita in un pool di archiviazione contenente tre nodi di archiviazione. Quando viene acquisito un oggetto che corrisponde a questa regola, StorageGRID ne posiziona una singola copia su un solo nodo di archiviazione.



Quando una regola ILM crea una sola copia replicata di un oggetto, l'oggetto diventa inaccessibile quando il nodo di archiviazione non è disponibile. In questo esempio, si perderà temporaneamente l'accesso all'oggetto AAA ogni volta che Storage Node 2 è offline, ad esempio durante un aggiornamento o un'altra procedura di manutenzione. Se il nodo di archiviazione 2 si guasta, l'oggetto AAA verrà perso completamente.



Per evitare di perdere i dati degli oggetti, è consigliabile effettuare sempre 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 archiviazione si guasta o va offline.



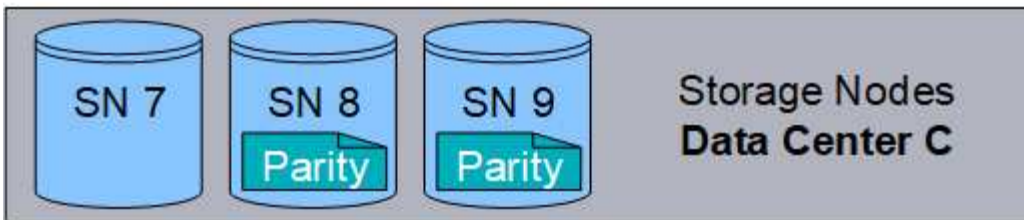
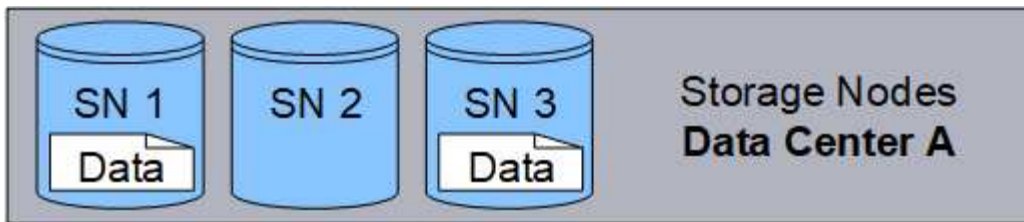
Che cos'è la codifica di cancellazione?

La codifica di cancellazione è uno dei due metodi utilizzati StorageGRID per archiviare i dati degli oggetti (l'altro metodo è la replica). Quando gli oggetti corrispondono a una regola ILM che utilizza la codifica di cancellazione, tali oggetti vengono suddivisi in frammenti di dati, vengono calcolati frammenti di parità aggiuntivi e ogni frammento viene archiviato su un diverso nodo di archiviazione.

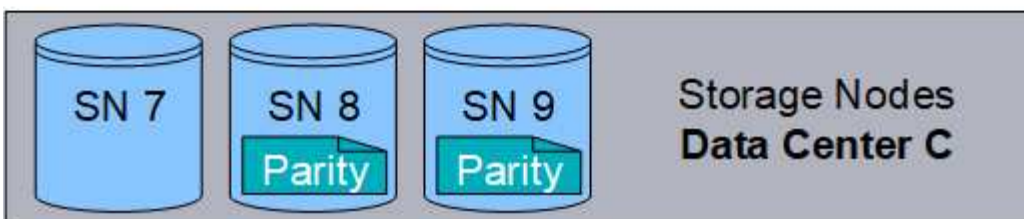
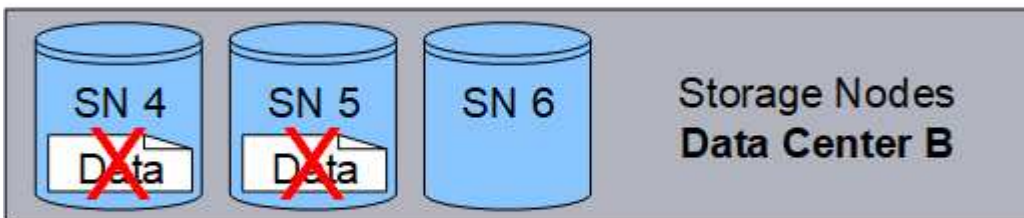
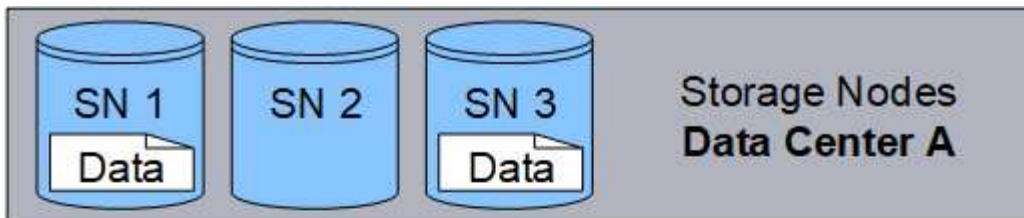
Quando si accede a un oggetto, questo viene riassembleato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità si danneggia o viene perso, l'algoritmo di codifica di cancellazione può ricreare quel frammento utilizzando un sottoinsieme dei dati e dei frammenti di parità rimanenti.

Quando si creano regole ILM, StorageGRID crea profili di codifica di cancellazione che supportano tali regole. È possibile visualizzare un elenco di profili di codifica di cancellazione, ["rinominare un profilo di codifica di cancellazione"](#), o ["disattivare un profilo di codifica di cancellazione se non è attualmente utilizzato in nessuna regola ILM"](#).

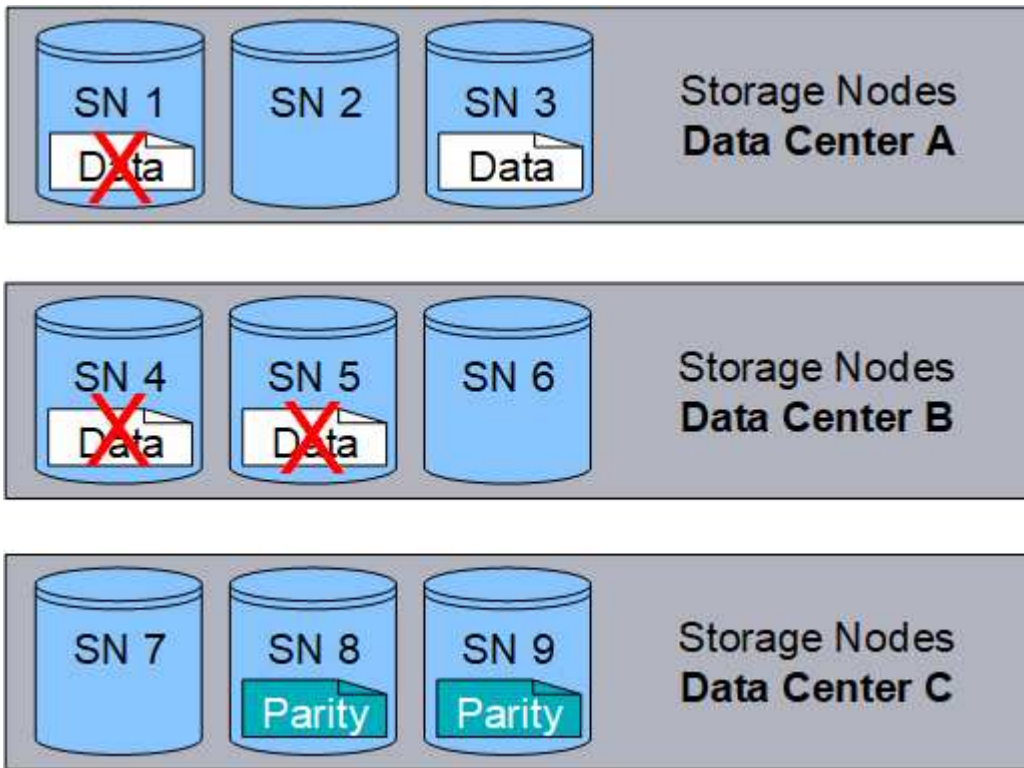
L'esempio seguente illustra l'uso di un algoritmo di codifica di cancellazione sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di codifica di cancellazione 4+2. Ogni oggetto viene suddiviso in quattro frammenti di dati uguali e dai dati dell'oggetto vengono calcolati due frammenti di parità. Ciascuno dei sei frammenti viene archiviato su un nodo diverso in tre siti di data center per garantire la protezione dei dati in caso di guasti dei nodi o perdite del sito.



Lo schema di codifica a cancellazione 4+2 può essere configurato in vari modi. Ad esempio, è possibile configurare un pool di archiviazione a sito singolo contenente sei nodi di archiviazione. Per ["protezione contro la perdita del sito"](#), è possibile utilizzare un pool di archiviazione contenente tre siti con tre nodi di archiviazione in ciascun sito. Un oggetto può essere recuperato finché rimangono disponibili quattro dei sei frammenti (dati o parità). È possibile perdere fino a due frammenti senza perdere i dati dell'oggetto. Se un intero sito viene perso, l'oggetto può comunque essere recuperato o riparato, a patto che tutti gli altri frammenti rimangano accessibili.



Se vengono persi più di due nodi di archiviazione, l'oggetto non sarà recuperabile.



Informazioni correlate

- ["Che cosa è la replicazione"](#)
- ["Che cos'è un pool di archiviazione"](#)
- ["Cosa sono gli schemi di codifica di cancellazione"](#)
- ["Rinominare un profilo di codifica di cancellazione"](#)
- ["Disattivare un profilo di codifica di cancellazione"](#)

Cosa sono gli schemi di codifica di cancellazione?

Gli schemi di codifica di cancellazione controllano quanti frammenti di dati e quanti frammenti di parità vengono creati per ciascun oggetto.

Quando si crea o si modifica una regola ILM, si seleziona uno schema di codifica di cancellazione disponibile. StorageGRID crea automaticamente schemi di codifica di cancellazione in base al numero di nodi di archiviazione e siti che compongono il pool di archiviazione che si intende utilizzare.

Protezione dei dati

Il sistema StorageGRID utilizza l'algoritmo di codifica della cancellazione Reed-Solomon. L'algoritmo divide un oggetto in k frammenti di dati e calcoli m frammenti di parità.

IL $k + m = n$ i frammenti sono sparsi n Nodi di archiviazione per garantire la protezione dei dati come segue:

- Per recuperare o riparare un oggetto, k sono necessari frammenti.
- Un oggetto può sostenere fino a m frammenti persi o corrotti. Più alto è il valore di m , maggiore è la tolleranza al guasto.

La migliore protezione dei dati è fornita dallo schema di codifica di cancellazione con la più alta tolleranza ai guasti del nodo o del volume all'interno di un pool di archiviazione.

Spese di archiviazione generali

Il sovraccarico di archiviazione di uno schema di codifica di cancellazione viene calcolato dividendo il numero di frammenti di parità(m) dal numero di frammenti di dati(k). È possibile utilizzare il sovraccarico di archiviazione per calcolare la quantità di spazio su disco richiesta da ciascun oggetto con codice di cancellazione:

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Ad esempio, se si archivia un oggetto da 10 MB utilizzando lo schema 4+2 (che ha un overhead di archiviazione del 50%), l'oggetto consuma 15 MB di spazio di archiviazione della griglia. Se si memorizza lo stesso oggetto da 10 MB utilizzando lo schema 6+2 (che ha un overhead di archiviazione del 33%), l'oggetto consuma circa 13,3 MB.

Selezionare lo schema di codifica di cancellazione con il valore totale più basso di $k+m$ che soddisfa le tue esigenze. Gli schemi di codifica di cancellazione con un numero inferiore di frammenti sono più efficienti dal punto di vista computazionale perché:

- Vengono creati e distribuiti (o recuperati) meno frammenti per oggetto
- Hanno prestazioni migliori perché la dimensione del frammento è maggiore
- Possono richiedere che vengano aggiunti meno nodi in un'[espansione quando è necessario più spazio di archiviazione](#)

Linee guida per i pool di stoccaggio

Quando si seleziona il pool di archiviazione da utilizzare per una regola che creerà una copia con codice di cancellazione, attenersi alle seguenti linee guida per i pool di archiviazione:

- Il pool di archiviazione deve includere tre o più siti oppure esattamente un sito.



Non è possibile utilizzare la codifica di cancellazione se il pool di archiviazione include due siti.

- [Schemi di codifica di cancellazione per pool di archiviazione contenenti tre o più siti](#)
- [Schemi di codifica di cancellazione per pool di archiviazione monosito](#)
- Non utilizzare un pool di archiviazione che includa il sito Tutti i siti.
- Il pool di archiviazione dovrebbe includere almeno $k+m + 1$ Nodi di archiviazione in grado di archiviare dati di oggetti.



Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano solo metadati degli oggetti e non dati degli oggetti. Per ulteriori informazioni, consultare ["Tipi di nodi di archiviazione"](#).

Il numero minimo di nodi di archiviazione richiesti è $k+m$. Tuttavia, avere almeno un nodo di archiviazione aggiuntivo può aiutare a prevenire errori di acquisizione o arretrati ILM se un nodo di archiviazione necessario non è temporaneamente disponibile.

Schemi di codifica di cancellazione per pool di archiviazione contenenti tre o più siti

Nella tabella seguente vengono descritti gli schemi di codifica di cancellazione attualmente supportati da StorageGRID per i pool di archiviazione che includono tre o più siti. Tutti questi schemi garantiscono una protezione contro le perdite del sito. Anche se un sito può andare perso, l'oggetto sarà comunque accessibile.

Per gli schemi di codifica di cancellazione che forniscono protezione contro la perdita del sito, il numero consigliato di nodi di archiviazione nel pool di archiviazione supera $k+m + 1$ perché ogni sito richiede un minimo di tre nodi di archiviazione.

Schema di codifica di cancellazione ($k+m$)	Numero minimo di siti distribuiti	Numero consigliato di nodi di archiviazione in ogni sito	Numero totale consigliato di nodi di archiviazione	Protezione contro le perdite del sito?	Spese di archiviazione generali
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%
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 archiviazione per sito. Per utilizzare lo schema 7+5, ogni sito richiede un minimo di quattro nodi di archiviazione. Si consiglia di utilizzare cinque nodi di archiviazione per sito.

Quando si seleziona uno schema di codifica di cancellazione che garantisca la protezione del sito, è necessario valutare 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.
- **Tolleranza ai guasti:** la tolleranza ai guasti aumenta avendo più segmenti di parità (ovvero, quando m ha un valore più alto.)
- **Traffico di rete:** durante il ripristino da guasti, utilizzando uno schema con più frammenti (ovvero, un totale più elevato per $k+m$) crea più traffico di rete.
- **Sovraccarico di archiviazione:** gli schemi con sovraccarico più elevato richiedono più spazio di archiviazione per oggetto.

Ad esempio, quando si decide tra uno schema 4+2 e uno schema 6+3 (entrambi con un overhead di archiviazione del 50%), selezionare lo schema 6+3 se è richiesta una tolleranza agli errori aggiuntiva. Selezionare lo schema 4+2 se le risorse di rete sono limitate. Se tutti gli altri fattori sono uguali, seleziona 4+2 perché ha un numero totale di frammenti inferiore.



Se non sei sicuro di quale schema utilizzare, seleziona 4+2 o 6+3 oppure contatta l'assistenza tecnica.

Schemi di codifica di cancellazione per pool di archiviazione monosito

Un pool di archiviazione con un solo sito supporta tutti gli schemi di codifica di cancellazione definiti per tre o più siti, a condizione che il sito disponga di un numero sufficiente di nodi di archiviazione.

Il numero minimo di nodi di archiviazione richiesti è $k+m$, ma un pool di archiviazione con $k+m + 1$ Si consiglia l'uso di Storage Nodes. Ad esempio, lo schema di codifica di cancellazione 2+1 richiede un pool di archiviazione con un minimo di tre nodi di archiviazione, ma si consigliano quattro nodi di archiviazione.

Schema di codifica di cancellazione ($k+m$)	Numero minimo di nodi di archiviazione	Numero consigliato di nodi di archiviazione	Spese di archiviazione generali
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 della codifica di cancellazione

Prima di decidere se utilizzare la codifica di replicazione o di cancellazione per proteggere i dati degli oggetti dalla perdita, è necessario comprendere i vantaggi, gli svantaggi e i requisiti della codifica di cancellazione.

Vantaggi della codifica di cancellazione

Rispetto alla replicazione, la codifica di cancellazione offre maggiore affidabilità, disponibilità ed efficienza di archiviazione.

- **Affidabilità:** l'affidabilità viene misurata in termini di tolleranza ai guasti, ovvero il numero di guasti simultanei che possono essere sostenuti senza perdita di dati. Con la replicazione, più copie identiche vengono archiviate su nodi diversi e in più siti. Con la codifica di cancellazione, un oggetto viene codificato in frammenti di dati e parità e distribuito su molti nodi e siti. Questa dispersione garantisce protezione contro i guasti sia del sito che del nodo. Rispetto alla replicazione, la codifica di cancellazione garantisce una maggiore affidabilità a costi di archiviazione comparabili.
- **Disponibilità:** la disponibilità può essere definita come la capacità di recuperare oggetti se i nodi di archiviazione falliscono o diventano inaccessibili. Rispetto alla replicazione, la codifica di cancellazione garantisce una maggiore disponibilità a costi di archiviazione comparabili.
- **Efficienza di archiviazione:** per livelli simili di disponibilità e affidabilità, gli oggetti protetti tramite codifica di cancellazione consumano meno spazio su disco rispetto a quanto farebbero se protetti tramite replica. Ad esempio, un oggetto da 10 MB replicato su due siti consuma 20 MB di spazio su disco (due copie), mentre un oggetto codificato con cancellazione su tre siti con uno schema di codifica con cancellazione 6+3 consuma solo 15 MB di spazio su disco.



Lo spazio su disco per gli oggetti con codice di cancellazione viene calcolato sommando le dimensioni dell'oggetto al sovraccarico di archiviazione. La percentuale di sovraccarico di archiviazione è il numero di frammenti di parità diviso per il numero di frammenti di dati.

Svantaggi della codifica di cancellazione

Rispetto alla replicazione, la codifica a cancellazione presenta i seguenti svantaggi:

- Si consiglia un numero maggiore di nodi e siti di archiviazione, a seconda dello schema di codifica di cancellazione. Al contrario, se si replicano i dati degli oggetti, è necessario un solo nodo di archiviazione per ogni copia. Vedere ["Schemi di codifica di cancellazione per pool di archiviazione contenenti tre o più siti"](#) E ["Schemi di codifica di cancellazione per pool di archiviazione monosito"](#) .
- Aumento dei costi e della complessità delle espansioni di storage. Per espandere una distribuzione che utilizza la replica, è necessario aggiungere capacità di archiviazione in ogni posizione in cui vengono eseguite le copie degli oggetti. Per espandere una distribuzione che utilizza la codifica di cancellazione, è necessario considerare sia lo schema di codifica di cancellazione in uso sia il livello di riempimento dei nodi di archiviazione esistenti. Ad esempio, se si attende che i nodi esistenti siano pieni al 100%, è necessario aggiungere almeno $k+m$ Nodi di archiviazione, ma se si espande quando i nodi esistenti sono pieni al 70%, è possibile aggiungere due nodi per sito e continuare a massimizzare la capacità di archiviazione utilizzabile. Per ulteriori informazioni, consultare ["Aggiungere capacità di archiviazione per oggetti con codice di cancellazione"](#) .
- Quando si utilizza la codifica di cancellazione su siti distribuiti geograficamente, si verificano latenze di recupero maggiori. I frammenti di un oggetto codificato in modo da essere cancellato e distribuito su siti remoti richiedono più tempo per essere recuperati tramite connessioni WAN rispetto a un oggetto replicato e disponibile localmente (lo stesso sito a cui si connette il client).
- Quando si utilizza la codifica di cancellazione su siti distribuiti geograficamente, si verifica un utilizzo maggiore del traffico di rete WAN per recuperi e riparazioni, in particolare per oggetti recuperati frequentemente o per riparazioni di oggetti su connessioni di rete WAN.
- Quando si utilizza la codifica di cancellazione su più siti, la velocità massima di elaborazione degli oggetti diminuisce drasticamente all'aumentare della latenza di rete tra i siti. Questa diminuzione è dovuta alla corrispondente diminuzione della velocità di trasmissione della rete TCP, che influisce sulla velocità con cui il sistema StorageGRID può archiviare e recuperare frammenti di oggetti.
- Maggiore utilizzo delle risorse di elaborazione.

Quando utilizzare la codifica di cancellazione

La codifica di cancellazione è più adatta ai seguenti requisiti:

- Oggetti di dimensioni superiori a 1 MB.



La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

- Archiviazione a lungo termine o a freddo per contenuti recuperati raramente.
- Elevata disponibilità e affidabilità dei dati.
- Protezione contro guasti completi del sito e del nodo.
- Efficienza di archiviazione.
- Distribuzioni in un unico sito che richiedono una protezione efficiente dei dati con una sola copia con codice di cancellazione anziché più copie replicate.
- Distribuzioni multi-sito in cui la latenza tra i siti è inferiore a 100 ms.

Come viene determinata la ritenzione dell'oggetto

StorageGRID offre opzioni sia agli amministratori della griglia sia ai singoli utenti tenant per specificare per quanto tempo archiviare gli 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 tenant possono utilizzare questi metodi per controllare per quanto tempo i loro oggetti vengono archiviati in StorageGRID:

- Se l'impostazione globale Blocco oggetti S3 è abilitata per la griglia, gli utenti del tenant S3 possono creare bucket con Blocco oggetti S3 abilitato e quindi selezionare un **Periodo di conservazione predefinito** per ciascun bucket.
- Se l'impostazione globale S3 Object Lock è abilitata 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 di scadenza e di conservazione legale per ogni versione dell'oggetto aggiunta a tale bucket.
 - Una versione di un oggetto sottoposta a conservazione legale non può essere eliminata con alcun metodo.
 - Prima che venga raggiunta la data di conservazione di una versione di un oggetto, tale versione non può essere eliminata con alcun metodo.
 - Gli oggetti nei bucket con S3 Object Lock 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. Vedere ["Gestisci gli oggetti con S3 Object Lock"](#).
- Gli utenti del tenant S3 possono aggiungere ai propri bucket una configurazione del ciclo di vita che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID archivia un oggetto finché non viene raggiunta la data o il numero di giorni specificati nell'azione Scadenza, a meno che il client non elimini prima l'oggetto. Vedere ["Crea la configurazione del ciclo di vita S3"](#).

- Un client S3 può inviare una richiesta di eliminazione di un oggetto. StorageGRID dà sempre priorità alle richieste di eliminazione del client rispetto al ciclo di vita del bucket S3 o all'ILM quando decide se eliminare o conservare un oggetto.

Come gli amministratori della griglia controllano la conservazione degli oggetti

Gli amministratori della griglia possono utilizzare questi metodi per controllare la conservazione degli oggetti:

- Imposta un periodo massimo di conservazione del blocco degli oggetti S3 per ciascun tenant. Quindi, gli utenti tenant possono impostare un periodo di conservazione predefinito per ciascuno dei loro bucket. Il periodo di conservazione massimo viene applicato anche a tutti gli oggetti appena acquisiti per quel bucket (data di conservazione dell'oggetto).
- Creare istruzioni di posizionamento ILM per controllare per quanto tempo gli oggetti vengono conservati. Quando gli oggetti corrispondono a una regola ILM, StorageGRID li memorizza finché non è trascorso l'ultimo periodo di tempo nella regola ILM. Gli oggetti vengono conservati indefinitamente se nelle istruzioni di posizionamento è specificato "per sempre".
- Indipendentemente da chi controlla per quanto tempo gli oggetti vengono conservati, le impostazioni ILM controllano quali tipi di copie degli oggetti (replicate o con codice di cancellazione) vengono archiviate e dove si trovano le copie (nodi di archiviazione o pool di archiviazione cloud).

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 mantenuto sulla griglia anche dopo che sono scadute tutte le istruzioni ILM per il posizionamento dell'oggetto.

Esempi di conservazione degli oggetti

Per comprendere meglio le interazioni tra S3 Object Lock, impostazioni del ciclo di vita del bucket, richieste di eliminazione client e ILM, prendere in considerazione i seguenti esempi.

Esempio 1: il ciclo di vita del bucket S3 conserva gli oggetti più a lungo di ILM

ILM

Conservare 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 conservati più a lungo di quanto specificato da ILM, StorageGRID continua a utilizzare le istruzioni di posizionamento ILM quando determina il numero e il tipo di copie da archiviare. In questo esempio, due copie dell'oggetto continueranno a essere archiviate in StorageGRID dal giorno 366 al giorno 730.

Esempio 2: il ciclo di vita del bucket S3 fa scadere gli oggetti prima di ILM

ILM

Conservare due copie per 2 anni (730 giorni)

Ciclo di vita del bucket

Scadenza degli 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

Conserva due copie sui nodi di archiviazione "per sempre"

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Richiesta di eliminazione del cliente

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 oggetto S3

La data di conservazione per una versione dell'oggetto è il 31/03/2026. Non è in vigore alcun blocco legale.

Regola ILM conforme

Conserva due copie sui nodi di archiviazione "per sempre"

Richiesta di eliminazione del cliente

Pubblicato il 31/03/2024

Risultato

StorageGRID non eliminerà la versione dell'oggetto perché la data di conservazione è ancora lontana 2 anni.

Come vengono eliminati gli oggetti

StorageGRID può eliminare oggetti in risposta diretta a una richiesta del client oppure automaticamente in seguito alla scadenza del ciclo di vita di un bucket S3 o ai requisiti della policy ILM. Comprendere i diversi modi in cui gli oggetti possono essere eliminati e il modo in cui StorageGRID gestisce le richieste di eliminazione può aiutarti 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 da parte del client, tutte le copie degli oggetti vengono rimosse immediatamente. Dopo aver rimosso le copie, il cliente viene

informato che l'eliminazione è avvenuta con successo.

- 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 che l'eliminazione è avvenuta correttamente. Le copie degli oggetti vengono rimosse in seguito tramite l'elaborazione ILM in background.

Quando si eliminano oggetti, StorageGRID utilizza il metodo che ottimizza le prestazioni di eliminazione, riduce al minimo i potenziali backlog di eliminazione e libera spazio più rapidamente.

La tabella riepiloga quando StorageGRID utilizza ciascun metodo.

Metodo di esecuzione dell'eliminazione	Quando 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: ◦ È stata raggiunta la data di scadenza o il numero di giorni nella configurazione del ciclo di vita per un bucket S3. ◦ Trascorre l'ultimo periodo di tempo specificato in una regola ILM. Nota: gli oggetti in un bucket in cui è abilitato il blocco degli oggetti S3 non possono essere eliminati se sono sottoposti a conservazione legale o se è stata specificata una data di conservazione fino a quando non è stata ancora rispettata. • Un client S3 richiede l'eliminazione e una o più di queste condizioni sono vere: ◦ Le copie non possono essere eliminate entro 30 secondi perché, ad esempio, la posizione di un oggetto non è temporaneamente disponibile. ◦ Le code di eliminazione in background sono inattive.
Gli oggetti vengono rimossi immediatamente (eliminazione sincrona)	Quando un client S3 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 effettuano richieste di eliminazione, StorageGRID inizia aggiungendo oggetti alla coda di eliminazione. Quindi passa all'esecuzione dell'eliminazione sincrona. Assicurandosi che la coda di eliminazione in background abbia oggetti da elaborare, StorageGRID può elaborare le eliminazioni in modo più efficiente, soprattutto per i client con bassa concorrenza, contribuendo al contempo a prevenire gli arretrati di eliminazione dei client.

Tempo necessario per eliminare gli oggetti

Il modo in cui StorageGRID elimina gli oggetti può influire sulle prestazioni apparenti del sistema:

- Quando StorageGRID esegue l'eliminazione sincrona, potrebbero essere necessari fino a 30 secondi prima che StorageGRID restituisca un risultato al client. Ciò significa che l'eliminazione può sembrare più

lenta, anche se in realtà le copie vengono rimosse più rapidamente rispetto a quando StorageGRID mette in coda gli oggetti per l'eliminazione.

- Se si monitorano attentamente le prestazioni di eliminazione durante un'eliminazione in blocco, si potrebbe 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 dalla messa in coda degli oggetti per l'eliminazione all'esecuzione dell'eliminazione sincrona. L'apparente riduzione del tasso di eliminazione non significa che le copie degli oggetti vengano rimosse più lentamente. Al contrario, indica che, in media, lo spazio viene ora liberato più rapidamente.

Se si eliminano un gran numero di oggetti e la priorità è liberare spazio rapidamente, si può prendere in considerazione l'utilizzo di una richiesta client per eliminare gli oggetti anziché eliminarli tramite 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.

Il tempo necessario 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 essere rimosse 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 client che per altri metodi).

Come vengono eliminati gli oggetti con versione S3

Quando il controllo delle versioni è abilitato per un bucket S3, StorageGRID segue il comportamento di Amazon S3 quando risponde alle richieste di eliminazione, indipendentemente dal fatto che tali richieste provengano da un client S3, dalla scadenza del ciclo di vita di un bucket S3 o dai requisiti della policy ILM.

Quando gli oggetti sono sottoposti a controllo di versione, le richieste di eliminazione degli oggetti non eliminano la versione corrente dell'oggetto e non liberano spazio. Al contrario, una richiesta di eliminazione di un oggetto crea un marcatore di eliminazione di zero byte come versione corrente dell'oggetto, il che rende 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 tale oggetto restituiscono 404 Not Found. Tuttavia, poiché i dati dell'oggetto non corrente non sono stati rimossi, le richieste che specificano una versione non corrente dell'oggetto possono avere esito positivo.

Per liberare spazio durante l'eliminazione di oggetti sottoposti a controllo di versione o per rimuovere i marcatori di eliminazione, utilizzare una delle seguenti opzioni:

- **Richiesta client S3:** specificare l'ID della versione dell'oggetto nella richiesta S3 DELETE Object(DELETE /object?versionId=ID). Tieni presente che questa richiesta rimuove solo le copie degli oggetti per la versione specificata (le altre versioni continuano a occupare spazio).
- **Ciclo di vita del bucket:** utilizzare il `NoncurrentVersionExpiration` azione nella configurazione del ciclo di vita del bucket. Quando viene raggiunto il numero di `NoncurrentDays` specificato, StorageGRID rimuove definitivamente tutte le copie delle versioni non correnti degli oggetti. Queste versioni degli oggetti non possono essere recuperate.

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 ci sono più versioni non correnti di `NewerNoncurrentVersions` specifica che StorageGRID rimuove le versioni precedenti

quando è trascorso il valore `NoncurrentDays`. IL `NewerNoncurrentVersions` la soglia 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 ne richiede l'eliminazione.

Per rimuovere i marcatori di eliminazione degli oggetti scaduti utilizzare `Expiration` azione con uno dei seguenti tag: `ExpiredObjectDeleteMarker`, `Days`, `O Date`.

- **ILM:** ["Clonare una policy attiva"](#) e aggiungere due regole ILM alla nuova policy:
 - Prima regola: utilizzare "Tempo non corrente" come tempo di riferimento per far corrispondere le versioni non correnti dell'oggetto. In ["Passaggio 1 \(Immissione dei dettagli\) della procedura guidata Crea una regola ILM"](#), seleziona **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con controllo delle versioni abilitato)?"
 - Seconda regola: utilizzare **Tempo di acquisizione** in modo che corrisponda alla versione corrente. La regola "Tempo non corrente" deve comparire nella policy sopra la regola **Tempo di inserimento**.

Per rimuovere i marcatori di eliminazione degli oggetti scaduti, utilizzare una regola **Tempo di acquisizione** che corrisponda ai marcatori di eliminazione correnti. I marcatori di eliminazione vengono rimossi solo quando è trascorso un **periodo di tempo di giorni** e l'attuale marcatore di eliminazione è scaduto (non ci sono versioni non correnti).

- **Elimina oggetti nel bucket:** usa il gestore tenant per ["elimina tutte le versioni dell'oggetto"](#), compresi i marcatori di eliminazione, da un bucket.

Quando un oggetto con versione viene eliminato, StorageGRID crea un marcatore di eliminazione a zero byte come versione corrente dell'oggetto. Prima di poter eliminare un bucket con versione, è necessario rimuovere tutti gli oggetti e i marcatori di eliminazione.

- I marcatori di eliminazione creati in StorageGRID 11.7 o versioni precedenti possono essere rimossi solo tramite richieste client S3; non vengono rimossi da ILM, dalle regole del ciclo di vita del bucket o dagli oggetti di eliminazione nelle operazioni del bucket.
- I marcatori di eliminazione da un bucket creato in StorageGRID 11.8 o versione successiva possono essere rimossi tramite ILM, regole del ciclo di vita del bucket, operazioni di eliminazione degli oggetti nelle bucket o un'eliminazione esplicita del client S3.

Informazioni correlate

- ["Utilizzare l'API REST S3"](#)
- ["Esempio 4: regole e policy ILM per oggetti con versione S3"](#)

Creare e assegnare gradi di archiviazione

I gradi di archiviazione identificano il tipo di archiviazione utilizzato da un nodo di archiviazione. È possibile creare gradi di archiviazione se si desidera che le regole ILM posizionino determinati oggetti su determinati nodi di archiviazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Informazioni su questo compito

Quando installi StorageGRID per la prima volta, il livello di archiviazione **Predefinito** viene assegnato automaticamente a ogni nodo di archiviazione nel tuo sistema. Se necessario, è possibile definire gradi di

archiviazione personalizzati e assegnarli a diversi nodi di archiviazione.

Utilizzando gradi di archiviazione personalizzati è possibile creare pool di archiviazione ILM che contengono solo un tipo specifico di nodo di archiviazione. Ad esempio, potresti voler archiviare determinati oggetti sui nodi di archiviazione più veloci, come gli storage appliance all-flash StorageGRID .



Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano solo metadati degli oggetti e non dati degli oggetti. Ai nodi di archiviazione solo metadati non può essere assegnato un grado di archiviazione. Per ulteriori informazioni, consultare "[Tipi di nodi di archiviazione](#)" .

Se il grado di archiviazione non è un problema (ad esempio, tutti i nodi di archiviazione sono identici), è possibile saltare questa procedura e utilizzare la selezione **include tutti i gradi di archiviazione** per il grado di archiviazione quando si "[creare pool di archiviazione](#)" . Utilizzando questa selezione si garantisce che il pool di archiviazione includa tutti i nodi di archiviazione del sito, indipendentemente dal loro grado di archiviazione.



Non creare più livelli di archiviazione del necessario. Ad esempio, non creare un grado di archiviazione per ogni nodo di archiviazione. Assegna invece ogni grado di archiviazione a due o più nodi. I gradi di archiviazione assegnati a un solo nodo possono causare arretrati ILM se il nodo in questione non è più disponibile.

Passi

1. Selezionare **ILM > Gradi di archiviazione**.
2. Definisci gradi di archiviazione personalizzati:
 - a. Per ogni grado di archiviazione personalizzato che desideri aggiungere, seleziona *Inserisci*  per aggiungere una riga.
 - b. Inserisci un'etichetta descrittiva.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

c. Selezionare **Applica modifiche**.

d. Facoltativamente, se devi modificare un'etichetta salvata, seleziona **Modifica*** e seleziona ***Applica modifiche**.



Non è possibile eliminare i gradi di archiviazione.

3. Assegna nuovi gradi di archiviazione ai nodi di archiviazione:

- Individuare il nodo di archiviazione nell'elenco LDR e selezionare la relativa icona ***Modifica*** .
- Selezionare dall'elenco il grado di conservazione appropriato.



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes



Assegnare un grado di archiviazione a un determinato nodo di archiviazione una sola volta. Un nodo di archiviazione ripristinato dopo un errore mantiene il grado di archiviazione assegnato in precedenza. Non modificare questa assegnazione dopo l'attivazione della policy ILM. Se l'assegnazione viene modificata, i dati vengono archiviati in base al nuovo grado di archiviazione.

a. Selezionare **Applica modifiche**.

Utilizzare pool di archiviazione

Che cos'è un pool di archiviazione?

Un pool di archiviazione è un raggruppamento logico di nodi di archiviazione.

Quando si installa StorageGRID, viene creato automaticamente un pool di archiviazione per sito. È possibile configurare pool di archiviazione aggiuntivi in base alle proprie esigenze di archiviazione.



Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano dati e metadati degli oggetti oppure solo metadati degli oggetti. I nodi di archiviazione solo metadati non possono essere utilizzati nei pool di archiviazione. Per ulteriori informazioni, consultare ["Tipi di nodi di archiviazione"](#).

I pool di archiviazione hanno due attributi:

- **Livello di archiviazione:** per i nodi di archiviazione, le prestazioni relative dell'archiviazione di supporto.
- **Sito:** Il centro dati in cui verranno archiviati gli oggetti.

I pool di archiviazione vengono utilizzati nelle regole ILM per determinare dove vengono archiviati i dati degli oggetti e il tipo di archiviazione utilizzato. Quando si configurano le regole ILM per la replica, si selezionano uno o più pool di archiviazione.

Linee guida per la creazione di pool di archiviazione

Configurare e utilizzare pool di archiviazione per proteggersi dalla perdita di dati distribuendo i dati su più siti. Le copie replicate e le copie con codice di cancellazione richiedono configurazioni di pool di archiviazione diverse.

Vedere ["Esempi di abilitazione della protezione contro la perdita del sito mediante la codifica di replicazione e cancellazione"](#) .

Linee guida per tutti i pool di archiviazione

- Mantenere le configurazioni dei pool di archiviazione il più semplici possibile. Non creare più pool di archiviazione del necessario.
- Creare pool di archiviazione con il maggior numero possibile di nodi. Ogni pool di archiviazione dovrebbe contenere due o più nodi. Un pool di archiviazione con nodi insufficienti può causare arretrati ILM se un nodo diventa non disponibile.
- Evitare di creare o utilizzare pool di archiviazione sovrapposti (che contengono uno o più nodi uguali). Se i pool di archiviazione si sovrappongono, è possibile che più copie dei dati degli oggetti vengano salvate sullo stesso nodo.
- In generale, non utilizzare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) o il sito All Sites. Questi elementi vengono aggiornati automaticamente per includere tutti i nuovi siti aggiunti in un'espansione, il che potrebbe non essere il comportamento desiderato.

Linee guida per i pool di archiviazione utilizzati per le copie replicate

- Per la protezione contro la perdita del sito utilizzando ["replicazione"](#) , specificare uno o più pool di archiviazione specifici del sito in ["istruzioni di posizionamento per ogni regola ILM"](#) .

Durante l'installazione StorageGRID viene creato automaticamente un pool di archiviazione per ogni sito.

L'utilizzo di un pool di archiviazione per ogni sito garantisce che le copie degli oggetti replicati vengano posizionate esattamente dove previsto (ad esempio, una copia di ogni oggetto in ogni sito per la protezione contro la perdita del sito).

- Se si aggiunge un sito in un'espansione, creare un nuovo pool di archiviazione che contenga solo il nuovo sito. Poi, ["aggiornare le regole ILM"](#) per controllare quali oggetti vengono archiviati nel nuovo sito.
- Se il numero di copie è inferiore al numero di pool di archiviazione, il sistema distribuisce le copie per bilanciare l'utilizzo del disco tra i pool.
- Se i pool di archiviazione si sovrappongono (contengono gli stessi nodi di archiviazione), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. È necessario assicurarsi che i pool di archiviazione selezionati non contengano gli stessi nodi di archiviazione.

Linee guida per i pool di archiviazione utilizzati per le copie con codice di cancellazione

- Per la protezione contro la perdita del sito utilizzando ["codifica di cancellazione"](#) , creare pool di archiviazione costituiti da almeno tre siti. Se un pool di archiviazione include solo due siti, non è possibile utilizzare tale pool di archiviazione per la codifica di cancellazione. Non sono disponibili schemi di codifica di cancellazione per un pool di archiviazione con due siti.
- Il numero di nodi di archiviazione e siti contenuti nel pool di archiviazione determina quali ["schemi di codifica di cancellazione"](#) sono disponibili.
- Se possibile, un pool di archiviazione dovrebbe includere un numero di nodi di archiviazione superiore a

quello minimo richiesto per lo schema di codifica di cancellazione selezionato. Ad esempio, se si utilizza uno schema di codifica di cancellazione 6+3, è necessario disporre di almeno nove nodi di archiviazione. Tuttavia, si consiglia di avere almeno un nodo di archiviazione aggiuntivo per sito.

- Distribuire i nodi di archiviazione tra i siti nel modo più uniforme possibile. Ad esempio, per supportare uno schema di codifica di cancellazione 6+3, configurare un pool di archiviazione che includa almeno tre nodi di archiviazione in tre siti.
- Se si hanno requisiti di throughput elevati, non è consigliabile utilizzare un pool di archiviazione che includa più siti se la latenza di rete tra i 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 della velocità di trasmissione della rete TCP.

La riduzione della produttività influisce sulle velocità massime raggiungibili di acquisizione e recupero degli oggetti (quando come comportamento di acquisizione è selezionato Bilanciato o Rigoroso) o potrebbe causare arretrati nella coda ILM (quando come comportamento di acquisizione è selezionato Doppio commit). Vedere ["Comportamento di acquisizione delle regole ILM"](#).



Se la griglia include un solo sito, non è possibile utilizzare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) o il sito All Sites in un profilo di codifica di cancellazione. Questo comportamento impedisce che il profilo diventi non valido se viene aggiunto un secondo sito.

Abilita la protezione contro la perdita del sito

Se la distribuzione StorageGRID include più di un sito, è possibile utilizzare la replicazione e la codifica di cancellazione con pool di archiviazione opportunamente configurati per abilitare la protezione contro la perdita del sito.

La replicazione e la codifica di cancellazione richiedono configurazioni di pool di archiviazione diverse:

- Per utilizzare la replica per la protezione contro la perdita del sito, utilizzare i pool di archiviazione specifici del sito creati automaticamente durante l'installazione StorageGRID. Quindi crea regole ILM con ["istruzioni per il posizionamento"](#) che specificano più pool di archiviazione in modo che una copia di ciascun oggetto venga posizionata in ogni sito.
- Per utilizzare la codifica di cancellazione per la protezione dalla perdita del sito, ["creare pool di archiviazione costituiti da più siti"](#). Quindi creare regole ILM che utilizzino un pool di archiviazione composto da più siti e qualsiasi schema di codifica di cancellazione disponibile.



Quando si configura la distribuzione StorageGRID per la protezione dalle perdite del sito, è necessario tenere conto anche degli effetti di ["opzioni di ingestione"](#) e ["coerenza"](#).

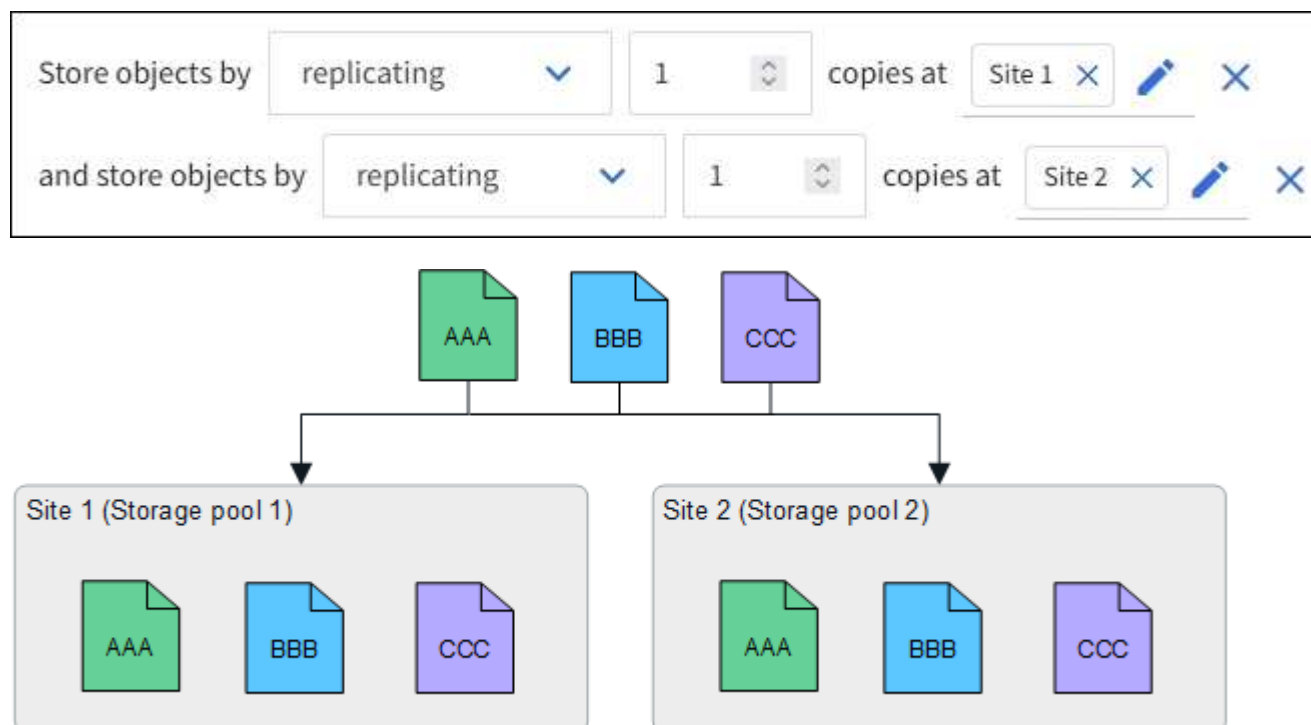
Esempio di replicazione

Per impostazione predefinita, durante l'installazione StorageGRID viene creato un pool di archiviazione per ogni sito. Disporre di pool di archiviazione costituiti da un solo sito consente di configurare regole ILM che utilizzano la replica per la protezione dalle perdite del sito. In questo esempio:

- Il pool di archiviazione 1 contiene il sito 1
- Il pool di archiviazione 2 contiene il sito 2
- La regola ILM contiene due posizionamenti:
 - Memorizza gli oggetti replicandone 1 copia nel Sito 1

- Memorizza gli oggetti replicandone 1 copia nel sito 2

Posizionamenti delle regole ILM:



Se un sito viene perso, copie degli oggetti sono disponibili nell'altro sito.

Esempio di codifica di cancellazione

Disporre di pool di archiviazione composti da più di un sito per pool di archiviazione consente di configurare regole ILM che utilizzano la codifica di cancellazione per la protezione dalla perdita del sito. In questo esempio:

- Il pool di archiviazione 1 contiene i siti da 1 a 3
- La regola ILM contiene un posizionamento: memorizzare gli oggetti tramite codifica di cancellazione utilizzando uno schema EC 4+2 nel pool di archiviazione 1, che contiene tre siti

Posizionamenti delle regole ILM:



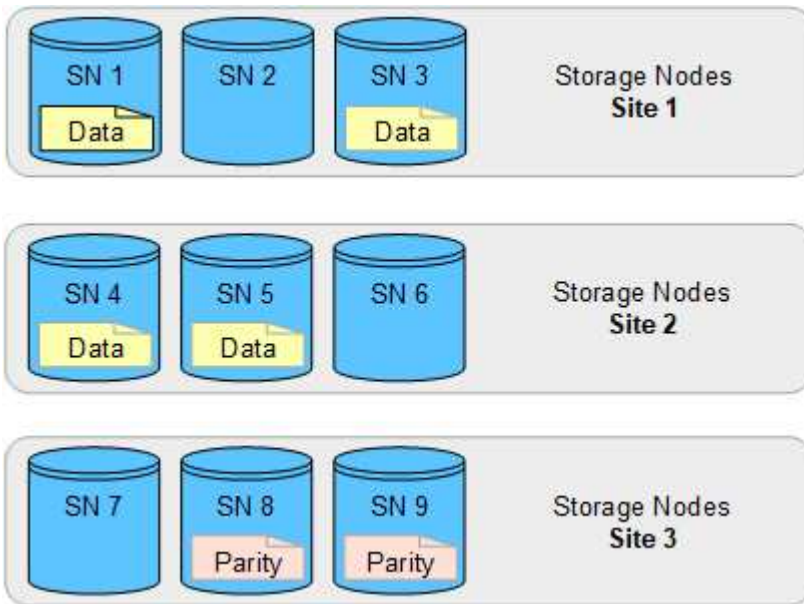
In questo esempio:

- La regola ILM utilizza uno schema di codifica a cancellazione 4+2.
- Ogni oggetto viene suddiviso in quattro frammenti di dati uguali e dai dati dell'oggetto vengono calcolati due frammenti di parità.
- Ciascuno dei sei frammenti viene archiviato su un nodo diverso in tre siti di data center per garantire la protezione dei dati in caso di guasti dei nodi o perdite del sito.

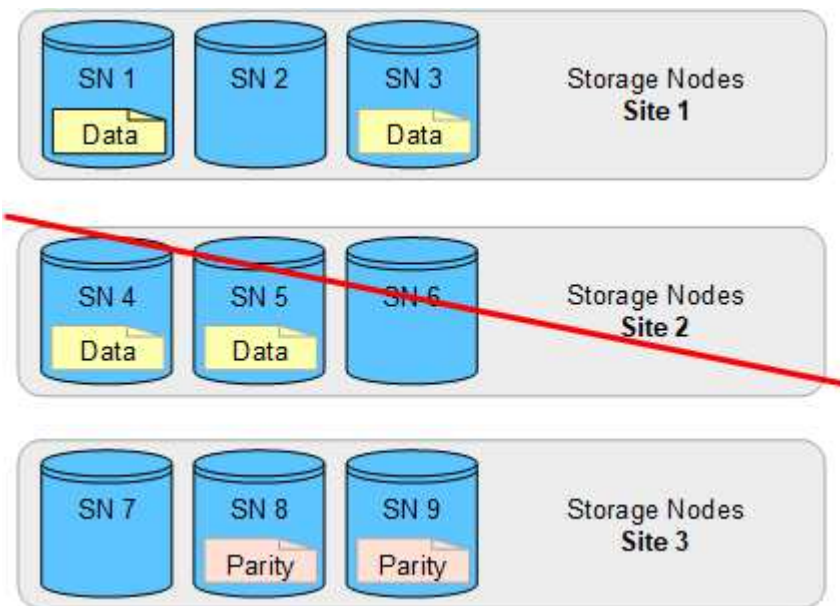


La codifica di cancellazione è consentita nei pool di archiviazione contenenti un numero qualsiasi di siti, *tranne* due siti.

Regola ILM che utilizza lo schema di codifica a cancellazione 4+2:



Se un sito viene perso, i dati possono comunque essere recuperati:



Creare un pool di archiviazione

È possibile creare pool di archiviazione per determinare dove il sistema StorageGRID archivia i dati degli oggetti e il tipo di archiviazione utilizzato. Ogni pool di archiviazione include uno o più siti e uno o più gradi di archiviazione.



Quando si installa StorageGRID 11.9 su una nuova griglia, vengono creati automaticamente pool di archiviazione per ciascun sito. Tuttavia, se inizialmente hai installato StorageGRID 11.6 o una versione precedente, i pool di archiviazione non vengono creati automaticamente per ogni sito.

Se si desidera creare pool di archiviazione cloud per archiviare dati di oggetti al di fuori del sistema

StorageGRID , vedere ["informazioni sull'utilizzo dei pool di archiviazione cloud"](#) .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Hai esaminato le linee guida per la creazione di pool di archiviazione.

Informazioni su questo compito

I pool di archiviazione determinano dove vengono archiviati i dati degli oggetti. Il numero di pool di archiviazione necessari dipende dal numero di siti nella griglia e dal tipo di copie desiderate: replicate o con codice di cancellazione.

- Per la replicazione e la codifica di cancellazione a sito singolo, creare un pool di archiviazione per ciascun sito. Ad esempio, se si desidera archiviare copie di oggetti replicati in tre siti, creare tre pool di archiviazione.
- Per la codifica di cancellazione in tre o più siti, creare un pool di archiviazione che includa una voce per ciascun sito. Ad esempio, se si desidera eliminare oggetti di codice in tre siti, creare un pool di archiviazione.



Non includere il sito Tutti i siti in un pool di archiviazione che verrà utilizzato in un profilo di codifica di cancellazione. Aggiungere invece una voce separata al pool di archiviazione per ogni sito in cui verranno archiviati i dati con codice di cancellazione. Vedere [questo passo](#) per fare un esempio.

- Se si dispone di più di un livello di archiviazione, non creare un pool di archiviazione che includa diversi livelli di archiviazione in un singolo sito. Vedi il ["Linee guida per la creazione di pool di archiviazione"](#) .

Passi

1. Selezionare **ILM > Pool di archiviazione**.

Nella scheda Pool di archiviazione sono elencati tutti i pool di archiviazione definiti.



Per le nuove installazioni di StorageGRID 11.6 o versioni precedenti, il pool di archiviazione All Storage Nodes viene aggiornato automaticamente ogni volta che si aggiungono nuovi siti di data center. Non utilizzare questo pool nelle regole ILM.

2. Per creare un nuovo pool di archiviazione, selezionare **Crea**.
3. Immettere un nome univoco per il pool di archiviazione. Utilizzare un nome che sia facile da identificare quando si configurano i profili di codifica di cancellazione e le regole ILM.
4. Dall'elenco a discesa **Sito**, selezionare un sito per questo pool di archiviazione.

Quando si seleziona un sito, il numero di nodi di archiviazione nella tabella viene aggiornato automaticamente.

In generale, non utilizzare il sito Tutti i siti in nessun pool di archiviazione. Le regole ILM che utilizzano un pool di archiviazione All Sites posizionano gli oggetti in qualsiasi sito disponibile, riducendo il controllo sul posizionamento degli oggetti. Inoltre, un pool di archiviazione All Sites utilizza immediatamente i nodi di archiviazione in un nuovo sito, il che potrebbe non essere il comportamento previsto.

5. Dall'elenco a discesa **Livello di archiviazione**, selezionare il tipo di archiviazione che verrà utilizzato se una regola ILM utilizza questo pool di archiviazione.

Il grado di archiviazione, *include tutti i gradi di archiviazione*, include tutti i nodi di archiviazione nel sito selezionato. Se hai creato gradi di archiviazione aggiuntivi per i nodi di archiviazione nella tua griglia, questi vengono elencati nel menu a discesa.

6. Se si desidera utilizzare il pool di archiviazione in un profilo di codifica di cancellazione multi-sito, selezionare **Aggiungi altri nodi** per aggiungere una voce per ciascun sito al pool di archiviazione.



Se aggiungi più di una voce con diversi gradi di archiviazione per un sito, verrai avvisato.

Per rimuovere una voce, seleziona l'icona Elimina .

7. Quando sei soddisfatto delle tue selezioni, seleziona **Salva**.

Il nuovo pool di archiviazione viene aggiunto all'elenco.

Visualizza i dettagli del pool di archiviazione

È possibile visualizzare i dettagli di un pool di archiviazione per determinare dove viene utilizzato e per vedere quali nodi e livelli di archiviazione sono inclusi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Passi

1. Selezionare **ILM > Pool di archiviazione**.

La tabella Pool di archiviazione include le seguenti informazioni per ogni pool di archiviazione che include nodi di archiviazione:

- **Nome:** nome visualizzato univoco del pool di archiviazione.
- **Conteggio nodi:** numero di nodi nel pool di archiviazione.
- **Utilizzo dello spazio di archiviazione:** la percentuale dello spazio utilizzabile totale che è stata utilizzata per i dati degli oggetti su questo nodo. Questo valore non include i metadati dell'oggetto.
- **Capacità totale:** la dimensione del pool di archiviazione, che equivale alla quantità totale di spazio utilizzabile per i dati degli oggetti per tutti i nodi nel pool di archiviazione.
- **Utilizzo ILM:** modalità di utilizzo attuale del pool di archiviazione. Un pool di archiviazione potrebbe non essere utilizzato oppure potrebbe essere utilizzato in una o più regole ILM, profili di codifica di cancellazione o entrambi.

2. Per visualizzare i dettagli di uno specifico pool di archiviazione, selezionarne il nome.

Viene visualizzata la pagina dei dettagli del pool di archiviazione.

3. Visualizza la scheda **Nodi** per informazioni sui nodi di archiviazione inclusi nel pool di archiviazione.

La tabella include le seguenti informazioni per ciascun nodo:

- Nome del nodo
- Nome del sito

- Grado di conservazione
- Utilizzo dello spazio di archiviazione: percentuale dello spazio totale utilizzabile per i dati degli oggetti che è stato utilizzato per il nodo di archiviazione.



Lo stesso valore di utilizzo dello storage (%) viene visualizzato anche nel grafico Storage Used - Object Data per ciascun Storage Node (selezionare **NODES > Storage Node > Storage**).

4. Visualizzare la scheda **Utilizzo ILM** per determinare se il pool di archiviazione è attualmente utilizzato in regole ILM o profili di codifica di cancellazione.
5. Facoltativamente, vai alla **pagina delle regole ILM** per scoprire e gestire tutte le regole che utilizzano il pool di archiviazione.

Vedi il "[istruzioni per lavorare con le regole ILM](#)".

Modifica pool di archiviazione

È possibile modificare un pool di archiviazione per cambiarne il nome o per aggiornare i siti e i livelli di archiviazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai "[autorizzazioni di accesso specifiche](#)".
- Hai esaminato il "[linee guida per la creazione di pool di archiviazione](#)".
- Se si prevede di modificare un pool di archiviazione utilizzato da una regola nel criterio ILM attivo, è necessario considerare in che modo le modifiche influiranno sul posizionamento dei dati degli oggetti.

Informazioni su questo compito

Se si aggiunge un nuovo sito o un nuovo livello di archiviazione a un pool di archiviazione utilizzato nella policy ILM attiva, tenere presente che i nodi di archiviazione nel nuovo sito o livello di archiviazione non verranno utilizzati automaticamente. Per forzare StorageGRID a utilizzare un nuovo sito o un nuovo livello di archiviazione, è necessario attivare un nuovo criterio ILM dopo aver salvato il pool di archiviazione modificato.

Passi

1. Selezionare **ILM > Pool di archiviazione**.
2. Selezionare la casella di controllo per il pool di archiviazione che si desidera modificare.

Non è possibile modificare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti).

3. Selezionare **Modifica**.
4. Se necessario, modificare il nome del pool di archiviazione.
5. Se necessario, selezionare altri siti e gradi di stoccaggio.

Non è possibile modificare il sito o il grado di archiviazione se il pool di archiviazione viene utilizzato in un profilo di codifica di cancellazione e la modifica renderebbe non valido lo schema di codifica di cancellazione. Ad esempio, se un pool di archiviazione utilizzato in un profilo di codifica di cancellazione include attualmente un grado di archiviazione con un solo sito, non è possibile utilizzare un grado di archiviazione con due siti perché la modifica renderebbe non valido lo schema di codifica di cancellazione.



L'aggiunta o la rimozione di siti da un pool di archiviazione esistente non sposterà alcun dato codificato per la cancellazione esistente. Se si desidera spostare i dati esistenti dal sito, è necessario creare un nuovo pool di archiviazione e un profilo EC per ricodificare i dati.

6. Seleziona **Salva**.

Dopo aver finito

Se hai aggiunto un nuovo sito o un nuovo livello di archiviazione a un pool di archiviazione utilizzato nel criterio ILM attivo, attiva un nuovo criterio ILM per forzare StorageGRID a utilizzare il nuovo sito o livello di archiviazione. Ad esempio, clona la tua policy ILM esistente e poi attiva il clone. Vedere "[Lavorare con le regole e le politiche ILM](#)".

Rimuovere un pool di archiviazione

È possibile rimuovere un pool di archiviazione non utilizzato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"[browser web supportato](#)".
- Tu hai il"[autorizzazioni di accesso richieste](#)".

Passi

1. Selezionare **ILM > Pool di archiviazione**.
2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il pool di archiviazione.

Non è possibile rimuovere un pool di archiviazione se è utilizzato in una regola ILM o in un profilo di codifica di cancellazione. Se necessario, selezionare **nome pool di archiviazione > Utilizzo ILM** per determinare dove viene utilizzato il pool di archiviazione.

3. Se il pool di archiviazione che si desidera rimuovere non è in uso, selezionare la casella di controllo.
4. Seleziona **Rimuovi**.
5. Selezionare **OK**.

Utilizzare i pool di archiviazione cloud

Che cos'è un Cloud Storage Pool?

Un Cloud Storage Pool consente di utilizzare ILM per spostare i dati degli oggetti all'esterno del sistema StorageGRID. Ad esempio, potresti voler spostare gli oggetti a cui si accede raramente su un archivio cloud più economico, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o il livello di accesso Archive nell'archivio BLOB di Microsoft Azure. In alternativa, potresti voler mantenere un backup cloud degli oggetti StorageGRID per migliorare il ripristino in caso di emergenza.

Dal punto di vista ILM, un Cloud Storage Pool è simile a un pool di archiviazione. Per archiviare gli oggetti in una delle due posizioni, selezionare il pool durante la creazione delle istruzioni di posizionamento per una regola ILM. Tuttavia, mentre i pool di archiviazione sono costituiti da nodi di archiviazione all'interno del sistema StorageGRID, un pool di archiviazione cloud è costituito da un bucket esterno (S3) o da un contenitore (archiviazione BLOB di Azure).

La tabella confronta i pool di archiviazione con i pool di archiviazione cloud e mostra le principali somiglianze e differenze.

	Pool di stoccaggio	Pool di archiviazione cloud
Come viene creato?	Utilizzando l'opzione ILM > Pool di archiviazione in Grid Manager.	Utilizzando l'opzione ILM > Pool di archiviazione > Pool di archiviazione cloud in Grid Manager. È necessario configurare il bucket o il contenitore esterno prima di poter creare il Cloud Storage Pool.
Quante piscine puoi creare?	Illimitato.	Fino a 10.
Dove vengono conservati gli oggetti?	Su uno o più nodi di archiviazione all'interno StorageGRID.	In un bucket Amazon S3, in un contenitore di archiviazione BLOB di Azure o in un Google Cloud esterno al sistema StorageGRID . Se il Cloud Storage Pool è un bucket Amazon S3: • Facoltativamente, è possibile configurare un ciclo di vita del bucket per trasferire gli oggetti in un archivio a basso costo e a lungo termine, come Amazon S3 Glacier o S3 Glacier Deep Archive. Il sistema di archiviazione esterno deve supportare la classe di archiviazione Glacier e l'API S3 RestoreObject. • È possibile creare pool di archiviazione cloud da utilizzare con AWS Commercial Cloud Services (C2S), che supporta la regione segreta AWS. Se il Cloud Storage Pool è un contenitore di archiviazione BLOB di Azure, StorageGRID trasferisce l'oggetto al livello Archivio. Nota: in generale, non configurare la gestione del ciclo di vita dell'archiviazione BLOB di Azure per il contenitore utilizzato per un pool di archiviazione cloud. Le operazioni di RestoreObject sugli oggetti nel Cloud Storage Pool possono essere influenzate dal ciclo di vita configurato.
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nelle policy ILM attive.	Una regola ILM nelle policy ILM attive.
Quale metodo di protezione dei dati viene utilizzato?	Codifica di replicazione o cancellazione.	Replicazione.

	Pool di stoccaggio	Pool di archiviazione cloud
Quante copie di ciascun oggetto sono consentite?	Multiplo.	Una copia nel Cloud Storage Pool e, facoltativamente, una o più copie in StorageGRID. Nota: non è possibile archiviare un oggetto in più di un Cloud Storage Pool contemporaneamente.
Quali sono i vantaggi?	Gli oggetti sono rapidamente accessibili in qualsiasi momento.	Archiviazione a basso costo. Nota: i dati FabricPool non possono essere suddivisi in livelli nei Cloud Storage Pool.

Ciclo di vita di un oggetto Cloud Storage Pool

Prima di implementare i Cloud Storage Pool, esaminare il ciclo di vita degli oggetti archiviati in ciascun tipo di Cloud Storage Pool.

S3: Ciclo di vita di un oggetto Cloud Storage Pool

I passaggi descrivono le fasi del ciclo di vita di un oggetto archiviato in un pool di archiviazione cloud S3.



"Glacier" si riferisce sia alla classe di archiviazione Glacier sia alla classe di archiviazione Glacier Deep Archive, con un'eccezione: la classe di archiviazione Glacier Deep Archive non supporta il livello di ripristino accelerato. È supportato solo il recupero in blocco o standard.



Google Cloud Platform (GCP) supporta il recupero di oggetti da archivi a lungo termine senza richiedere un'operazione di ripristino POST.

1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato nel pool di archiviazione cloud S3

- Quando l'oggetto corrisponde a una regola ILM che utilizza un pool di archiviazione cloud S3 come posizione di posizionamento, StorageGRID sposta l'oggetto nel bucket S3 esterno specificato dal pool di archiviazione cloud.
- Quando l'oggetto è stato spostato nel pool di archiviazione cloud S3, l'applicazione client può recuperarlo utilizzando una richiesta S3 GetObject da StorageGRID, a meno che l'oggetto non sia stato trasferito nello storage Glacier.

3. Oggetto trasferito a Glacier (stato non recuperabile)

- Facoltativamente, l'oggetto può essere trasferito nello 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.



Se si desidera effettuare la transizione degli oggetti, è necessario creare una configurazione del ciclo di vita per il bucket S3 esterno e utilizzare una soluzione di archiviazione che implementi la classe di archiviazione Glacier e supporti l'API S3 RestoreObject.

- Durante la transizione, l'applicazione client può utilizzare una richiesta S3 HeadObject per monitorare lo stato dell'oggetto.

4. Oggetto ripristinato dal deposito Glacier

Se un oggetto è stato trasferito nello storage Glacier, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nello storage pool S3 Cloud. La richiesta specifica per quanti giorni la copia deve essere disponibile nel Cloud Storage Pool e il livello di accesso ai dati da utilizzare per l'operazione di ripristino (Expedited, Standard o Bulk). Quando viene raggiunta la data di scadenza della copia recuperabile, la copia torna automaticamente allo stato non recuperabile.



Se una o più copie dell'oggetto sono presenti anche sui nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier inviando una richiesta RestoreObject. In alternativa, è possibile recuperare direttamente la copia locale, utilizzando una richiesta GetObject.

5. Oggetto recuperato

Una volta ripristinato un oggetto, l'applicazione client può inviare una richiesta GetObject per recuperare l'oggetto ripristinato.

Azure: ciclo di vita di un oggetto Cloud Storage Pool

I passaggi descrivono le fasi del ciclo di vita di un oggetto archiviato in un pool di Azure Cloud Storage.

1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato nel pool di archiviazione cloud di Azure

Quando l'oggetto corrisponde a una regola ILM che utilizza un pool di archiviazione cloud di Azure come posizione di posizionamento, StorageGRID sposta l'oggetto nel contenitore di archiviazione BLOB di Azure esterno specificato dal pool di archiviazione cloud.

3. Oggetto trasferito al livello Archivio (stato non recuperabile)

Subito dopo aver spostato l'oggetto nel pool di archiviazione cloud di Azure, StorageGRID trasferisce automaticamente l'oggetto al livello di archivio di archiviazione BLOB di Azure.

4. Oggetto ripristinato dal livello Archivio

Se un oggetto è stato trasferito al livello Archivio, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel pool di archiviazione cloud di Azure.

Quando StorageGRID riceve RestoreObject, trasferisce temporaneamente l'oggetto al livello Cool di archiviazione BLOB di Azure. Non appena viene raggiunta la data di scadenza nella richiesta RestoreObject, StorageGRID riporta l'oggetto al livello Archivio.



Se una o più copie dell'oggetto sono presenti anche sui nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso all'archivio inviando una richiesta RestoreObject. In alternativa, è possibile recuperare direttamente la copia locale, utilizzando una richiesta GetObject.

5. Oggetto recuperato

Una volta ripristinato un oggetto nel pool di archiviazione cloud di Azure, l'applicazione client può inviare una richiesta GetObject per recuperare l'oggetto ripristinato.

Informazioni correlate

["Utilizzare l'API REST S3"](#)

Quando utilizzare i pool di archiviazione cloud

Utilizzando i Cloud Storage Pool, è possibile eseguire il backup o suddividere i dati in livelli in una posizione esterna. Inoltre, è possibile eseguire il backup o suddividere i dati in più cloud.

Eseguire il backup dei dati StorageGRID in una posizione esterna

È possibile utilizzare un Cloud Storage Pool per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, i dati degli oggetti nel Cloud Storage Pool possono essere utilizzati per soddisfare le richieste dei client. Tuttavia, potrebbe essere necessario inviare una richiesta S3 RestoreObject per accedere alla copia dell'oggetto di backup nel Cloud Storage Pool.

I dati degli oggetti in un Cloud Storage Pool possono essere utilizzati anche per recuperare i dati persi da StorageGRID a causa di un errore del volume di archiviazione o del nodo di archiviazione. Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di archiviazione recuperato.

Per implementare una soluzione di backup:

1. Crea un singolo Cloud Storage Pool.
2. Configurare una regola ILM che memorizzi simultaneamente copie di oggetti su nodi di archiviazione (come copie replicate o con codice di cancellazione) e una singola copia di oggetti nel pool di archiviazione cloud.
3. Aggiungi la regola alla tua policy ILM. Quindi, simulare e attivare la policy.

Dati di livello da StorageGRID alla posizione esterna

È possibile utilizzare un Cloud Storage Pool per archiviare oggetti al di fuori del sistema StorageGRID. Supponiamo, ad esempio, di avere un gran numero di oggetti che devi conservare, ma che prevedi di accedervi raramente, se non mai. È possibile utilizzare un Cloud Storage Pool per suddividere gli oggetti in livelli di archiviazione più economici e liberare spazio in StorageGRID.

Per implementare una soluzione a livelli:

1. Crea un singolo Cloud Storage Pool.

2. Configura una regola ILM che sposta gli oggetti raramente utilizzati dai nodi di archiviazione al pool di archiviazione cloud.
3. Aggiungi la regola alla tua policy ILM. Quindi, simulare e attivare la policy.

Gestisci più endpoint cloud

È possibile configurare più endpoint del Cloud Storage Pool se si desidera suddividere in livelli o eseguire il backup dei dati degli oggetti su più cloud. I filtri nelle regole ILM consentono di specificare quali oggetti vengono archiviati in ciascun Cloud Storage Pool. Ad esempio, potresti voler archiviare oggetti da alcuni tenant o bucket in Amazon S3 Glacier e oggetti da altri tenant o bucket nell'archiviazione BLOB di Azure. Oppure potresti voler spostare i dati tra Amazon S3 Glacier e Azure Blob Storage.



Quando si utilizzano più endpoint Cloud Storage Pool, tenere presente che un oggetto può essere archiviato in un solo Cloud Storage Pool alla volta.

Per implementare più endpoint cloud:

1. Crea fino a 10 pool di archiviazione cloud.
2. Configurare le regole ILM per archiviare i dati degli oggetti appropriati al momento opportuno in ogni Cloud Storage Pool. Ad esempio, archivia gli oggetti dal bucket A nel Cloud Storage Pool A e archivia gli oggetti dal bucket B nel Cloud Storage Pool B. Oppure, archivia gli oggetti nel Cloud Storage Pool A per un certo periodo di tempo e poi spostali nel Cloud Storage Pool B.
3. Aggiungi le regole alla tua policy ILM. Quindi, simulare e attivare la policy.

Considerazioni sui pool di archiviazione cloud

Se si prevede di utilizzare un Cloud Storage Pool per spostare oggetti fuori dal sistema StorageGRID, è necessario esaminare le considerazioni per la configurazione e l'utilizzo dei Cloud Storage Pool.

Considerazioni generali

- In generale, l'archiviazione cloud, come Amazon S3 Glacier o Azure Blob Storage, è un modo economico per archiviare dati di oggetti. Tuttavia, i costi per recuperare i dati dall'archiviazione cloud sono relativamente elevati. Per ottenere il costo complessivo più basso, è necessario considerare quando e con quale frequenza si accederà agli oggetti nel Cloud Storage Pool. Si consiglia di utilizzare un pool di archiviazione cloud solo per i contenuti a cui si prevede di accedere raramente.
- L'utilizzo di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva necessaria per recuperare un oggetto dalla destinazione di Cloud Storage Pool.
- Gli oggetti con S3 Object Lock abilitato non possono essere inseriti nei Cloud Storage Pool.
- Se il bucket S3 di destinazione per un Cloud Storage Pool ha abilitato il blocco degli oggetti S3, il tentativo di configurare la replica del bucket (PutBucketReplication) fallirà con un errore AccessDenied.
- Le seguenti combinazioni di piattaforma, autenticazione e protocollo con blocco oggetto S3 non sono supportate per i pool di archiviazione cloud:
 - **Piattaforme:** Google Cloud Platform e Azure
 - **Tipi di autenticazione:** ruoli IAM ovunque e accesso anonimo
 - **Protocollo:** HTTP

Considerazioni sulle porte utilizzate per i pool di archiviazione cloud

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 archiviazione del sistema. È necessario assicurarsi che le seguenti porte possano comunicare con il Cloud Storage Pool.

Per impostazione predefinita, i pool di archiviazione cloud utilizzano le seguenti porte:

- **80**: Per gli URI degli endpoint che iniziano con http
- **443**: Per gli URI degli 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 di messaggi a endpoint esterni, ad esempio un endpoint su Internet.

Considerazioni sui costi

Per accedere allo storage nel cloud tramite un Cloud Storage Pool è necessaria la connettività di rete al cloud. È necessario considerare il costo dell'infrastruttura di rete che verrà utilizzata per accedere al cloud e predisporla in modo appropriato, in base alla quantità di dati che si prevede di spostare tra StorageGRID e il cloud utilizzando il Cloud Storage Pool.

Quando StorageGRID si connette all'endpoint esterno del Cloud Storage Pool, invia varie richieste per monitorare la connettività e garantire che possa eseguire le operazioni richieste. Sebbene a queste richieste siano associati alcuni costi aggiuntivi, il costo del monitoraggio di un Cloud Storage Pool dovrebbe rappresentare solo una piccola frazione del costo complessivo dell'archiviazione degli oggetti in S3 o Azure.

Potrebbero essere sostenuti costi più significativi se è necessario spostare oggetti da un endpoint Cloud Storage Pool esterno a StorageGRID. Gli oggetti potrebbero essere spostati nuovamente su StorageGRID in uno dei seguenti casi:

- L'unica copia dell'oggetto si trova in un Cloud Storage Pool e si decide di archiviare l'oggetto in StorageGRID. In questo caso, è necessario riconfigurare le regole e i criteri ILM. Quando si verifica la valutazione ILM, StorageGRID invia più richieste per recuperare l'oggetto dal Cloud Storage Pool. StorageGRID crea quindi localmente il numero specificato di copie replicate o con codice di cancellazione. Dopo che l'oggetto viene spostato nuovamente su StorageGRID, la copia nel Cloud Storage Pool viene eliminata.
- Gli oggetti vengono persi a causa di un errore del nodo di archiviazione. Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di archiviazione recuperato.



Quando gli oggetti vengono spostati nuovamente su StorageGRID da un Cloud Storage Pool, StorageGRID invia più richieste all'endpoint del Cloud Storage Pool per ciascun oggetto. Prima di spostare un gran numero di oggetti, contattare l'assistenza tecnica per ottenere assistenza nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket Cloud Storage Pool

I criteri per il bucket S3 esterno utilizzato per un Cloud Storage Pool devono concedere a StorageGRID l'autorizzazione per spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto dallo storage Glacier quando necessario e altro ancora. Idealmente, StorageGRID dovrebbe avere accesso completo al bucket(`s3 : *`); tuttavia, se ciò non è possibile, la policy del 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 Cloud Storage Pool è controllato dalle regole ILM e dai criteri ILM attivi 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 archiviazione che implementa la classe di archiviazione Glacier) è controllata dalla configurazione del ciclo di vita di quel bucket.

Se si desidera trasferire oggetti dal Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata sul bucket S3 esterno e utilizzare una soluzione di archiviazione che implementi la classe di archiviazione Glacier e supporti l'API S3 RestoreObject.

Ad esempio, supponiamo di voler trasferire immediatamente tutti gli oggetti spostati da StorageGRID al Cloud Storage Pool allo storage Amazon S3 Glacier. Dovresti 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 trasferirà tutti gli oggetti bucket ad Amazon S3 Glacier il giorno in cui sono stati creati (ovvero il giorno in cui sono stati spostati da StorageGRID al Cloud Storage Pool).



Quando si configura il ciclo di vita del bucket esterno, non utilizzare mai azioni **Scadenza** per definire quando scadono gli oggetti. Le azioni di scadenza determinano l'eliminazione degli oggetti scaduti da parte del sistema di archiviazione esterno. Se in seguito si tenta di accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non verrà trovato.

Se si desidera trasferire gli oggetti nel Cloud Storage Pool a S3 Glacier Deep Archive (anziché ad Amazon S3 Glacier), specificare `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tuttavia, tieni presente che non puoi utilizzare il Expedited livello per ripristinare gli oggetti dall'archivio profondo del ghiacciaio S3.

Azure: considerazioni sul livello di accesso

Quando si configura un account di archiviazione di Azure, è possibile impostare il livello di accesso predefinito su Accesso frequente o Accesso sporadico. Quando si crea un account di archiviazione da utilizzare con un Cloud Storage Pool, è consigliabile utilizzare il livello Hot come livello predefinito. Anche se StorageGRID imposta immediatamente il livello su Archivio quando sposta gli oggetti nel Cloud Storage Pool, l'utilizzo di un'impostazione predefinita su Caldo garantisce che non verrà addebitata alcuna commissione per l'eliminazione anticipata degli oggetti rimossi dal livello Freddo prima del minimo di 30 giorni.

Azure: gestione del ciclo di vita non supportata

Non utilizzare la gestione del ciclo di vita dell'archiviazione BLOB di Azure per il contenitore utilizzato con un pool di archiviazione cloud. Le operazioni del ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

["Creare un pool di archiviazione cloud"](#)

Confronta i pool di archiviazione cloud e la replica di CloudMirror

Quando si inizia a utilizzare Cloud Storage Pools, potrebbe essere utile comprendere le somiglianze e le differenze tra Cloud Storage Pools e il servizio di replica StorageGRID CloudMirror.

	Pool di archiviazione cloud	Servizio di replica CloudMirror
Qual è lo scopo principale?	Funziona come destinazione di archivio. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure una copia aggiuntiva. Ciò significa che, invece di conservare due copie in loco, è possibile conservarne una copia in StorageGRID e inviarne una copia al Cloud Storage Pool.	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 è impostato?	Definiti allo stesso modo dei pool di archiviazione, utilizzando Grid Manager o Grid Management API. Può essere selezionato come posizione di posizionamento in una regola ILM. Mentre un pool di archiviazione è costituito da un gruppo di nodi di archiviazione, un pool di archiviazione cloud viene definito utilizzando un endpoint S3 o Azure remoto (indirizzo IP, credenziali e così via).	Un utente tenant configura la replica di CloudMirror definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) tramite Tenant Manager o l'API S3. Dopo aver configurato l'endpoint CloudMirror, qualsiasi bucket di proprietà di quell'account tenant può essere configurato in modo che punti all'endpoint CloudMirror.

	Pool di archiviazione cloud	Servizio di replica CloudMirror
Chi è responsabile della sua istituzione?	In genere, un amministratore di rete	In genere, un utente tenant
Qual è la destinazione?	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Livello di archivio BLOB di Azure • Piattaforma Google Cloud (GCP)	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Piattaforma Google Cloud (GCP)
Cosa determina lo spostamento degli oggetti verso la destinazione?	Una o più regole ILM nelle policy ILM attive. Le regole ILM definiscono quali oggetti StorageGRID sposta nel Cloud Storage Pool e quando gli oggetti vengono spostati.	L'atto di ingerire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror. Gli oggetti presenti nel bucket di origine prima che il bucket fosse configurato con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come vengono recuperati gli oggetti?	Le applicazioni devono inviare richieste a StorageGRID per recuperare gli oggetti che sono stati spostati in un Cloud Storage Pool. Se l'unica copia di un oggetto è stata trasferita in un archivio, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia speculare nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto inviando richieste a StorageGRID o alla destinazione S3. Supponiamo, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti su un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è obbligatorio utilizzare StorageGRID.
Riesci a leggere direttamente dalla destinazione?	No. Gli oggetti spostati in un Cloud Storage Pool vengono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero da Cloud Storage Pool).	Sì, perché la copia speculare è una copia indipendente.
Cosa succede se un oggetto viene eliminato dalla sorgente?	L'oggetto viene eliminato anche dal Cloud Storage Pool.	L'azione di eliminazione non viene replicata. Un oggetto eliminato non esiste più nel bucket StorageGRID, ma continua a esistere nel bucket di destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere eliminati senza influire sulla sorgente.

	Pool di archiviazione cloud	Servizio di replica CloudMirror
Come si accede agli oggetti dopo un disastro (sistema StorageGRID non operativo)?	I nodi StorageGRID non riusciti devono essere ripristinati. Durante questo processo, le copie degli oggetti replicati potrebbero essere ripristinate utilizzando le copie presenti nel Cloud Storage Pool.	Le copie degli oggetti nella destinazione CloudMirror sono indipendenti da StorageGRID, quindi è possibile accedervi direttamente prima che i nodi StorageGRID vengano ripristinati.

Creare un pool di archiviazione cloud

Un Cloud Storage Pool specifica un singolo bucket Amazon S3 esterno o un altro provider compatibile con S3 oppure un contenitore di archiviazione BLOB di Azure.

Quando si crea un Cloud Storage Pool, si specifica il nome e la posizione del bucket o del contenitore esterno che StorageGRID utilizzerà per archiviare gli oggetti, il tipo di provider cloud (Amazon S3/GCP o Azure Blob Storage) e le informazioni necessarie a StorageGRID per accedere al bucket o al contenitore esterno.

StorageGRID convalida il Cloud Storage Pool non appena lo salvi, quindi devi assicurarti che il bucket o il contenitore specificato nel Cloud Storage Pool esista e sia raggiungibile.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["autorizzazioni di accesso richieste"](#) .
- Hai esaminato il ["considerazioni per i pool di archiviazione cloud"](#) .
- Il bucket o contenitore esterno a cui fa riferimento il Cloud Storage Pool esiste già e si dispone di [informazioni sull'endpoint del servizio](#) .
- Per accedere al secchio o al contenitore, hai il [informazioni sull'account per il tipo di autenticazione](#) sceglierai tu.

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.
2. Seleziona **Crea**, quindi inserisci le seguenti informazioni:

Campo	Descrizione
Nome del pool di archiviazione cloud	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.
Tipo di fornitore	Quale provider cloud utilizzerai per questo Cloud Storage Pool: • Amazon S3/GCP: seleziona questa opzione per un provider Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) o un altro provider compatibile con S3. • Archiviazione BLOB di Azure

Campo	Descrizione
Secchio o contenitore	Nome del bucket S3 esterno o del contenitore di Azure. Non è possibile modificare questo valore dopo aver salvato il Cloud Storage Pool.

3. In base alla selezione del tipo di provider, immettere 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. Inserisci il nome host. Esempio:

`s3-aws-region.amazonaws.com`

- c. Seleziona lo stile URL:

Opzione	Descrizione
Rilevamento automatico	Tenta di rilevare automaticamente quale stile URL utilizzare, in base alle informazioni fornite. Ad esempio, se si specifica un indirizzo IP, StorageGRID utilizzerà un URL in stile percorso. Seleziona questa opzione solo se non sai quale stile specifico utilizzare.
Stile ospitato virtuale	Utilizzare un URL in stile virtual-hosted per accedere al bucket. Gli URL in stile virtual-hosted includono il nome del bucket come parte del nome di dominio. Esempio: <code>https://bucket-name.s3.company.com/key-name</code>
Stile percorso	Utilizzare un URL in stile percorso per accedere al bucket. Gli URL in stile percorso includono il nome del bucket alla fine. Esempio: <code>https://s3.company.com/bucket-name/key-name</code> Nota: l'opzione URL in stile percorso non è consigliata e verrà deprecata in una futura versione di StorageGRID.

- d. Facoltativamente, immettere il numero di porta oppure utilizzare la porta predefinita: 443 per HTTPS o 80 per HTTP.

Archiviazione BLOB di Azure

- 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. Seleziona **Continua**. Quindi seleziona il tipo di autenticazione e inserisci le informazioni richieste per l'endpoint del Cloud Storage Pool:

Chiave di accesso

Per Amazon S3/GCP o altri provider compatibili con S3

- a. **ID chiave di accesso:** immettere l'ID chiave di accesso per l'account proprietario del bucket esterno.
- b. **Chiave di accesso segreta:** Inserisci la chiave di accesso segreta.

Ruoli IAM ovunque

Per il servizio AWS IAM Roles Anywhere

StorageGRID utilizza AWS Security Token Service (STS) per generare dinamicamente un token di breve durata per accedere alle risorse AWS.

- a. **Regione AWS IAM Roles Anywhere:** seleziona la regione per il Cloud Storage Pool. Ad esempio, `us-east-1`.
- b. **URN dell'ancora di trust:** immettere l'URN dell'ancora di trust che convalida le richieste di credenziali STS di breve durata. Può essere una CA radice o intermedia.
- c. **URN del profilo:** immettere l'URN del profilo IAM Roles Anywhere che elenca i ruoli che possono essere assunti da chiunque sia considerato attendibile.
- d. **URN del ruolo:** immettere l'URN del ruolo IAM che può essere assunto da chiunque sia considerato attendibile.
- e. **Durata sessione:** immettere la durata delle credenziali di sicurezza temporanee e della sessione del ruolo. Inserisci almeno 15 minuti e non più di 12 ore.
- f. **Certificato CA del server** (facoltativo): uno o più certificati CA attendibili, in formato PEM, per la verifica del server IAM Roles Anywhere. Se omissso, il server non verrà verificato.
- g. **Certificato dell'entità finale:** la chiave pubblica, in formato PEM, del certificato X509 firmato dal trust anchor. AWS IAM Roles Anywhere utilizza questa chiave per emettere un token STS.
- h. **Chiave privata dell'entità finale:** la chiave privata per il certificato dell'entità finale.

CAP (portale di accesso C2S)

Per il servizio S3 dei servizi cloud commerciali (C2S)

- a. **URL delle credenziali temporanee:** immettere l'URL completo che StorageGRID utilizzerà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati al proprio account C2S.
- b. **Certificato CA del server:** seleziona **Sfogliala** e carica il certificato CA che StorageGRID utilizzerà per verificare il server CAP. Il certificato deve essere codificato PEM ed emesso da un'autorità di certificazione governativa (CA) appropriata.
- c. **Certificato client:** seleziona **Sfogliala** e carica il certificato che StorageGRID utilizzerà per identificarsi sul server CAP. Il certificato client deve essere codificato PEM, rilasciato da un'autorità di certificazione governativa (CA) appropriata e deve consentire l'accesso al tuo account C2S.
- d. **Chiave privata client:** selezionare **Sfogliala** e caricare la chiave privata codificata PEM per il certificato client.
- e. Se la chiave privata del client è crittografata, immettere la passphrase per decrittografare la chiave privata del client. In caso contrario, lasciare vuoto il campo **Passphrase della chiave privata del client**.



Se il certificato client verrà crittografato, utilizzare il formato tradizionale per la crittografia. Il formato crittografato PKCS #8 non è supportato.

Archiviazione BLOB di Azure

Per Azure Blob Storage, solo chiave condivisa

- Nome account:** immettere il nome dell'account di archiviazione proprietario del contenitore esterno
- Chiave account:** inserisci la chiave segreta per l'account di archiviazione

È possibile utilizzare il portale di Azure per trovare questi valori.

Anonimo

Non sono richieste ulteriori informazioni.

5. Selezionare **Continua**. Quindi scegli il tipo di verifica del server che desideri utilizzare:

Opzione	Descrizione
Utilizzare i certificati CA radice nel sistema operativo Storage Node	Utilizzare i certificati Grid CA installati sul sistema operativo per proteggere le connessioni.
Utilizza un certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Selezionare Sfoglia e caricare il certificato codificato PEM.
Non verificare il certificato	Selezionando questa opzione le connessioni TLS al Cloud Storage Pool non saranno sicure.

6. Seleziona **Salva**.

Quando si salva un Cloud Storage Pool, StorageGRID esegue le seguenti operazioni:

- Verifica che il bucket o il contenitore e l'endpoint del servizio esistano e che possano essere raggiunti utilizzando le credenziali specificate.
- Scrive un file marcatore nel bucket o nel contenitore per identificarlo come Cloud Storage Pool. Non rimuovere mai questo file, che si chiama `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega il motivo per cui la convalida non è riuscita. Ad esempio, potrebbe essere segnalato un errore se si verifica un errore del certificato o se il bucket o il contenitore specificato non esiste già.

7. Se si verifica un errore, vedere il ["Istruzioni per la risoluzione dei problemi dei pool di archiviazione cloud"](#), risolvere eventuali problemi e quindi provare a salvare nuovamente il Cloud Storage Pool.

Visualizza i dettagli del Cloud Storage Pool

È possibile visualizzare i dettagli di un Cloud Storage Pool per determinare dove viene utilizzato e vedere quali nodi e livelli di archiviazione sono inclusi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.

La tabella Cloud Storage Pools include le seguenti informazioni per ogni Cloud Storage Pool che include nodi di archiviazione:

- **Nome:** il nome visualizzato univoco del pool.
- **URI:** Uniform Resource Identifier del Cloud Storage Pool.
- **Tipo di provider:** quale provider cloud viene utilizzato per questo Cloud Storage Pool.
- **Contenitore:** il nome del bucket utilizzato per il Cloud Storage Pool.
- **Utilizzo ILM:** modalità di utilizzo attuale del pool. Un Cloud Storage Pool potrebbe non essere utilizzato oppure potrebbe essere utilizzato in una o più regole ILM, profili di codifica di cancellazione o entrambi.
- **Ultimo errore:** l'ultimo errore rilevato durante un controllo dello stato di questo Cloud Storage Pool.

2. Per visualizzare i dettagli di uno specifico Cloud Storage Pool, selezionarne il nome.

Viene visualizzata la pagina dei dettagli del pool.

3. Visualizza la scheda **Autenticazione** per informazioni sul tipo di autenticazione per questo Cloud Storage Pool e per modificare i dettagli di autenticazione.
4. Visualizza la scheda **Verifica del server** per conoscere i dettagli della verifica, modificare la verifica, scaricare un nuovo certificato o copiare il certificato PEM.
5. Visualizzare la scheda **Utilizzo ILM** per determinare se il Cloud Storage Pool è attualmente utilizzato in regole ILM o profili di codifica di cancellazione.
6. Facoltativamente, vai alla **pagina delle regole ILM** per ["conoscere e gestire tutte le regole"](#) che utilizzano il Cloud Storage Pool.

Modifica un pool di archiviazione cloud

È possibile modificare un Cloud Storage Pool per cambiarne il nome, l'endpoint del servizio o altri dettagli; tuttavia, non è possibile modificare il bucket S3 o il contenitore di Azure per un Cloud Storage Pool.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Hai esaminato il ["considerazioni per i pool di archiviazione cloud"](#) .

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.

Nella tabella Cloud Storage Pools sono elencati i Cloud Storage Pool esistenti.

2. Seleziona la casella di controllo per il Cloud Storage Pool che desideri modificare, quindi seleziona **Azioni > Modifica**.

In alternativa, seleziona il nome del Cloud Storage Pool, quindi seleziona **Modifica**.

3. Se necessario, modificare il nome del Cloud Storage Pool, l'endpoint del servizio, le credenziali di autenticazione o il metodo di verifica del certificato.



Non è possibile modificare il tipo di provider, il bucket S3 o il contenitore di Azure per un pool di archiviazione cloud.

Se in precedenza hai caricato un certificato server o client, puoi espandere la voce **Dettagli certificato** per esaminare il certificato attualmente in uso.

4. Seleziona **Salva**.

Quando si salva un Cloud Storage Pool, StorageGRID verifica che il bucket o il contenitore e l'endpoint del servizio esistano e che possano essere raggiunti utilizzando le credenziali specificate.

Se la convalida del Cloud Storage Pool fallisce, viene visualizzato un messaggio di errore. Ad esempio, potrebbe essere segnalato un errore se si verifica un errore nel certificato.

Vedi le istruzioni per "[risoluzione dei problemi dei pool di archiviazione cloud](#)", risolvere il problema e quindi provare a salvare nuovamente il Cloud Storage Pool.

Rimuovere un pool di archiviazione cloud

È possibile rimuovere un Cloud Storage Pool se non è utilizzato in una regola ILM e non contiene dati di oggetti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu 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 di oggetti, è necessario utilizzare ILM per spostare i dati in una posizione diversa. Ad esempio, puoi spostare i dati sui nodi di archiviazione nella tua griglia o su un pool di archiviazione cloud diverso.

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.
2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il Cloud Storage Pool.

Non è possibile rimuovere un Cloud Storage Pool se è utilizzato in una regola ILM o in un profilo di codifica di cancellazione.

3. Se si utilizza il Cloud Storage Pool, selezionare **nome del cloud storage pool > Utilizzo ILM**.
4. "[Clona ogni regola ILM](#)" che attualmente posiziona gli oggetti nel Cloud Storage Pool che desideri rimuovere.
5. Determina dove vuoi spostare gli oggetti esistenti gestiti da ciascuna regola clonata.

È possibile utilizzare uno o più pool di archiviazione oppure un diverso Cloud Storage Pool.

6. Modifica ciascuna delle regole che hai clonato.

Per il passaggio 2 della procedura guidata Crea regola ILM, selezionare la nuova posizione dal campo **copie in**.

7. ["Crea una nuova policy ILM"](#) e sostituire ciascuna delle vecchie regole con una regola clonata.

8. Attiva la nuova politica.

9. Attendi che ILM rimuova gli oggetti dal Cloud Storage Pool e li posizioni nella nuova posizione.

Elimina pool di archiviazione 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 contenitore di Azure non contiene alcun oggetto.

Si verifica un errore se si tenta di rimuovere un Cloud Storage Pool che contiene oggetti. Vedere ["Risoluzione dei problemi dei pool di archiviazione cloud"](#).



Quando si crea un Cloud Storage Pool, StorageGRID scrive un file marcatore nel bucket o nel contenitore per identificarlo come Cloud Storage Pool. Non rimuovere questo file, che si chiama `x-ntap-sgws-cloud-pool-uuid`.

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.
2. Se la colonna Utilizzo ILM indica che Cloud Storage Pool non è in uso, selezionare la casella di controllo.
3. Selezionare **Azioni > Rimuovi**.
4. Selezionare **OK**.

Risoluzione dei problemi dei pool di archiviazione cloud

Utilizza questi passaggi per la risoluzione dei problemi per risolvere gli errori che potresti riscontrare durante la creazione, la modifica o l'eliminazione di un Cloud Storage Pool.

Determina se si è verificato un errore

StorageGRID esegue un semplice controllo dello stato di salute su ogni Cloud Storage Pool leggendo l'oggetto noto `x-ntap-sgws-cloud-pool-uuid` per garantire che il Cloud Storage Pool sia accessibile e funzioni correttamente. Quando StorageGRID rileva un errore sull'endpoint, esegue un controllo dello stato ogni minuto da ciascun nodo di archiviazione. Una volta risolto l'errore, i controlli di integrità si interrompono. Se un controllo dello stato rileva un problema, viene visualizzato un messaggio nella colonna Ultimo errore della tabella Cloud Storage Pools nella pagina Storage Pools.

La tabella mostra l'errore più recente rilevato per ciascun Cloud Storage Pool e indica da quanto tempo si è verificato l'errore.

Inoltre, viene attivato un avviso di **Errore di connettività del Cloud Storage Pool** se il controllo dello stato rileva che si sono verificati uno o più nuovi errori del Cloud Storage Pool negli ultimi 5 minuti. Se ricevi una notifica via e-mail per questo avviso, vai alla pagina Pool di archiviazione (seleziona **ILM > Pool di**

archiviazione), esamina i messaggi di errore nella colonna Ultimo errore e fai riferimento alle linee guida per la risoluzione dei problemi riportate di seguito.

Controlla se un errore è stato risolto

Dopo aver risolto eventuali problemi di fondo, è possibile determinare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, seleziona l'endpoint e seleziona **Cancella errore**. Un messaggio di conferma indica che StorageGRID ha eliminato l'errore per il Cloud Storage Pool.

Se il problema di fondo è stato risolto, il messaggio di errore non viene più visualizzato. Tuttavia, se il problema di fondo non è stato risolto (o se si verifica un errore diverso), il messaggio di errore verrà visualizzato nella colonna Ultimo errore entro pochi minuti.

Errore: controllo dello stato di integrità non riuscito. Errore dall'endpoint

Potresti riscontrare questo errore quando abiliti S3 Object Lock con conservazione predefinita per il tuo bucket Amazon S3 dopo aver iniziato a utilizzare questo bucket per un Cloud Storage Pool. Questo errore si verifica quando l'operazione PUT non ha un'intestazione HTTP con un valore di checksum del payload come Content-MD5 . Questo valore di intestazione è richiesto da AWS per le operazioni PUT nei bucket con S3 Object Lock abilitato.

Per correggere questo problema, seguire i passaggi in ["Modifica un pool di archiviazione cloud"](#) senza apportare alcuna modifica. Questa azione attiva la convalida della configurazione del Cloud Storage Pool che rileva e aggiorna automaticamente il flag S3 Object Lock su una configurazione dell'endpoint del Cloud Storage Pool.

Errore: questo pool di archiviazione cloud contiene contenuti inaspettati

Potresti riscontrare questo errore quando provi a creare, modificare o eliminare un Cloud Storage Pool. Questo errore si verifica se il bucket o il contenitore include x-ntap-sgws-cloud-pool-uuid file marker, ma quel file non ha il campo metadati con l'UUID previsto.

In genere, questo errore viene visualizzato solo se si sta creando un nuovo Cloud Storage Pool e un'altra istanza di StorageGRID sta già utilizzando lo stesso Cloud Storage Pool.

Prova uno di questi passaggi per correggere il problema:

- Se si sta configurando un nuovo Cloud Storage Pool e il bucket contiene x-ntap-sgws-cloud-pool-uuid file e chiavi di oggetti aggiuntivi simili all'esempio seguente, crea un nuovo bucket e usalo al suo posto.

Esempio di una chiave oggetto aggiuntiva: my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410

- Se il x-ntap-sgws-cloud-pool-uuid file è l'unico oggetto nel bucket, elimina questo file.

Se questi passaggi non si applicano al tuo scenario, contatta l'assistenza.

Errore: impossibile creare o aggiornare il Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi nelle seguenti circostanze:

- Quando si tenta di creare o modificare un Cloud Storage Pool.
- Quando si seleziona una combinazione di piattaforma, autenticazione o protocollo non supportata con S3 Object Lock durante la configurazione di un nuovo Cloud Storage Pool. Vedere ["Considerazioni sui pool di"](#)

Questo errore indica che un problema di connettività o di configurazione impedisce a StorageGRID di scrivere sul Cloud Storage Pool.

Per correggere il problema, rivedere il messaggio di errore dall'endpoint.

- Se il messaggio di errore contiene `Get url: EOF`, verificare che l'endpoint del servizio utilizzato per Cloud Storage Pool non utilizzi HTTP per un contenitore o un 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 archiviazione di accedere all'endpoint del servizio utilizzato per il pool di archiviazione cloud.
- Se l'errore è dovuto a una piattaforma, un'autenticazione o un protocollo non supportati, passare a una configurazione supportata con S3 Object Lock e provare a salvare nuovamente il nuovo Cloud Storage Pool.
- Per tutti gli altri messaggi di errore dell'endpoint, provare una o più delle seguenti soluzioni:
 - Crea un contenitore o un bucket esterno con lo stesso nome immesso per il Cloud Storage Pool e prova a salvare nuovamente il nuovo Cloud Storage Pool.
 - Correggi il nome del contenitore o del bucket specificato per il Cloud Storage Pool e prova a salvare nuovamente il nuovo Cloud Storage Pool.

Errore: impossibile analizzare il certificato CA

Potresti riscontrare questo errore quando provi a creare o modificare un Cloud Storage Pool. L'errore si verifica se StorageGRID non è riuscito ad analizzare il certificato immesso durante la configurazione del Cloud Storage Pool.

Per correggere il problema, controlla il certificato CA fornito per eventuali problemi.

Errore: non è stato trovato un pool di archiviazione cloud con questo ID

Potresti riscontrare questo errore quando provi a modificare o eliminare un Cloud Storage Pool. Questo errore si verifica se l'endpoint restituisce una risposta 404, che può significare uno dei seguenti:

- Le credenziali utilizzate per 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 marcatore.

Prova uno o più di questi passaggi per correggere il problema:

- Verificare che l'utente associato alla chiave di accesso configurata disponga delle autorizzazioni richieste.
- Modificare il Cloud Storage Pool con credenziali che dispongono delle autorizzazioni richieste.
- Se le autorizzazioni sono corrette, contattare l'assistenza.

Errore: impossibile controllare il contenuto del Cloud Storage Pool. Errore dall'endpoint

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Questo errore indica che un problema di connettività o di configurazione impedisce a StorageGRID di leggere il contenuto del bucket Cloud Storage Pool.

Per correggere il problema, rivedere il messaggio di errore dall'endpoint.

Errore: gli oggetti sono già stati inseriti in questo bucket

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Non è possibile eliminare un Cloud Storage Pool se contiene dati spostati lì 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.

Prova uno o più di questi passaggi per correggere il problema:

- Seguire le istruzioni per spostare nuovamente gli oggetti su StorageGRID in "Ciclo di vita di un oggetto Cloud Storage Pool".
- Se sei certo che gli oggetti rimanenti non siano stati inseriti nel Cloud Storage Pool da ILM, eliminali manualmente dal bucket.



Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbero essere stati inseriti lì da ILM. Se in seguito si tenta di accedere a un oggetto eliminato manualmente da StorageGRID, l'oggetto eliminato non verrà trovato.

Errore: il proxy ha riscontrato un errore esterno durante il tentativo di raggiungere il Cloud Storage Pool

Questo errore potrebbe verificarsi se è stato configurato un proxy di archiviazione non trasparente tra i nodi di archiviazione e l'endpoint S3 esterno utilizzato per il pool di archiviazione cloud. 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 oppure potrebbe esserci un problema di rete esterna.

Prova uno o più di questi passaggi per correggere il problema:

- Controllare le impostazioni per il Cloud Storage Pool (**ILM > Storage pool**).
- Controllare la configurazione di rete del server proxy di archiviazione.

Errore: il certificato X.509 è scaduto nel periodo di validità

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Questo errore si verifica quando l'autenticazione richiede un certificato X.509 per garantire che venga convalidato il corretto Cloud Storage Pool esterno e che il pool esterno sia vuoto prima che la configurazione del Cloud Storage Pool venga eliminata.

Per risolvere il problema, prova a seguire questi passaggi:

- Aggiornare il certificato configurato per l'autenticazione nel Cloud Storage Pool.
- Assicurarsi che tutti gli avvisi di scadenza dei certificati su questo Cloud Storage Pool siano stati risolti.

Informazioni correlate

["Ciclo di vita di un oggetto Cloud Storage Pool"](#)

Gestisci i profili di codifica di cancellazione

È possibile visualizzare i dettagli di un profilo di codifica di cancellazione e, se necessario, rinominare un profilo. È possibile disattivare un profilo di codifica di cancellazione se non è attualmente utilizzato in alcuna regola ILM.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[autorizzazioni di accesso richieste](#)".

Visualizza i dettagli del profilo di codifica di cancellazione

È possibile visualizzare i dettagli di un profilo di codifica di cancellazione per determinarne lo stato, lo schema di codifica di cancellazione utilizzato e altre informazioni.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Codifica di cancellazione**.
2. Seleziona il profilo. Viene visualizzata la pagina dei dettagli del profilo.
3. Facoltativamente, visualizza la scheda Regole ILM per un elenco delle regole ILM che utilizzano il profilo e i criteri ILM che utilizzano tali regole.
4. Facoltativamente, visualizza 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 spazio di archiviazione.

Rinominare un profilo di codifica di cancellazione

Potresti voler rinominare un profilo di codifica di cancellazione per rendere più evidente la sua funzione.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Codifica di cancellazione**.
2. Seleziona il profilo che vuoi rinominare.
3. Selezionare **Rinomina**.
4. Immettere un nome univoco per il profilo di codifica di cancellazione.

Il nome del profilo di codifica di cancellazione viene aggiunto al nome del pool di archiviazione nelle istruzioni di posizionamento per una regola ILM.



I nomi dei profili di codifica di cancellazione 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. Seleziona **Salva**.

Disattivare un profilo di codifica di cancellazione

È possibile disattivare un profilo di codifica di cancellazione se non si prevede più di utilizzarlo e se il profilo non è attualmente utilizzato in alcuna regola ILM.



Verificare che non siano in corso operazioni di riparazione di dati codificati tramite cancellazione o procedure di disattivazione. Se si tenta di disattivare un profilo di codifica di cancellazione mentre è in corso una di queste operazioni, viene visualizzato un messaggio di errore.

Informazioni su questo compito

StorageGRID impedisce la disattivazione di un profilo di codifica di cancellazione se si verifica una delle seguenti condizioni:

- Il profilo di codifica della cancellazione è attualmente utilizzato in una regola ILM.

- Il profilo di codifica della cancellazione non è più utilizzato in nessuna regola ILM, ma i dati degli oggetti e i frammenti di parità per il profilo esistono ancora.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Codifica di cancellazione**.
2. Nella scheda Attivo, rivedere la colonna **Stato** per confermare che il profilo di codifica di cancellazione che si desidera disattivare non sia utilizzato in alcuna regola ILM.

Non è possibile disattivare un profilo di codifica di cancellazione se è utilizzato in una regola ILM. Nell'esempio, il profilo 2+1 Data Center 1 viene utilizzato in almeno una regola ILM.

☐	Profile name ?	Status ?	Storage pool ?	Erasure-coding scheme ?
☐	2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
☐	New profile	Deactivated	Data Center 1	2+1

3. Se il profilo viene utilizzato in una regola ILM, attenersi alla seguente procedura:
 - a. Selezionare **ILM > Regole**.
 - b. Selezionare ciascuna regola e rivedere il diagramma di conservazione per determinare se la regola utilizza il profilo di codifica di cancellazione che si desidera disattivare.
 - c. Se la regola ILM utilizza il profilo di codifica di cancellazione che si desidera disattivare, determinare se la regola viene utilizzata in un criterio ILM.
 - d. Completare i passaggi aggiuntivi nella tabella, in base al punto in cui viene utilizzato il profilo di codifica di cancellazione.

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 richiesti passaggi aggiuntivi. Continuare con questa procedura.	Nessuno
In una regola ILM che non è mai stata utilizzata in nessuna politica ILM	i. Modifica o elimina tutte le regole ILM interessate. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di codifica di cancellazione. ii. Continuare con questa procedura.	"Lavorare con le regole e le politiche 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 una policy ILM attiva	i. Clonare la policy. ii. Rimuovere la regola ILM che utilizza il profilo di codifica di cancellazione. iii. Aggiungere una o più nuove regole ILM per garantire la protezione degli oggetti. iv. Salva, simula e attiva la nuova policy. v. Attendi che la nuova policy venga applicata 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 prima che le operazioni ILM spostino gli oggetti in nuove posizioni, in base alle nuove regole ILM. Sebbene sia possibile tentare in tutta sicurezza di disattivare un profilo di codifica di cancellazione mentre è ancora associato ai dati, l'operazione di disattivazione non andrà a buon fine. Un messaggio di errore ti informerà se il profilo non è ancora pronto per essere disattivato. vi. Modifica o elimina la regola rimossa dal criterio. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di codifica di cancellazione. vii. Continuare con questa procedura.	"Creare una policy ILM" "Lavorare con le regole e le politiche ILM"
In una regola ILM che è attualmente in una politica ILM	i. Modifica la politica. ii. Rimuovere la regola ILM che utilizza il profilo di codifica di cancellazione. iii. Aggiungere una o più nuove regole ILM per garantire che tutti gli oggetti siano protetti. iv. Salva la polizza. v. Modifica o elimina la regola rimossa dal criterio. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di codifica di cancellazione. vi. Continuare con questa procedura.	"Creare una policy ILM" "Lavorare con le regole e le politiche ILM"

e. Aggiornare la pagina Profili di codifica di cancellazione 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 scegliere **Disattiva**.

Viene visualizzata la finestra di dialogo Disattiva profilo di codifica di cancellazione.



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 codifica di cancellazione, il suo stato è Disattivato. Non è più possibile selezionare questo profilo per nessuna regola ILM. Non è possibile riattivare un profilo disattivato.
- Se StorageGRID non riesce a disattivare il profilo, viene visualizzato un messaggio di errore. Ad esempio, viene visualizzato un messaggio di errore se i dati dell'oggetto sono ancora associati a questo profilo. Potrebbe essere necessario attendere diverse settimane prima di provare nuovamente la procedura di disattivazione.

Configurare le regioni (facoltativo e solo S3)

Le regole ILM possono filtrare gli oggetti in base alle regioni in cui vengono creati i bucket S3, consentendo di archiviare oggetti provenienti da regioni diverse in posizioni di archiviazione diverse.

Se si desidera utilizzare una regione bucket S3 come filtro in una regola, è necessario prima creare le regioni che possono essere utilizzate dai bucket nel sistema.



Non è possibile modificare la regione di un bucket dopo averlo creato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Informazioni su questo compito

Quando si crea un bucket S3, è possibile specificare che il bucket venga creato in una regione specifica. Specificando una regione, il bucket può essere geograficamente vicino ai suoi utenti, il che può aiutare a ottimizzare la latenza, ridurre al minimo i costi e soddisfare i requisiti normativi.

Quando si crea una regola ILM, potrebbe essere opportuno 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 copie di tali oggetti vengano posizionate su nodi di archiviazione in un sito di data center all'interno di quella regione per ottimizzare la latenza.

Quando si configurano le regioni, seguire queste linee guida:

- Per impostazione predefinita, tutti i bucket sono considerati appartenenti a `us-east-1` regione.
- È necessario creare le regioni utilizzando Grid Manager prima di poter specificare una regione non predefinita quando si creano bucket utilizzando Tenant Manager o Tenant Management API oppure con l'elemento di richiesta LocationConstraint per le richieste S3 PUT Bucket API. Si verifica un errore se una richiesta PUT Bucket utilizza una regione non definita in StorageGRID.
- Quando si crea il bucket S3, è necessario utilizzare il nome esatto della regione. I nomi delle regioni sono sensibili alle maiuscole e alle minuscole. I caratteri validi sono numeri, lettere e trattini.



EU non è considerato un alias di 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 è utilizzata in una regola assegnata a un criterio (attivo o inattivo).
- Se si utilizza una regione non valida come filtro avanzato in una regola ILM, non è possibile aggiungere tale regola a un criterio.

Una regione non valida può verificarsi se si utilizza una regione come filtro avanzato in una regola ILM ma in seguito si elimina tale regione oppure se si utilizza l'API di gestione della griglia per creare una regola e si specifica una regione che non è stata definita.

- Se elimini una regione dopo averla utilizzata per creare un bucket S3, dovrai aggiungere nuovamente la regione se desideri utilizzare il filtro avanzato Vincolo di posizione per trovare oggetti in quel bucket.

Passi

1. Selezionare **ILM > Regioni**.

Viene visualizzata la pagina Regioni, in cui sono elencate le regioni attualmente definite. **Regione 1** mostra la regione predefinita, `us-east-1`, che non può essere modificato o rimosso.

2. Per aggiungere una regione:

- a. Seleziona **Aggiungi un'altra regione**.
- b. Inserisci il nome della regione che desideri utilizzare durante la creazione dei bucket S3.

Quando si crea il bucket S3 corrispondente, è necessario utilizzare questo nome di regione esatto come elemento di richiesta LocationConstraint.

3. Per rimuovere una regione non utilizzata, seleziona l'icona Elimina .

Se si tenta di rimuovere una regione attualmente utilizzata in un criterio (attivo o inattivo), viene visualizzato un messaggio di errore.

4. Una volta completate le modifiche, seleziona **Salva**.

Ora puoi selezionare queste regioni dalla sezione Filtri avanzati nel passaggio 1 della procedura guidata Crea regola ILM. Vedere ["Utilizzare filtri avanzati nelle regole ILM"](#).

Crea regola ILM

Utilizzare le regole ILM per gestire gli oggetti

Per gestire gli oggetti, è necessario creare un set di regole di gestione del ciclo di vita delle informazioni (ILM) e organizzarle in una policy ILM.

Ogni oggetto inserito nel sistema viene valutato in base alla policy attiva. Quando una regola nella policy corrisponde ai metadati di un oggetto, le istruzioni nella regola determinano quali azioni intraprende StorageGRID per copiare e archiviare quell'oggetto.



I metadati degli oggetti non sono gestiti dalle regole ILM. I metadati degli oggetti vengono invece archiviati in un database Cassandra, in quello che è noto come archivio di metadati. In ogni sito vengono conservate automaticamente tre copie dei metadati degli oggetti per proteggere i dati da eventuali perdite.

Elementi di una regola ILM

Una regola ILM è composta da tre elementi:

- **Criteri di filtraggio:** 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 dell'oggetto. Ogni regola può includere una sequenza di istruzioni di posizionamento per modificare nel tempo il numero, il tipo e la posizione delle copie dell'oggetto. Quando scade il periodo di tempo per un tirocinio, le istruzioni del tirocinio successivo vengono applicate automaticamente dalla successiva valutazione ILM.
- **Comportamento di acquisizione:** 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 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 ampi e distinti. Questi filtri consentono di applicare una regola a specifici account tenant, a specifici bucket S3 o a entrambi.

I filtri di base offrono un modo semplice per applicare regole diverse a un gran numero di oggetti. Ad esempio, potrebbe essere necessario archiviare i registri finanziari della tua azienda per soddisfare i requisiti normativi, mentre i dati del reparto marketing potrebbero dover essere archiviati per facilitare le operazioni quotidiane. Dopo aver creato account tenant separati per ciascun reparto o dopo aver suddiviso i dati dei 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 ti offrono un controllo granulare. È possibile creare filtri per selezionare gli oggetti in base alle seguenti proprietà:
 - Tempo di ingestione
 - Ultimo orario di accesso
 - Tutto o parte del nome dell'oggetto (Chiave)
 - Vincolo di posizione (solo S3)
 - Dimensione dell'oggetto
 - Metadati utente
 - Tag oggetto (solo S3)

È possibile filtrare gli oggetti in base a criteri molto specifici. Ad esempio, gli oggetti archiviati dal reparto di

diagnostica per immagini di un ospedale potrebbero essere utilizzati frequentemente quando hanno meno di 30 giorni e raramente in seguito, mentre gli oggetti che contengono informazioni sulle visite dei pazienti potrebbero dover essere copiati nel reparto di fatturazione presso la sede centrale della rete sanitaria. È possibile creare filtri che identificano ogni tipo di oggetto in base al nome dell'oggetto, alle dimensioni, ai tag dell'oggetto S3 o a qualsiasi altro criterio rilevante, quindi creare regole separate per archiviare in modo appropriato ogni set di oggetti.

È possibile combinare i filtri in base alle proprie esigenze in un'unica regola. Ad esempio, il reparto marketing potrebbe voler archiviare file di immagini di grandi dimensioni in modo diverso rispetto ai record dei fornitori, mentre il reparto delle risorse umane potrebbe dover archiviare i record del personale in una specifica area geografica e le informazioni sulle politiche in modo centralizzato. In questo caso è possibile creare regole che filtrano in base all'account del tenant per separare i record da ciascun reparto, utilizzando al contempo filtri in ogni 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 archiviati 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 istruzioni di posizionamento:

- Si inizia specificando l'ora di riferimento, che determina quando iniziano le istruzioni di posizionamento. Il momento di riferimento potrebbe essere il momento in cui un oggetto viene acquisito, quando si accede a un oggetto, quando un oggetto con versione diventa non corrente o un momento definito dall'utente.
- Successivamente, si specifica quando verrà applicato il posizionamento, in relazione all'orario di riferimento. Ad esempio, un posizionamento potrebbe iniziare il giorno 0 e continuare per 365 giorni, in relazione al momento in cui l'oggetto è stato acquisito.
- Infine, si specifica il tipo di copie (codifica di replicazione o di cancellazione) e la posizione in cui vengono archiviate le copie. Ad esempio, potresti voler archiviare due copie replicate in due siti diversi.

Ogni regola può definire più posizionamenti per un singolo periodo di tempo e posizionamenti diversi per periodi di tempo diversi.

- Per posizionare oggetti in più posizioni durante un singolo periodo di tempo, seleziona **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, seleziona **Aggiungi un altro periodo di tempo** per aggiungere il periodo di tempo successivo. Quindi, specificare una o più righe all'interno del periodo di tempo.

L'esempio mostra due istruzioni di posizionamento nella pagina Definisci posizionamenti della procedura guidata Crea regola ILM.

Time period and placements Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1
From Day store for days

Store objects by copies at ,

and store objects by using

1

Add other type or location

Time period 2
From Day store forever

Store objects by copies at

2

Add other type or location

Le prime istruzioni di posizionamento **1** ha due linee per il primo anno:

- La prima riga crea due copie replicate dell'oggetto in due siti di data center.
- La seconda riga crea una copia con codice di cancellazione 6+3 utilizzando tutti i siti del data center.

La seconda istruzione di posizionamento **2** ne 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 di posizionamento finale continui per sempre o finché non saranno più necessarie copie dell'oggetto.

Alla scadenza di ogni periodo di tempo previsto dalla regola, vengono applicate le istruzioni di posizionamento dei contenuti per il periodo di tempo successivo. Vengono create nuove copie dell'oggetto e quelle 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 oppure se vengono create copie provvisorie e le istruzioni di posizionamento vengono applicate in un secondo momento. Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Bilanciato:** StorageGRID tenta di effettuare tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono effettuate copie provvisorie e il client riceve un messaggio di conferma dell'operazione riuscita. Quando possibile, vengono effettuate le copie specificate nella norma ILM.
- **Rigoroso:** tutte le copie specificate nella regola ILM devono essere eseguite prima che il risultato positivo venga restituito al client.

- **Doppio commit:** StorageGRID crea immediatamente copie provvisorie dell'oggetto e restituisce il risultato positivo al client. Quando possibile, vengono effettuate le copie specificate nella norma ILM.

Informazioni correlate

- ["Opzioni di acquisizione"](#)
- ["Vantaggi, svantaggi e limitazioni delle opzioni di ingestione"](#)
- ["Come la coerenza e le regole ILM interagiscono per influenzare la protezione dei dati"](#)

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applica solo agli oggetti appartenenti all'inquilino A.
- Realizza due copie replicate di quegli oggetti e conserva ciascuna copia in un luogo diverso.
- Conservare le due copie "per sempre", il che significa che StorageGRID non le eliminerà automaticamente. StorageGRID conserverà invece questi oggetti finché non verranno eliminati da una richiesta di eliminazione del client o dalla scadenza del ciclo di vita di un bucket.
- Utilizzare l'opzione Bilanciato per il comportamento di acquisizione: l'istruzione di posizionamento su due siti viene applicata non appena il Tenant A salva un oggetto in StorageGRID, a meno che non sia possibile effettuare 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 provvisorie sui nodi di archiviazione del sito 1. Non appena il Sito 2 sarà disponibile, StorageGRID effettuerà la copia richiesta in quel sito.

Informazioni correlate

- ["Che cos'è un pool di archiviazione"](#)
- ["Che cos'è un Cloud Storage Pool"](#)

Accedi 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.

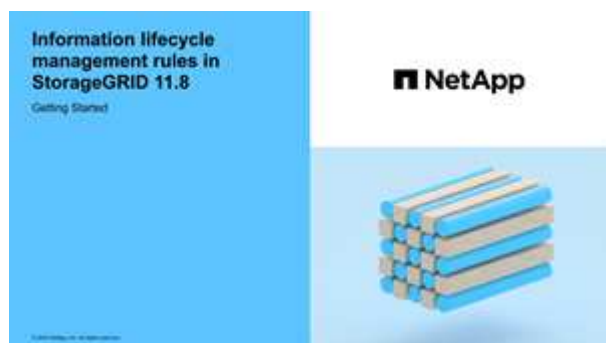


Se si desidera creare la regola ILM predefinita per una policy, seguire la procedura ["istruzioni per la creazione di una regola ILM predefinita"](#) Invece.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Se si desidera specificare a quali account tenant si applica questa regola, è necessario ["Autorizzazione degli account degli inquilini"](#) oppure conosci l'ID account per ogni account.
- Se si desidera che la regola filtri gli oggetti in base ai metadati dell'ora dell'ultimo accesso, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati dal bucket S3.
- Hai configurato tutti i Cloud Storage Pool che intendi utilizzare. Vedere ["Crea un pool di archiviazione cloud"](#) .
- Hai familiarità con il ["opzioni di ingestione"](#) .

- Se è necessario creare una regola conforme da utilizzare con S3 Object Lock, è necessario avere familiarità con ["requisiti per S3 Object Lock"](#) .
- Facoltativamente, hai guardato il video: ["Video: panoramica delle regole ILM"](#) .



Informazioni su questo compito

Durante la creazione delle regole ILM:

- Prendiamo in considerazione la topologia e le configurazioni di archiviazione del sistema StorageGRID .
- Considera quali tipi di copie di oggetti vuoi realizzare (replicate o con codice di cancellazione) e il numero di copie necessarie per ciascun oggetto.
- Determinare quali tipi di metadati degli oggetti vengono utilizzati nelle applicazioni che si connettono al sistema StorageGRID . Le regole ILM filtrano gli oggetti in base ai loro metadati.
- Considera dove vuoi che vengano posizionate le copie degli oggetti nel tempo.
- Decidi quale opzione di gestione utilizzare (Bilanciata, Rigorosa o Doppio commit).

Passi

1. Selezionare **ILM > Regole**.
2. Seleziona **Crea**. ["Passaggio 1 \(Inserisci i dettagli\)"](#) viene visualizzata la procedura guidata Crea una regola ILM.

Passaggio 1 di 3: Inserisci i dettagli

Il passaggio **Inserisci dettagli** della procedura guidata Crea una regola ILM consente di immettere un nome e una descrizione per la regola e di definire i filtri per la regola.

L'inserimento di una descrizione e la definizione dei filtri per la regola sono facoltativi.

Informazioni su questo compito

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 di bucket, oppure filtri avanzati, come le dimensioni dell'oggetto o i metadati dell'utente.

Passi

1. Immettere un nome univoco per la regola nel campo **Nome**.
2. Facoltativamente, inserisci una breve descrizione della regola nel campo **Descrizione**.

Dovresti descrivere lo scopo o la funzione della regola in modo da poterla riconoscere in seguito.

3. Facoltativamente, seleziona uno o più account tenant S3 a cui si applica questa regola. Se questa regola si applica a tutti gli inquilini, lasciare vuoto questo campo.

Se non si dispone né dell'autorizzazione di accesso Root né dell'autorizzazione Account tenant, non è possibile selezionare i tenant dall'elenco. In alternativa, immettere l'ID tenant oppure più ID come stringa delimitata da virgole.

4. Facoltativamente, specificare i bucket S3 a cui si applica questa regola.

Se è selezionata l'opzione **si applica a tutti i bucket** (impostazione predefinita), la regola si applica a tutti i bucket S3.

5. Per i tenant S3, selezionare facoltativamente **Sì** per applicare la regola solo alle versioni precedenti degli oggetti nei bucket S3 in cui è abilitato il controllo delle versioni.

Se selezioni **Sì**, "Tempo non corrente" verrà automaticamente selezionato per il tempo di riferimento in ["Passaggio 2 della procedura guidata Crea una regola ILM"](#).



Il tempo non corrente si applica solo agli oggetti S3 nei bucket abilitati al controllo delle versioni. Vedere ["Operazioni sui bucket, PutBucketVersioning"](#) E ["Gestisci gli oggetti con S3 Object Lock"](#).

È possibile utilizzare questa opzione per ridurre l'impatto sull'archiviazione degli oggetti sottoposti a controllo delle versioni, filtrando le versioni degli oggetti non correnti. Vedere ["Esempio 4: regole e policy ILM per oggetti con versione S3"](#).

6. Facoltativamente, seleziona **Aggiungi un filtro avanzato** per specificare filtri aggiuntivi.

Se non si configura il filtro avanzato, la regola si applica a tutti gli oggetti che corrispondono ai filtri di base. Per ulteriori informazioni sul filtraggio avanzato, vedere [Utilizzare filtri avanzati nelle regole ILM](#) E [Specificare più tipi e valori di metadati](#).

7. Selezionare **Continua**. ["Fase 2 \(Definire i posizionamenti\)"](#) viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare filtri avanzati nelle regole ILM

Il filtraggio avanzato consente di creare regole ILM che si applicano solo a oggetti specifici in base ai loro metadati. Quando si imposta un filtro avanzato per una regola, si seleziona il tipo di metadati che si desidera abbinare, si seleziona un operatore e si specifica un valore per i metadati. Quando gli oggetti vengono valutati, la regola ILM viene applicata solo agli oggetti che hanno metadati corrispondenti al filtro avanzato.

Nella tabella sono indicati i tipi di metadati che è possibile specificare nei filtri avanzati, gli operatori che è possibile utilizzare per ciascun tipo di metadati e i valori dei metadati previsti.

Tipo di metadati	Operatori supportati	Valore dei metadati
Tempo di ingestione	• È • non è • è prima • è acceso o prima • è dopo • è acceso o dopo	Ora e data in cui l'oggetto è stato ingerito. Nota: per evitare problemi di risorse durante l'attivazione di un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Tempo di acquisizione in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare il tempo di acquisizione su un valore maggiore o uguale al momento approssimativo in cui la nuova policy entrerà in vigore, per garantire che gli oggetti esistenti non vengano spostati inutilmente.
Chiave	• è uguale • non è uguale • contiene • non contiene • inizia con • non inizia con • finisce con • non finisce con	Tutta o parte di una chiave univoca dell'oggetto S3. Ad esempio, potresti voler abbinare oggetti che terminano con <code>.txt</code> o inizia con <code>test-object/</code>.
Ultimo orario di accesso	• È • non è • è prima • è acceso o prima • è dopo • è acceso o dopo	Ora e data dell'ultimo recupero (lettura o visualizzazione) dell'oggetto. Nota: se hai intenzione di "usa l'ultimo orario di accesso" come filtro avanzato, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati per il bucket S3.
Vincolo di posizione (solo S3)	• è uguale • non è uguale	La regione in cui è stato creato un bucket S3. Utilizzare ILM > Regioni per definire le regioni visualizzate. Nota: il valore <code>us-east-1</code> corrisponderà agli oggetti nei bucket creati nella regione <code>us-east-1</code> e agli oggetti nei bucket per i quali non è specificata alcuna regione. Vedere "Configurare le regioni (facoltativo e solo S3)".

Tipo di metadati	Operatori supportati	Valore dei metadati
Dimensione dell'oggetto	• è uguale • non è uguale • meno di • minore o uguale a • maggiore di • maggiore o uguale a	Le dimensioni dell'oggetto. La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.
Metadati utente	• contiene • finisce con • è uguale • esiste • inizia con • non contiene • non finisce con • non è uguale • non esiste • non inizia con	Coppia chiave-valore, dove Nome metadati utente è la chiave e Valore metadati è il valore. Ad esempio, per filtrare gli oggetti che hanno metadati utente di <code>color=blue</code>, specificare <code>color</code> per Nome metadati utente, <code>equals</code> per l'operatore, e <code>blue</code> per Valore metadati. Nota: i nomi dei metadati utente non sono sensibili alle maiuscole e alle minuscole; lo sono invece i valori dei metadati utente.
Tag oggetto (solo S3)	• contiene • finisce con • è uguale • esiste • inizia con • non contiene • non finisce con • non è uguale • non esiste • non inizia con	Coppia chiave-valore, dove Nome tag oggetto è la chiave e Valore tag oggetto è il valore. Ad esempio, per filtrare gli oggetti che hanno un tag oggetto di <code>Image=True</code>, specificare <code>Image</code> per nome tag oggetto, <code>equals</code> per l'operatore, e <code>True</code> per valore tag oggetto. Nota: i nomi e i valori dei tag degli oggetti sono sensibili alle maiuscole e alle minuscole. È necessario immettere questi elementi esattamente come sono stati definiti per l'oggetto.

Specificare più tipi e valori di metadati

Quando si definisce un filtro 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, è necessario selezionare il tipo di metadati **Dimensione oggetto** e specificare due valori di metadati.

- Il primo valore dei metadati specifica oggetti maggiori o uguali a 10 MB.
- Il secondo valore dei metadati specifica oggetti di dimensioni inferiori o uguali a 100 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than or equal to ▼ 10 ↕ MB ▼ ✕

and Object size ▼ less than or equal to ▼ 100 ↕ MB ▼ ✕

Utilizzando più voci è possibile avere un controllo preciso sugli oggetti da abbinare. Nell'esempio seguente, la regola si applica agli oggetti che hanno Brand A o Brand B come valore dei metadati utente camera_type. Tuttavia, la regola si applica solo agli oggetti Brand B di dimensioni inferiori a 10 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

User metadata ▼ camera_type equals ▼ Brand A ✕

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

User metadata ▼ camera_type equals ▼ Brand B ✕

and Object size ▼ less than or equal to ▼ 10 ↕ MB ▼ ✕

[Add another advanced filter](#)

Fase 2 di 3: definire i posizionamenti

Il passaggio **Definisci posizionamenti** della procedura guidata Crea regola ILM consente di definire le istruzioni di posizionamento che determinano per quanto tempo gli oggetti vengono archiviati, il tipo di copie (replicate o con codice di cancellazione), la posizione di archiviazione e il numero di copie.



Gli screenshot mostrati sono esempi. I risultati potrebbero variare a seconda della versione StorageGRID .

Informazioni su questo compito

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 all'infinito oppure finché non avrai più bisogno di copie dell'oggetto.

Ogni istruzione di posizionamento può avere più righe se si desidera creare diversi tipi di copie o utilizzare posizioni diverse durante quel 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 realizzata una copia con codice di cancellazione 2+1 e salvata in un solo sito.

Time period 1
From Day
0
store
for
365
days

Store objects by
replicating
1
copies at
Site 1

and store objects by
replicating
1
copies at
Site 2

Add other type or location

Time period 2
From Day
365
store
forever

Store objects by
erasure coding
using
2+1 EC scheme at Site 3

Add other type or location

Passi

1. Per **Tempo di riferimento**, seleziona il tipo di tempo da utilizzare per calcolare l'ora di inizio di un'istruzione di tirocinio.

Opzione	Descrizione
Tempo di ingestione	Il momento in cui l'oggetto è stato ingerito.
Ultimo orario di accesso	Ora dell'ultima volta in cui l'oggetto è stato recuperato (letto o visualizzato). Per utilizzare questa opzione, è necessario abilitare gli aggiornamenti all'ora dell'ultimo accesso per il bucket S3. Fare riferimento a "Utilizzare l'orario dell'ultimo accesso nelle regole ILM" .
Ora di creazione definita dall'utente	Un orario specificato nei metadati definiti dall'utente.
Tempo non corrente	"Tempo non corrente" viene selezionato automaticamente se hai selezionato Sì per la domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con controllo delle versioni abilitato)?" in "Passaggio 1 della procedura guidata Crea una regola ILM" .

Se vuoi creare una regola *conforme*, devi selezionare **Ora di inserimento**. Fare riferimento a ["Gestisci gli oggetti con S3 Object Lock"](#) .

2. Nella sezione **Periodo di tempo e posizionamenti**, inserisci un orario di inizio e una durata per il primo periodo di tempo.

Ad esempio, potresti voler specificare dove archiviare gli oggetti per il primo anno (*Dal giorno 0 archivia 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**, seleziona **replica**.
- b. Seleziona il numero di copie che desideri effettuare.

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 espone i dati al rischio di perdita permanente. Fare riferimento a ["Perché non dovresti usare la replicazione a copia singola"](#).

Per evitare il rischio, eseguire una o più delle seguenti operazioni:

- Aumentare il numero di copie per il periodo di tempo.
- Aggiungere copie ad altri pool di archiviazione o a un pool di archiviazione cloud.
- Selezionare **codifica di cancellazione** invece di **replicazione**.

È possibile ignorare tranquillamente questo avviso se questa regola crea già più copie per tutti i periodi di tempo.

- c. Nel campo **copie in**, seleziona i pool di archiviazione che desideri aggiungere.

Se si specifica un solo pool di archiviazione, tenere presente che StorageGRID può archiviare solo una copia replicata di un oggetto su un dato nodo di archiviazione. Se la griglia include tre nodi di archiviazione e si seleziona 4 come numero di copie, verranno effettuate solo tre copie, una copia per ciascun nodo di archiviazione.

L'avviso **Posizionamento ILM non realizzabile** viene attivato per indicare che la regola ILM non può essere applicata completamente.

Se si specifica più di un pool di archiviazione, tenere a mente queste regole:

- Il numero di copie non può essere maggiore del numero di pool di archiviazione.
- Se il numero di copie è uguale al numero di pool di archiviazione, una copia dell'oggetto viene archiviata in ciascun pool di archiviazione.
- Se il numero di copie è inferiore al numero di pool di archiviazione, una copia viene archiviata nel sito di acquisizione, quindi il sistema distribuisce le copie rimanenti per mantenere bilanciato l'utilizzo del disco tra i pool, garantendo al contempo che nessun sito riceva più di una copia di un oggetto.
- Se i pool di archiviazione si sovrappongono (contengono gli stessi nodi di archiviazione), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. Per questo motivo, non specificare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) e un altro pool di archiviazione.

4. Se vuoi creare una copia con codice di cancellazione:

- a. Dall'elenco a discesa **Memorizza oggetti per**, seleziona **codifica di cancellazione**.



La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

- b. Se non hai aggiunto un filtro Dimensione oggetto per un valore superiore a 200 KB, seleziona **Precedente** per tornare al passaggio 1. Quindi, seleziona **Aggiungi un filtro avanzato** e imposta un

filtro **Dimensione oggetto** su un valore maggiore di 200 KB.

- c. Selezionare il pool di archiviazione che si desidera aggiungere e lo schema di codifica di cancellazione che si desidera utilizzare.

La posizione di archiviazione per una copia con codice di cancellazione include il nome dello schema di codifica di cancellazione, seguito dal nome del pool di archiviazione.

Gli schemi di codifica di cancellazione disponibili sono limitati dal numero di nodi di archiviazione nel pool di archiviazione selezionato. UN Recommended Il badge appare accanto agli schemi che forniscono entrambi i "migliore protezione o il minimo sovraccarico di archiviazione" .

5. Facoltativamente:

- a. Seleziona **Aggiungi altro tipo o posizione** per creare copie aggiuntive in posizioni diverse.
- b. Seleziona **Aggiungi un altro periodo di tempo** per aggiungere periodi di tempo diversi.



L'eliminazione degli oggetti avviene in base alle seguenti impostazioni:

- 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**.
- A seconda di "impostazioni del periodo di conservazione del bucket e del tenant" , gli oggetti potrebbero non essere eliminati anche se termina il periodo di conservazione ILM.

6. Se si desidera archiviare oggetti in un Cloud Storage Pool:

- a. Nell'elenco a discesa **Archivia oggetti per**, seleziona **replica**.
- b. Selezionare il campo **copie in**, quindi selezionare un Cloud Storage Pool.

Quando si utilizzano i Cloud Storage Pool, tenere a mente queste regole:

- Non è possibile 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 archiviazione nella stessa istruzione di posizionamento.
- È possibile archiviare solo una copia di un oggetto in un determinato Cloud Storage Pool. Se si imposta **Copie** su 2 o più, viene visualizzato un messaggio di errore.
- Non è possibile archiviare più di una copia dell'oggetto contemporaneamente in un Cloud Storage Pool. Viene visualizzato un messaggio di errore se più posizionamenti che utilizzano un Cloud Storage Pool hanno date sovrapposte o se più righe nello stesso posizionamento utilizzano un Cloud Storage Pool.
- È possibile archiviare un oggetto in un Cloud Storage Pool nello stesso momento in cui l'oggetto viene archiviato come copie replicate o con codice di cancellazione 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 ogni posizione.

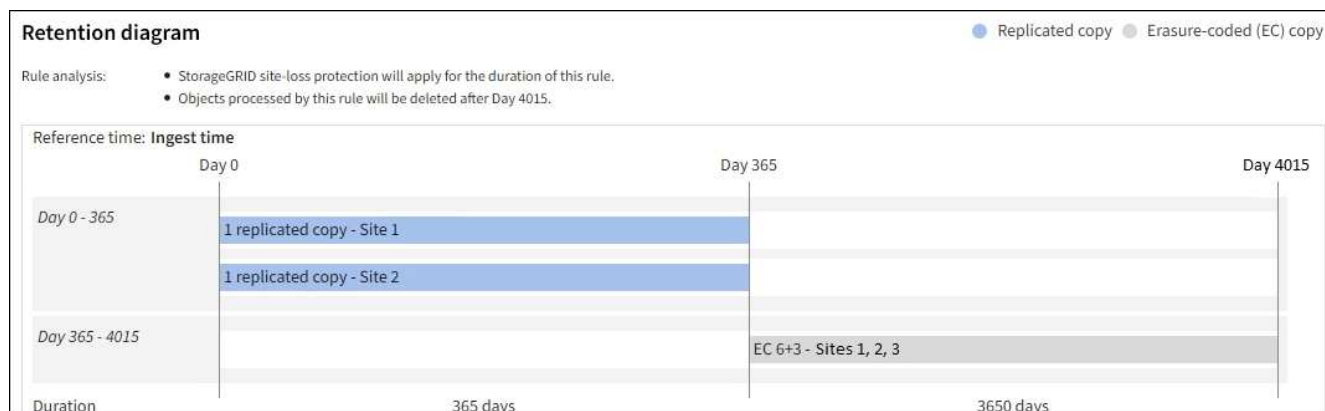
7. Nel diagramma di ritenzione, conferma le istruzioni di posizionamento.

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 siti. Dopo 11 anni totali, gli oggetti verranno eliminati da StorageGRID.

La sezione Analisi delle regole del diagramma di conservazione afferma:

- La protezione contro le perdite del sito StorageGRID sarà valida per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola verranno eliminati dopo il giorno 4015.

Fare riferimento a ["Abilita la protezione contro la perdita del sito."](#)



- Selezionare **Continua**. ["Passaggio 3 \(selezionare il comportamento di acquisizione\)"](#) viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare l'orario dell'ultimo accesso nelle regole ILM

È possibile utilizzare l'orario dell'ultimo accesso come orario di riferimento in una regola ILM. Ad esempio, potresti voler lasciare gli oggetti visualizzati negli ultimi tre mesi sui nodi di archiviazione locali, spostando invece gli oggetti non visualizzati di recente in una posizione esterna. È anche possibile utilizzare l'ora dell'ultimo accesso come filtro avanzato se si desidera che una regola ILM venga applicata solo agli oggetti a cui si è effettuato l'ultimo accesso in una data specifica.

Informazioni su questo compito

Prima di utilizzare l'orario dell'ultimo accesso in una regola ILM, esaminare le seguenti considerazioni:

- Quando si utilizza l'orario dell'ultimo accesso come orario di riferimento, tenere presente che la modifica dell'orario dell'ultimo accesso per un oggetto non attiva una valutazione ILM immediata. Al contrario, vengono valutati i posizionamenti dell'oggetto e l'oggetto viene spostato secondo necessità quando l'ILM in background valuta l'oggetto. Potrebbero volerci due settimane o più dopo l'accesso all'oggetto.

Tieni conto di questa latenza quando crei regole ILM basate sull'orario dell'ultimo accesso ed evita posizionamenti che utilizzano periodi di tempo brevi (meno di un mese).

- Quando si utilizza l'orario dell'ultimo accesso come filtro avanzato o come orario di riferimento, è necessario abilitare gli aggiornamenti dell'orario dell'ultimo accesso per i bucket S3. Puoi usare il ["Responsabile degli inquilini"](#) o il ["API di gestione degli inquilini"](#).



Per impostazione predefinita, gli aggiornamenti dell'orario dell'ultimo accesso sono disabilitati per i bucket S3.



Tieni presente che l'abilitazione degli aggiornamenti dell'ora dell'ultimo accesso può ridurre le prestazioni, soprattutto nei sistemi con oggetti di piccole dimensioni. L'impatto sulle prestazioni si verifica perché StorageGRID deve aggiornare gli oggetti con nuovi timestamp ogni volta che vengono recuperati.

La tabella seguente riassume se l'orario dell'ultimo accesso viene aggiornato per tutti gli oggetti nel bucket per diversi tipi di richieste.

Tipo di richiesta	Se l'orario dell'ultimo accesso viene aggiornato quando gli aggiornamenti dell'orario dell'ultimo accesso sono disabilitati	Se l'orario dell'ultimo accesso viene aggiornato quando sono abilitati gli aggiornamenti dell'orario dell'ultimo accesso
Richiesta di recupero di un oggetto, del suo elenco di controllo di accesso o dei suoi metadati	NO	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì
Richiesta di copiare un oggetto da un bucket all'altro	• No, per la copia sorgente • Sì, per la copia di destinazione	• Sì, per la copia sorgente • Sì, per la copia di destinazione
Richiesta di completamento di un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Passaggio 3 di 3: seleziona il comportamento di acquisizione

Il passaggio **Seleziona comportamento di acquisizione** della procedura guidata Crea regola ILM consente di scegliere in che modo gli oggetti filtrati da questa regola vengono protetti durante l'acquisizione.

Informazioni su questo compito

StorageGRID può creare copie provvisorie e mettere in coda gli oggetti per una successiva valutazione ILM, oppure può creare copie per soddisfare immediatamente le istruzioni di posizionamento della regola.

Passi

1. Seleziona il ["comportamento di ingestione"](#) da usare.

Per ulteriori informazioni, consultare ["Vantaggi, svantaggi e limitazioni delle opzioni di ingestione"](#).



Non è possibile utilizzare l'opzione Bilanciato o Rigoroso se la regola utilizza uno di questi posizionamenti:

- Un pool di archiviazione cloud al giorno 0
- Un pool di archiviazione cloud quando la regola utilizza un orario di creazione definito dall'utente come orario di riferimento

Vedere ["Esempio 5: regole e policy ILM per un comportamento di acquisizione rigoroso"](#).

2. Seleziona **Crea**.

Viene creata la regola ILM. La regola non diventa attiva finché non viene aggiunta a un ["Politica ILM"](#) e tale politica viene attivata.

Per visualizzare i dettagli della regola, seleziona il nome della regola nella pagina delle regole ILM.

Crea una regola ILM predefinita

Prima di creare un criterio ILM, è necessario creare una regola predefinita per posizionare nel criterio tutti 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"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Informazioni su questo compito

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 nel criterio.

In questo esempio di policy, la prima regola si applica solo agli oggetti appartenenti a test-tenant-1. La regola predefinita, che è l'ultima, si applica agli oggetti appartenenti a tutti gli altri account tenant.

Proposed policy name

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.

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

Select rules

Rule order	Rule name	Filters
1	EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	—

Quando crei la regola predefinita, tieni a mente questi requisiti:

- La regola predefinita verrà automaticamente posizionata come ultima regola quando la aggiungi a un criterio.
- La regola predefinita non può utilizzare filtri di base o avanzati.
- La regola predefinita deve essere applicata a tutte le versioni dell'oggetto.

- La regola predefinita dovrebbe creare copie replicate.



Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per una policy. Le regole di codifica di cancellazione dovrebbero utilizzare un filtro avanzato per impedire che gli oggetti più piccoli vengano codificati in modo errato.

- In generale, la regola predefinita dovrebbe conservare gli oggetti per sempre.
- Se si utilizza (o si prevede di abilitare) l'impostazione globale S3 Object Lock, la regola predefinita deve essere conforme.

Passi

1. Selezionare **ILM > Regole**.

2. Seleziona **Crea**.

Viene visualizzato il passaggio 1 (Immissione dei dettagli) della procedura guidata Crea regola ILM.

3. Immettere un nome univoco per la regola nel campo **Nome regola**.

4. Facoltativamente, inserisci una breve descrizione della regola nel campo **Descrizione**.

5. Lasciare vuoto il campo **Account inquilino**.

La regola predefinita deve essere applicata a tutti gli account tenant.

6. Lasciare la selezione a discesa Nome bucket come **applicabile a tutti i bucket**.

La regola predefinita deve essere applicata a tutti i bucket S3.

7. Mantenere la risposta predefinita, **No**, per la domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con controllo delle versioni abilitato)?"

8. Non aggiungere filtri avanzati.

La regola predefinita non può specificare alcun filtro.

9. Selezionare **Avanti**.

Viene visualizzato il passaggio 2 (Definizione dei posizionamenti).

10. Per Tempo di riferimento, selezionare un'opzione qualsiasi.

Se hai mantenuto la risposta predefinita, **No**, alla domanda "Applicare questa regola solo alle versioni precedenti dell'oggetto?" Il tempo non corrente non verrà incluso nell'elenco a discesa. La regola predefinita deve essere applicata a tutte le versioni dell'oggetto.

11. Specificare le istruzioni di posizionamento per la regola predefinita.

- La regola predefinita dovrebbe 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 una policy. Le regole di codifica di cancellazione dovrebbero includere il filtro avanzato **Dimensione oggetto (MB) maggiore di 200 KB** per impedire che oggetti più piccoli vengano codificati in modo da essere cancellati.

- Se si utilizza (o si prevede di abilitare) l'impostazione globale S3 Object Lock, la regola predefinita deve essere conforme:
 - Deve creare almeno due copie replicate dell'oggetto o una copia con codice di cancellazione.
 - Queste copie devono essere presenti sui nodi di archiviazione per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
 - Le copie degli oggetti non possono essere salvate in un Cloud Storage Pool.
 - Almeno una riga delle istruzioni di posizionamento deve iniziare dal giorno 0, utilizzando l'ora di acquisizione come ora di riferimento.
 - Almeno una riga delle istruzioni di posizionamento deve essere "per sempre".

12. Consultare il diagramma di ritenzione per confermare le istruzioni di posizionamento.

13. Selezionare **Continua**.

Viene visualizzato il passaggio 3 (Seleziona comportamento di acquisizione).

14. Seleziona l'opzione di acquisizione da utilizzare e seleziona **Crea**.

Gestire le policy ILM

Utilizzare le policy ILM

Una policy di gestione del ciclo di vita delle informazioni (ILM) è un insieme ordinato di regole ILM che determinano il modo in cui il sistema StorageGRID gestisce i dati degli oggetti nel tempo.



Una policy ILM configurata in modo errato può comportare una perdita di dati irrecoverabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Criterio ILM predefinito

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 di un sito, la regola predefinita replica una copia di ciascun oggetto in ogni sito.

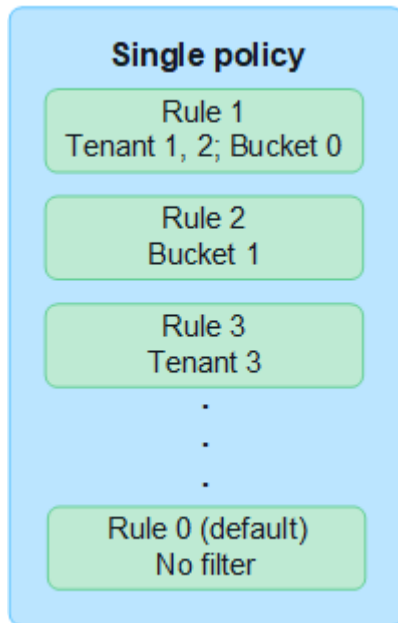
Se la policy predefinita non soddisfa i requisiti di archiviazione, è possibile creare regole e policy personalizzate. Vedere ["Crea una regola ILM"](#) E ["Creare una policy ILM"](#) .

Una o più polizze ILM attive?

È possibile avere una o più polizze ILM attive contemporaneamente.

Una politica

Se la griglia utilizzerà uno schema di protezione dei dati semplice con poche regole specifiche per tenant e bucket, utilizzare un singolo criterio ILM attivo. Le regole ILM possono contenere filtri per gestire diversi bucket o tenant.



Quando si dispone di una sola policy e i requisiti di un tenant cambiano, è necessario creare una nuova policy ILM o clonare la policy esistente per applicare le modifiche, simulare e quindi attivare la nuova policy ILM. Le modifiche alla policy ILM potrebbero comportare spostamenti di oggetti che potrebbero richiedere molti giorni e causare latenza del sistema.

Politiche multiple

Per offrire agli inquilini diverse opzioni di qualità del servizio, è possibile avere più di una polizza attiva contemporaneamente. Ogni policy può gestire tenant, bucket S3 e oggetti specifici. Quando si applica o si modifica una policy per un set specifico di tenant o oggetti, le policy applicate ad altri tenant e oggetti non vengono modificate.

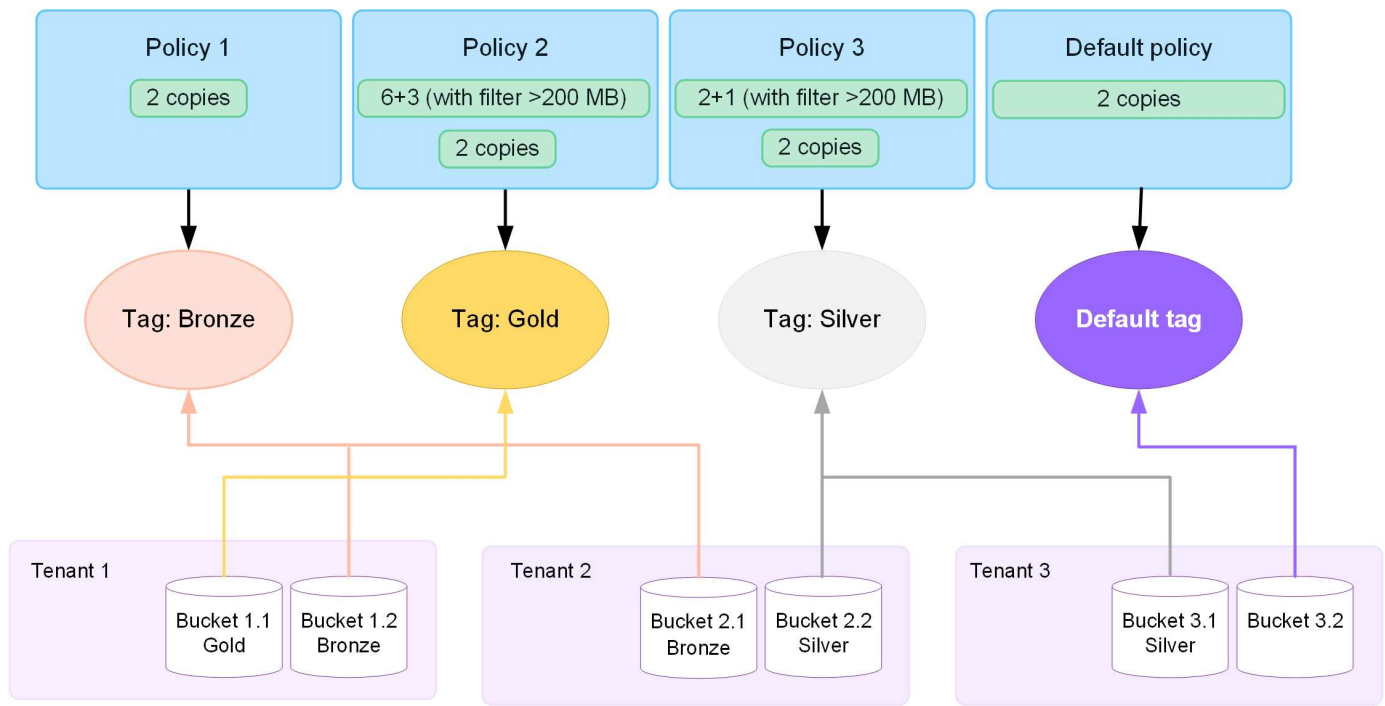
Tag di policy ILM

Se si desidera consentire ai tenant di passare facilmente da una policy di protezione dei dati all'altra per ogni bucket, utilizzare più policy ILM con *tag policy ILM*. Si assegna ogni policy ILM a un tag, quindi i tenant taggano un bucket per applicare la policy a quel bucket. È possibile impostare i tag dei criteri ILM solo sui bucket S3.

Ad esempio, potresti avere tre tag denominati Oro, Argento e Bronzo. È possibile assegnare un criterio ILM a ciascun tag, in base alla durata e alla posizione in cui tale criterio archivia gli oggetti. Gli inquilini possono scegliere quale policy utilizzare etichettando i propri bucket. Un bucket contrassegnato come Gold è gestito dalla policy Gold e riceve il livello Gold di protezione dei dati e prestazioni.

Tag di policy ILM predefinito

Un tag di policy ILM predefinito viene creato automaticamente quando si installa StorageGRID. Ogni griglia deve avere una policy attiva assegnata al tag Default. Il criterio predefinito si applica a tutti i bucket S3 non taggati.



In che modo una policy ILM valuta gli oggetti?

Una policy ILM attiva controlla il posizionamento, la durata e la protezione dei dati degli oggetti.

Quando i client salvano oggetti in StorageGRID, gli oggetti vengono valutati in base al set ordinato di regole ILM nella policy, come segue:

1. Se i filtri per la prima regola nel criterio corrispondono a un oggetto, l'oggetto viene acquisito in base al comportamento di acquisizione di quella regola e archiviato in base alle istruzioni di posizionamento di quella regola.
2. Se i filtri per la prima regola non corrispondono all'oggetto, l'oggetto viene valutato rispetto a ogni regola successiva nel criterio finché non viene trovata una corrispondenza.
3. Se nessuna regola corrisponde a un oggetto, vengono applicate le istruzioni di posizionamento e comportamento di acquisizione per la regola predefinita nel criterio. La regola predefinita è l'ultima regola di una policy. La regola predefinita deve essere applicata a tutti i tenant, a tutti i bucket S3 e a tutte le versioni degli oggetti e non può utilizzare filtri avanzati.

Esempio di politica ILM

Ad esempio, una policy ILM potrebbe contenere tre regole ILM che specificano quanto segue:

- **Regola 1: Copie replicate per l'inquilino A**

- Abbina tutti gli oggetti appartenenti all'inquilino A.
- Conservare questi oggetti in tre copie replicate in tre siti.
- Gli oggetti appartenenti ad altri tenant non sono soggetti alla Regola 1, pertanto vengono valutati in base alla Regola 2.

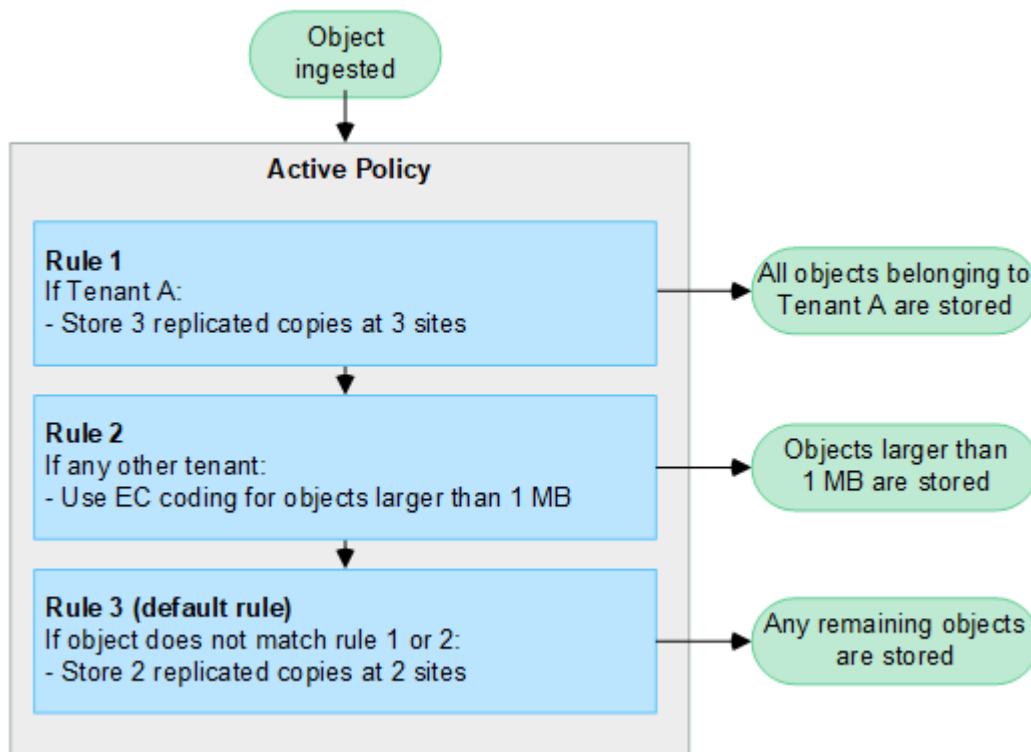
- **Regola 2: Codifica di cancellazione per oggetti di dimensioni superiori a 1 MB**

- Corrisponde a tutti gli oggetti degli altri tenant, ma solo se sono maggiori di 1 MB. Questi oggetti di grandi dimensioni 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** (predefinita)

- È l'ultima regola predefinita della policy. Non utilizza filtri.
- Eseguire 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 le politiche attive e inattive?

Ogni sistema StorageGRID deve avere almeno una policy ILM attiva. Se si desidera avere più di un criterio ILM attivo, è possibile creare tag di 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 a cui non è assegnato un tag di criterio.

Quando si crea per la prima volta un criterio ILM, si selezionano una o più regole ILM e le si dispone in un ordine specifico. Dopo aver simulato la policy per confermarne il comportamento, attivarla.

Quando si attiva un criterio ILM, StorageGRID utilizza tale criterio per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Gli oggetti esistenti potrebbero essere spostati in nuove posizioni quando verranno implementate le regole ILM nella nuova policy.

Se si attivano più policy ILM contemporaneamente e i tenant applicano tag policy ai bucket S3, gli oggetti in ciascun 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 una politica ILM

- Nei sistemi di test utilizzare solo la policy fornita dal sistema, ovvero la policy delle copie Baseline 2. Per StorageGRID 11.6 e versioni precedenti, la regola Crea 2 copie in questo criterio utilizza il pool di archiviazione Tutti i nodi di archiviazione, che contiene tutti i siti. Se il sistema StorageGRID ha più di un sito, è possibile che due copie di un oggetto siano posizionate sullo stesso sito.



Il pool di archiviazione All Storage Nodes 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 All Storage Nodes continuerà a esistere. Se si installa StorageGRID 11.7 o versione successiva come nuova installazione, il pool. Tutti i nodi di archiviazione non viene creato.

- Quando si progetta una nuova policy, bisogna considerare tutti i diversi tipi di oggetti che potrebbero essere inseriti nella griglia. Assicurarsi che la policy includa regole per abbinare e posizionare questi oggetti come richiesto.
- Mantenere la politica 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 .
- Assicuratevi che le regole della policy siano nell'ordine corretto. Quando la policy viene attivata, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'alto. Ad esempio, se la prima regola di un criterio corrisponde a un oggetto, tale oggetto non verrà valutato da nessun'altra regola.
- L'ultima regola in ogni policy ILM è la regola ILM predefinita, che non può utilizzare alcun filtro. Se un oggetto non è stato abbinato a un'altra regola, la regola predefinita controlla dove viene posizionato l'oggetto e per quanto tempo viene conservato.
- Prima di attivare una nuova policy, esaminare tutte le modifiche apportate dalla policy al posizionamento degli oggetti esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Creare policy ILM

Crea una o più policy ILM per soddisfare i tuoi requisiti di qualità del servizio.

Avere un criterio ILM attivo consente di applicare le stesse regole ILM a tutti i tenant e bucket.

Disporre di più policy ILM attive consente di applicare le regole ILM appropriate a tenant e bucket specifici per soddisfare più requisiti di qualità del servizio.

Creare una policy ILM

Informazioni su questo compito

Prima di creare la tua politica, verifica che ["politica ILM predefinita"](#) non soddisfa i tuoi requisiti di archiviazione.



Nei sistemi di test, utilizzare solo le policy fornite dal sistema, ovvero 2 copie della policy (per griglie a un sito) o 1 copia per sito (per griglie a più siti). Per StorageGRID 11.6 e versioni precedenti, la regola predefinita in questo criterio utilizza il pool di archiviazione All Storage Nodes, che contiene tutti i siti. Se il sistema StorageGRID ha più di un sito, è possibile che due copie di un oggetto siano posizionate sullo stesso sito.



Se il ["l'impostazione globale S3 Object Lock è stata abilitata"](#) , è necessario assicurarsi che la policy ILM sia conforme ai requisiti dei bucket in cui è abilitato S3 Object Lock. In questa sezione, seguire le istruzioni che indicano di aver abilitato S3 Object Lock.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["autorizzazioni di accesso richieste"](#) .

- Hai ["regole ILM create"](#) in base all'abilitazione o meno del blocco oggetti S3.

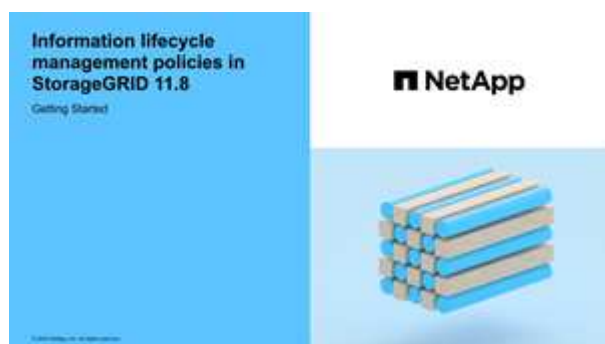
Blocco oggetto S3 non abilitato

- Hai ["ha creato le regole ILM"](#) che vuoi aggiungere alla polizza. Se necessario, è possibile salvare una policy, creare regole aggiuntive e quindi modificare la policy per aggiungere le nuove regole.
- Hai ["ha creato una regola ILM predefinita"](#) che non contiene alcun filtro.

Blocco oggetto S3 abilitato

- IL ["l'impostazione globale di blocco degli oggetti S3 è già abilitata"](#) per il sistema StorageGRID .
- Hai ["ha creato le regole ILM conformi e non conformi"](#) che vuoi aggiungere alla polizza. Se necessario, è possibile salvare una policy, creare regole aggiuntive e quindi modificare la policy per aggiungere le nuove regole.
- Hai ["ha creato una regola ILM predefinita"](#) per la politica conforme.

- Facoltativamente, hai guardato il video: ["Video: Panoramica delle politiche ILM"](#)



Vedere anche ["Utilizzare le policy ILM"](#) .

Passi

1. Selezionare **ILM > Criteri**.

Se l'impostazione globale Blocco oggetti S3 è abilitata, la pagina Criteri ILM indica quali regole ILM sono conformi.

2. Determina come desideri creare la policy ILM.

Crea una nuova politica

- a. Selezionare **Crea policy**.

Clona la politica esistente

- a. Seleziona la casella di controllo relativa al criterio da cui vuoi iniziare, quindi seleziona **Clona**.

Modifica la policy esistente

- a. Se una policy è inattiva, puoi modificarla. Seleziona la casella di controllo per il criterio inattivo da cui vuoi iniziare, quindi seleziona **Modifica**.

3. Nel campo **Nome policy**, immettere un nome univoco per la policy.

4. Facoltativamente, nel campo **Motivo della modifica**, inserisci il motivo per cui stai creando una nuova policy.
5. Per aggiungere regole al criterio, selezionare **Seleziona regole**. Selezionare il nome di una regola per visualizzarne le impostazioni.

Se stai clonando una policy:

- Vengono selezionate le regole utilizzate dalla policy che stai clonando.
- Se il criterio che stai clonando utilizzava regole senza filtri che non erano la regola predefinita, ti verrà chiesto di rimuovere tutte le regole tranne una.
- Se la regola predefinita utilizza un filtro, ti verrà chiesto di selezionare una nuova regola predefinita.
- Se la regola predefinita non era l'ultima regola, è possibile spostarla alla fine del nuovo criterio.

Blocco oggetto S3 non abilitato

- a. Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, seleziona **Pagina regole ILM**.

La regola predefinita si applica a tutti gli oggetti che non corrispondono a un'altra regola nel criterio. La regola predefinita non può utilizzare alcun filtro e viene sempre valutata per ultima.



Non utilizzare la regola Crea 2 copie come regola predefinita per una policy. La regola Crea 2 copie utilizza un singolo pool di archiviazione, Tutti i nodi di archiviazione, che contiene tutti i siti. Se il sistema StorageGRID ha più di un sito, è possibile che due copie di un oggetto siano posizionate sullo stesso sito.

Blocco oggetto S3 abilitato

- a. Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, seleziona **Pagina regole ILM**.

L'elenco delle regole contiene solo le regole conformi e non utilizzano alcun filtro.



Non utilizzare la regola Crea 2 copie come regola predefinita per una policy. La regola Crea 2 copie utilizza un singolo pool di archiviazione, Tutti i nodi di archiviazione, che contiene tutti i siti. Se si utilizza questa regola, è possibile che più copie di un oggetto vengano posizionate nello stesso sito.

- 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 utilizzi un filtro.

Ad esempio, potresti voler utilizzare un Cloud Storage Pool per archiviare oggetti in bucket in cui non è abilitato il blocco degli oggetti S3.



È possibile selezionare solo una regola non conforme che non utilizzi un filtro.

Vedere anche ["Esempio 7: Politica ILM conforme per S3 Object Lock"](#).

6. Dopo aver selezionato la regola predefinita, seleziona **Continua**.

7. Per il passaggio Altre regole, seleziona tutte le altre regole che desideri aggiungere al criterio. Queste regole utilizzano almeno un filtro (account tenant, nome bucket, filtro avanzato o ora di riferimento non corrente). Quindi seleziona **Seleziona**.

Nella finestra Crea un criterio sono ora elencate le regole selezionate. La regola predefinita è alla fine, mentre le altre regole sono sopra.

Se è abilitato il blocco degli oggetti S3 e si è selezionata anche una regola "predefinita" non conforme, tale regola viene aggiunta come penultima regola nel criterio.



Se una regola non conserva gli oggetti per sempre, viene visualizzato un avviso. Quando si attiva questo criterio, è necessario confermare che si desidera che StorageGRID elimini gli oggetti quando scadono le istruzioni di posizionamento per la regola predefinita (a meno che un ciclo di vita del bucket non conservi gli oggetti per un periodo di tempo più lungo).

8. Trascinare le righe delle regole non predefinite per determinare l'ordine in cui tali regole verranno valutate.

Non è possibile spostare la regola predefinita. Se è abilitato il Blocco oggetto S3, non è possibile spostare la regola "predefinita" non conforme, se ne è stata selezionata una.



È necessario confermare che le regole ILM siano nell'ordine corretto. Quando la policy viene attivata, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'alto.

9. Se necessario, selezionare **Seleziona regole** per aggiungere o rimuovere regole.
10. Al termine, seleziona **Salva**.
11. Ripetere questi passaggi per creare ulteriori policy ILM.
12. [Simulare una politica ILM](#) . Dovresti sempre simulare una policy prima di attivarla per assicurarti che funzioni come previsto.

Simulare una politica

Simulare una policy sugli oggetti di prova prima di attivarla e applicarla ai dati di produzione.

Prima di iniziare

- Conosci il bucket S3/chiave oggetto per ogni oggetto che vuoi testare.

Passi

1. Utilizzando un client S3 o "[Console S3](#)" , ingerire gli oggetti necessari per testare ciascuna regola.
2. Nella pagina Criteri ILM, seleziona la casella di controllo per il criterio, quindi seleziona **Simula**.
3. Nel campo **Oggetto**, immettere S3 bucket/object-key per un oggetto di prova. Ad esempio, bucket-01/filename.png .
4. Se è abilitato il controllo delle versioni S3, è possibile immettere facoltativamente un ID versione per l'oggetto nel campo **ID versione**.
5. Selezionare **Simula**.
6. Nella sezione Risultati della simulazione, verificare che a ciascun oggetto sia stata applicata la regola corretta.
7. Per determinare quale pool di archiviazione o profilo di codifica di cancellazione è attivo, selezionare il nome della regola corrispondente per accedere alla pagina dei dettagli della regola.



Esaminare eventuali modifiche al posizionamento degli oggetti replicati e codificati con cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Risultati

Eventuali modifiche alle regole della policy verranno riflesse nei risultati della simulazione e mostreranno la nuova corrispondenza e quella precedente. La finestra Criterio di simulazione conserva gli oggetti testati finché non selezioni **Cancella tutto** o l'icona di rimozione  per ogni oggetto nell'elenco dei risultati della simulazione.

Informazioni correlate

["Esempio di simulazioni di policy ILM"](#)

Attiva una politica

Quando si attiva una nuova policy ILM, gli oggetti esistenti e quelli appena acquisiti vengono gestiti da tale policy. Quando si attivano più policy, i tag delle policy ILM assegnati ai bucket determinano gli oggetti da gestire.

Prima di attivare una nuova polizza:

1. Simula la policy per verificare che si comporti come previsto.
2. Esaminare eventuali modifiche al posizionamento degli oggetti replicati e codificati con cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.



Gli errori in una policy ILM possono causare una perdita di dati irrecuperabile.

Informazioni su questo compito

Quando si attiva una policy ILM, il sistema distribuisce la nuova policy a tutti i nodi. Tuttavia, la nuova policy attiva potrebbe non avere effetto finché tutti i nodi della griglia non saranno disponibili a riceverla. In alcuni casi, il sistema attende di implementare una nuova policy attiva per garantire che gli oggetti della griglia non vengano rimossi accidentalmente. Nello specifico:

- Se si apportano modifiche ai criteri che **aumentano la ridondanza o la durabilità dei dati**, tali modifiche vengono implementate immediatamente. Ad esempio, se si attiva una nuova policy che include una regola a tre copie anziché a due copie, tale policy verrà implementata immediatamente perché aumenta la ridondanza dei dati.
- Se si apportano modifiche ai criteri che **potrebbero ridurre la ridondanza o la durabilità dei dati**, tali modifiche non verranno implementate finché tutti i nodi della griglia non saranno disponibili. Ad esempio, se si attiva una nuova policy che utilizza una regola a due copie anziché una regola a tre copie, la nuova policy verrà visualizzata nella scheda Policy attiva, ma non avrà effetto finché tutti i nodi non saranno online e disponibili.

Passi

Seguire i passaggi per attivare una o più policy:

Attiva una politica

Se si desidera avere una sola polizza attiva, seguire questi passaggi. Se hai già una o più policy attive e stai attivando policy aggiuntive, segui i passaggi per l'attivazione di più policy.

1. Quando sei pronto ad attivare una policy, seleziona **ILM > Policy**.

In alternativa, è possibile attivare una singola policy dalla pagina **ILM > Tag policy**.

2. Nella scheda Criteri, seleziona la casella di controllo per il criterio che desideri attivare, quindi seleziona **Attiva**.
3. Seguire il passaggio appropriato:
 - Se un messaggio di avviso richiede di confermare l'attivazione del criterio, selezionare **OK**.
 - Se viene visualizzato un messaggio di avviso contenente dettagli sulla policy:
 - i. Esaminare i dettagli per assicurarsi che la policy gestisca i dati come previsto.
 - ii. Se la regola predefinita memorizza gli oggetti per un numero limitato di giorni, rivedere il diagramma di conservazione e digitare tale 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 **sì** nella casella di testo.
 - iv. Seleziona **Attiva policy**.

Attiva più policy

Per attivare più policy, è necessario creare dei tag e assegnare una policy a ciascun tag.



Quando vengono utilizzati più tag, se i tenant riassegnano frequentemente i tag dei criteri ai bucket, le prestazioni della griglia potrebbero risentirne. Se hai tenant non attendibili, valuta la possibilità di utilizzare solo il tag Default.

1. Selezionare **ILM > Tag policy**.
2. Seleziona **Crea**.
3. Nella finestra di dialogo Crea tag criterio, digitare un nome per il tag e, facoltativamente, una descrizione per il tag.



I nomi e le descrizioni dei tag sono visibili agli inquilini. 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 la policy assegnata eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni sensibili in questi campi.

4. Seleziona **Crea tag**.
5. Nella tabella dei tag dei criteri ILM, utilizzare il menu a discesa per selezionare un criterio da assegnare al tag.
6. Se nella colonna Limitazioni della policy vengono visualizzati degli avvisi, selezionare **Visualizza dettagli policy** per rivedere la policy.
7. Assicurarsi che ogni policy gestisca i dati come previsto.
8. Selezionare **Attiva policy assegnate**. Oppure seleziona **Cancella modifiche** per rimuovere l'assegnazione del criterio.

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 i criteri gestiscano gli oggetti come previsto.
10. Quando sei sicuro di voler attivare i criteri, digita **si** nella casella di testo, quindi seleziona **Attiva criteri**.

Informazioni correlate

["Esempio 6: Modifica di una policy ILM"](#)

Esempio di simulazioni di policy ILM

Gli esempi di simulazioni di policy ILM forniscono linee guida per strutturare e modificare le simulazioni per il tuo ambiente.

Esempio 1: verificare le regole durante la simulazione di una policy ILM

Questo esempio descrive come verificare le regole durante la simulazione di una policy.

In questo esempio, la **politica ILM di esempio** viene simulata sugli oggetti acquisiti in due bucket. La politica comprende tre regole, come segue:

- La prima regola, **Due copie, due anni per il bucket-a**, si applica solo agli oggetti nel bucket-a.
- La seconda regola, **Oggetti EC > 1 MB**, si applica a tutti i bucket ma filtra gli oggetti di dimensioni superiori a 1 MB.
- La terza regola, **Due copie, due data center**, è la regola predefinita. Non include alcun filtro e non utilizza il tempo di riferimento non corrente.

Dopo aver simulato la policy, verificare che a ciascun oggetto corrisponda la regola corretta.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
<button>Clear all</button> 				
Object 	Version ID 	Rule matched  	Previous match  	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	

In questo esempio:

- bucket-a/bucket-a object.pdf`ha abbinato correttamente la prima regola, che filtra gli oggetti in `bucket-a`.
- bucket-b/test object greater than 1 MB.pdf`è dentro `bucket-b`, quindi non corrispondeva alla prima regola. Invece, è stato correttamente abbinato dalla seconda regola, che filtra gli oggetti di dimensioni superiori a 1 MB.

- `bucket-b/test object less than 1 MB.pdf` non corrisponde ai filtri nelle prime due regole, quindi verrà inserito dalla regola predefinita, che non include filtri.

Esempio 2: riordinare le regole durante la simulazione di una policy ILM

Questo esempio mostra come è possibile riordinare le regole per modificare i risultati durante la simulazione di una policy.

In questo esempio viene simulata la policy **Demo**. Questa politica, che ha lo scopo di trovare oggetti che hanno metadati utente `series=x-men`, include tre regole, come segue:

- La prima regola, **PNG**, filtra i nomi delle chiavi che terminano in `.png`.
- La seconda regola, **X-men**, si applica solo agli oggetti per l'inquilino 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.

Passi

1. Dopo aver aggiunto le regole e salvato il criterio, seleziona **Simula**.
2. Nel campo **Oggetto**, immettere il bucket S3/chiave oggetto per un oggetto di prova e selezionare **Simula**.

Vengono visualizzati i risultati della simulazione, che mostrano che `Havok.png` l'oggetto è stato abbinato dalla regola **PNG**.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

Tuttavia, `Havok.png` aveva lo scopo di testare la regola degli **X-men**.

3. Per risolvere il problema, riordina le regole.
 - a. Selezionare **Fine** per chiudere la finestra Simula criterio ILM.
 - b. Selezionare **Modifica** per modificare la policy.
 - c. Trascina la regola **X-men** in cima all'elenco.
 - d. Seleziona **Salva**.
4. Selezionare **Simula**.

Gli oggetti precedentemente testati vengono rivalutati in base alla policy aggiornata e vengono mostrati i nuovi risultati della simulazione. Nell'esempio, la colonna Regola corrispondente mostra che `Havok.png` l'oggetto ora corrisponde alla regola dei metadati degli X-men, come previsto. La colonna Corrispondenza precedente mostra che la regola PNG corrispondeva all'oggetto nella simulazione precedente.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	X

Esempio 3: correggere una regola durante la simulazione di una policy 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**. Questa politica ha lo scopo di trovare oggetti che hanno `series=x-men` metadati dell'utente. Tuttavia, si sono verificati risultati inaspettati quando si è simulata questa politica contro il `Beast.jpg` oggetto. Invece di corrispondere alla regola dei metadati degli X-Men, l'oggetto corrispondeva alla regola predefinita: due copie di due data center.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	X

Quando un oggetto di prova non corrisponde alla regola prevista nel criterio, è necessario esaminare ogni regola nel criterio e correggere eventuali errori.

Passi

1. Selezionare **Fine** per chiudere la finestra di dialogo Simula criterio. Nella pagina dei dettagli della policy, seleziona **Diagramma di conservazione**. Quindi seleziona **Espandi tutto** o **Visualizza dettagli** per ogni regola, a seconda delle necessità.
2. Esaminare l'account tenant della regola, l'ora di riferimento e i criteri di filtraggio.

Ad esempio, supponiamo che i metadati per la regola X-men siano stati inseriti come "x-men01" anziché "x-men".

3. Per risolvere l'errore, correggere la regola come segue:
 - Se la regola fa parte della policy, puoi clonarla o rimuoverla dalla policy e poi modificarla.
 - Se la regola fa parte della policy attiva, 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 degli X-men ora corrisponde a `Beast.jpg` oggetto basato su `series=x-men` metadati dell'utente, come previsto.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	X-men	—	X

Gestisci 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"](#).
- Tu hai il ["autorizzazioni di accesso richieste"](#).

Visualizza i dettagli del tag della policy ILM

Per visualizzare i dettagli di un tag:

1. Selezionare **ILM > Tag policy**.
2. Selezionare il nome della policy dalla tabella. Viene visualizzata la pagina dei dettagli del tag.
3. Nella pagina dei dettagli, visualizza la cronologia precedente delle policy assegnate.
4. Visualizza una policy selezionandola.

Modifica tag policy ILM



I nomi e le descrizioni dei tag sono visibili agli inquilini. 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 la policy assegnata eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni sensibili in questi campi.

Per modificare la descrizione di un tag esistente:

1. Selezionare **ILM > Tag policy**.
2. Seleziona la casella di controllo per il tag, quindi seleziona **Modifica**.

In alternativa, seleziona il nome del tag. Viene visualizzata la pagina dei dettagli del tag, in cui puoi selezionare **Modifica**.

3. Modificare la descrizione del tag secondo necessità
4. Seleziona **Salva**.

Rimuovi il tag della policy ILM

Quando si rimuove un tag di policy, a tutti i bucket a cui è assegnato quel tag verrà applicata la policy predefinita.

Per rimuovere un tag:

1. Selezionare **ILM > Tag policy**.
2. Seleziona la casella di controllo per il tag, quindi seleziona **Rimuovi**. Viene visualizzata una finestra di dialogo di conferma.

In alternativa, seleziona il nome del tag. Viene visualizzata la pagina dei dettagli del tag, in cui puoi selezionare **Rimuovi**.

3. Selezionare **Sì** per eliminare il tag.

Verifica una policy ILM con la ricerca dei metadati degli oggetti

Dopo aver attivato un criterio ILM, importare oggetti di prova rappresentativi nel sistema StorageGRID , quindi eseguire una ricerca dei metadati degli oggetti per confermare che le copie vengano eseguite come previsto e posizionate nelle posizioni corrette.

Prima di iniziare

Hai un identificatore di oggetto, che può essere uno dei seguenti: * **UUID**: l'identificatore univoco universale dell'oggetto. * **CBID**: Identificatore univoco dell'oggetto all'interno StorageGRID. È possibile ottenere il CBID di un oggetto dal registro di controllo. Inserire il CBID in maiuscolo. * **Chiave oggetto e bucket S3**: quando un oggetto viene acquisito tramite l'interfaccia S3, l'applicazione client utilizza una combinazione di chiave oggetto e bucket per archiviare e identificare l'oggetto. Se il bucket S3 è sottoposto a controllo di versione e si desidera cercare una versione specifica di un oggetto S3 utilizzando il bucket e la chiave dell'oggetto, si ottiene l'**ID versione**.

Passi

1. Ingerire l'oggetto.
2. Selezionare **ILM > Ricerca metadati oggetto**.
3. Digitare l'identificatore dell'oggetto nel campo **Identificatore**. È possibile immettere un UUID, un CBID o un bucket/chave oggetto S3.
4. Facoltativamente, immettere un ID versione per l'oggetto (solo S3).
5. Seleziona **Cerca**.

Vengono visualizzati i risultati della ricerca dei metadati dell'oggetto. In questa pagina sono elencati i seguenti tipi di informazioni:

- Metadati di sistema, come ID oggetto (UUID), tipo di risultato (oggetto, marcatore di eliminazione, bucket S3) e dimensione logica dell'oggetto. Per maggiori dettagli, fare riferimento allo screenshot di esempio riportato di seguito.
- Qualsiasi coppia chiave-valore di metadati utente personalizzati associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore del tag oggetto associata all'oggetto.
- Per le copie di oggetti replicati, la posizione di archiviazione corrente di ciascuna copia.
- Per le copie di oggetti con codice di cancellazione, la posizione di archiviazione 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 oggetti multiparte, un elenco di segmenti di oggetti, inclusi gli identificatori di

segmento e le dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono mostrati solo i primi 100 segmenti.

- Tutti i metadati degli oggetti nel formato di archiviazione interna non elaborato. Questi metadati grezzi includono metadati di sistema interni la cui persistenza da una versione all'altra non è garantita.

6. Verificare che l'oggetto sia archiviato nella posizione o nelle posizioni corrette e che si tratti del tipo di copia corretto.

Se l'opzione Audit è abilitata, è anche possibile monitorare il registro di audit per il messaggio ORLM Object Rules Met. Il messaggio di controllo ORLM può fornire maggiori 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. Devi valutarlo tu stesso. Per maggiori dettagli, vedere ["Esaminare i registri di controllo"](#).

L'esempio seguente mostra i risultati della ricerca dei metadati dell'oggetto per un oggetto di test S3 archiviato come due copie replicate.



La seguente schermata è un esempio. I risultati varieranno a seconda della versione StorageGRID.

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",

```

Informazioni correlate

["Utilizzare l'API REST S3"](#)

Lavorare con le policy e le regole ILM

Man mano che cambiano i requisiti di archiviazione, potrebbe essere necessario implementare policy aggiuntive o modificare le regole ILM associate a una policy. È possibile visualizzare le metriche ILM per determinare le prestazioni del sistema.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Visualizza le policy ILM

Per visualizzare le policy ILM attive e inattive e la cronologia delle attivazioni delle policy:

1. Selezionare **ILM > Criteri**.
2. Selezionare **Criteri** per visualizzare un elenco dei criteri attivi e inattivi. Nella tabella sono elencati il nome di ciascun criterio, i tag a cui è assegnato e se il criterio è attivo o inattivo.
3. Selezionare **Cronologia attivazioni** per visualizzare un elenco delle date di inizio e fine dell'attivazione delle polizze.
4. Selezionare il nome di una policy per visualizzarne i dettagli.



Se si visualizzano i dettagli di una policy il cui stato è Modificato o Eliminato, viene visualizzato un messaggio che spiega che si sta visualizzando la versione della policy che era attiva per l'intervallo di tempo specificato e che da allora è stata modificata o eliminata.

Modifica una policy ILM

È possibile modificare solo una policy inattiva. Se si desidera modificare una policy attiva, è possibile disattivarla oppure creare un clone e modificarlo.

Per modificare una policy:

1. Selezionare **ILM > Criteri**.
2. Seleziona la casella di controllo relativa alla policy che desideri modificare, quindi seleziona **Modifica**.
3. Modifica la policy seguendo le istruzioni in "[Creare policy ILM](#)".
4. Simulare la policy prima di riattivarla.



Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Clonare una policy ILM

Per clonare una policy ILM:

1. Selezionare **ILM > Criteri**.
2. Seleziona la casella di controllo relativa alla policy che desideri clonare, quindi seleziona **Clona**.
3. Crea una nuova policy partendo dalla policy che hai clonato seguendo le istruzioni in "[Creare policy ILM](#)".



Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Rimuovere una policy ILM

È possibile rimuovere un criterio ILM solo se è inattivo. Per rimuovere una policy:

1. Selezionare **ILM > Criteri**.
2. Seleziona la casella di controllo relativa al criterio inattivo che desideri rimuovere.
3. Seleziona **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 per la regola:

1. Selezionare **ILM > Regole**.
2. Seleziona il nome della regola di cui vuoi visualizzare i dettagli. Esempio:

2 copies 2 data centers

Compliant: No
Ingest behavior: Strict
Reference time: Noncurrent time

[Clone](#) [Edit](#) [Remove](#)

[Rule detail](#) [Used in policies](#)

Time period and placements

[Retention diagram](#) [Placement instructions](#)

Sort placements by [Time period](#) [Storage pool](#) ● Replicated copy ● Erasure-coded (EC) copy

Rule analysis:

- Objects processed by this rule will not be deleted by ILM.

Reference time: Noncurrent time Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Data Center 1

EC 2+1 - Data Center 1

Duration Forever

Inoltre, puoi utilizzare la pagina dei dettagli per clonare, modificare o rimuovere una regola. Non è possibile modificare o rimuovere una regola se è utilizzata in una policy.

Clona 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 una policy, è sufficiente clonare la regola e apportare le modifiche al clone. Dopo aver apportato 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.

Passi

1. Selezionare **ILM > Regole**.
2. Seleziona la casella di controllo relativa alla regola che desideri clonare, quindi seleziona **Clona**. In alternativa, seleziona il nome della regola, quindi seleziona **Clona** dalla pagina dei dettagli della regola.
3. Aggiorna la regola clonata seguendo i passaggi per [modifica di una regola ILM E"utilizzo di filtri avanzati nelle regole ILM"](#).

Quando si clona una regola ILM, è necessario immettere un nuovo nome.

Modifica una regola ILM

Potrebbe essere necessario modificare una regola ILM per cambiare un filtro o un'istruzione di posizionamento.

Non è possibile modificare una regola se è utilizzata in una policy ILM. Invece, puoi [clonare la regola](#) e apportare tutte le modifiche necessarie alla copia clonata.



Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Passi

1. Selezionare **ILM > Regole**.
2. Verificare che la regola che si desidera modificare non sia utilizzata in alcuna policy ILM.
3. Se la regola che vuoi modificare non è in uso, seleziona la casella di controllo per la regola e seleziona **Azioni > Modifica**. In alternativa, seleziona il nome della regola, quindi seleziona **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 probabilmente non utilizzerai.

Passi

Per rimuovere una regola ILM attualmente utilizzata in un criterio attivo:

1. Clonare la policy.
2. Rimuovere la regola ILM dal clone della policy.
3. Salvare, simulare e attivare la nuova policy per assicurarsi che gli oggetti siano protetti come previsto.
4. Vai ai passaggi per rimuovere una regola ILM attualmente utilizzata in un criterio inattivo.

Per rimuovere una regola ILM attualmente utilizzata in un criterio inattivo:

1. Selezionare la policy inattiva.
2. Rimuovere la regola ILM dalla policy [rimuovere la politica](#).
3. Vai ai passaggi per rimuovere una regola ILM attualmente non utilizzata.

Per rimuovere una regola ILM attualmente non utilizzata:

1. Selezionare **ILM > Regole**.
2. Verificare che la regola che si desidera rimuovere non sia utilizzata in alcun criterio.

3. Se la regola che vuoi rimuovere non è in uso, selezionala e seleziona **Azioni > Rimuovi**. È possibile selezionare più regole e rimuoverle tutte contemporaneamente.
4. Selezionare **Sì** per confermare che si desidera rimuovere la regola ILM.

Visualizza le metriche ILM

È possibile visualizzare le metriche per ILM, come il numero di oggetti nella coda e la frequenza di valutazione. È possibile monitorare queste metriche per determinare le prestazioni del sistema. Una coda o una frequenza di valutazione elevate potrebbero indicare che il sistema non è in grado di tenere il passo con la frequenza di acquisizione, che il carico delle applicazioni client è eccessivo o che si è verificata una condizione anomala.

Passi

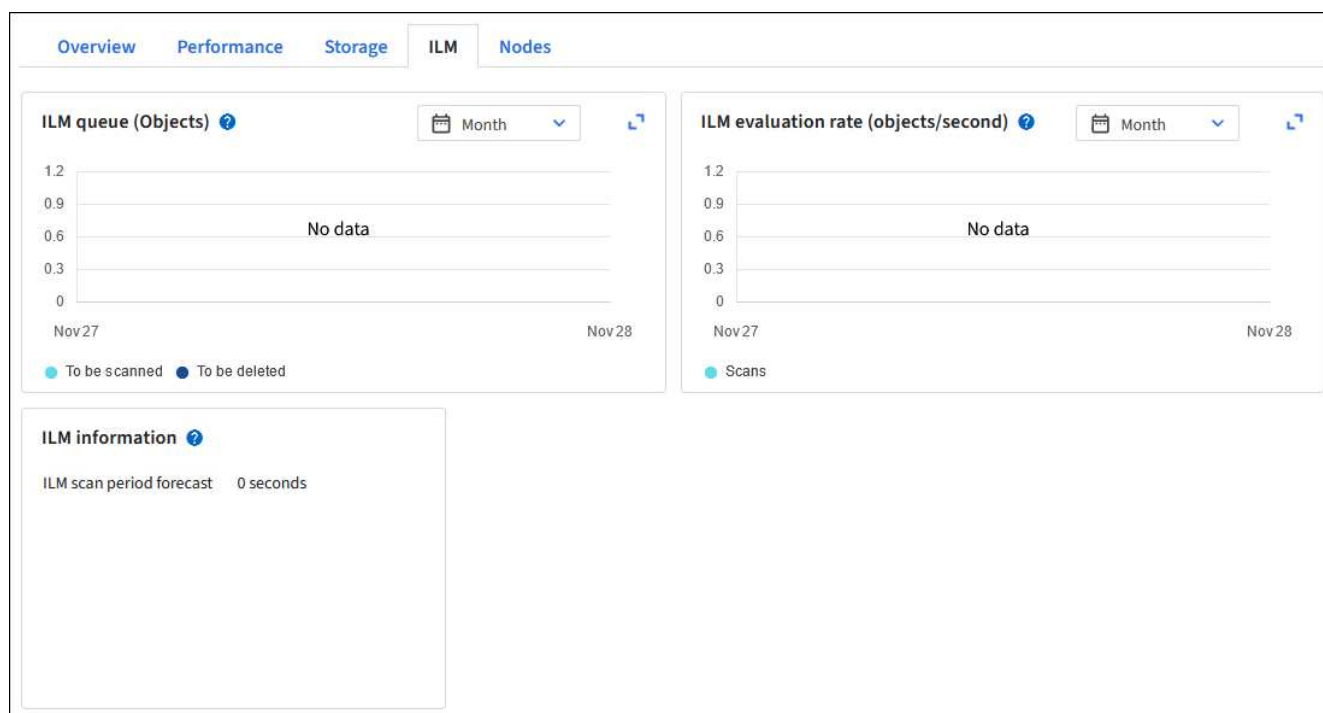
1. Selezionare **Dashboard > ILM**.



Poiché la dashboard può essere personalizzata, la scheda ILM potrebbe non essere disponibile.

2. Monitorare le metriche nella scheda ILM.

Puoi selezionare il punto interrogativo per visualizzare una descrizione degli elementi nella scheda ILM.



Utilizzare il blocco oggetto S3

Gestisci gli oggetti con S3 Object Lock

In qualità di amministratore della griglia, puoi abilitare S3 Object Lock per il tuo sistema StorageGRID e implementare una policy ILM conforme per garantire che gli oggetti in bucket S3 specifici non vengano eliminati o sovrascritti per un periodo di tempo specificato.

Che cos'è S3 Object Lock?

La funzionalità StorageGRID S3 Object Lock è una soluzione di protezione degli oggetti equivalente a S3 Object Lock in Amazon Simple Storage Service (Amazon S3).

Quando l'impostazione globale S3 Object Lock è abilitata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se in un bucket è abilitato S3 Object Lock, è necessario il controllo delle versioni del bucket, che viene abilitato automaticamente.

Un bucket senza S3 Object Lock può contenere solo oggetti per i quali non sono specificate impostazioni di conservazione. Nessun oggetto ingerito avrà impostazioni di conservazione.

Un bucket con S3 Object Lock può contenere oggetti con e senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con S3 Object Lock e conservazione predefinita configurata può contenere oggetti caricati con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, perché l'impostazione di conservazione non è stata configurata a livello di oggetto.

Di fatto, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurata la conservazione predefinita. Gli oggetti esistenti senza impostazioni di conservazione degli oggetti rimangono inalterati.

Modalità di conservazione

La funzionalità StorageGRID S3 Object Lock supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità sono equivalenti alle modalità di conservazione di Amazon S3.

- In modalità conformità:
 - L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione.
 - La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.
 - La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.
- In modalità di governance:
 - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare determinate impostazioni di conservazione.
 - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione.
 - Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.

Impostazioni di conservazione per le versioni degli oggetti

Se viene creato un bucket con S3 Object Lock abilitato, gli utenti possono utilizzare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ciascun oggetto aggiunto al bucket:

- **Modalità di conservazione:** conformità o governance.
- **Retain-until-date:** se la retain-until-date di una versione di un oggetto è futura, l'oggetto può essere recuperato, ma non eliminato.
- **Sospensione legale:** l'applicazione di una sospensione legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potrebbe essere necessario applicare un blocco legale a un oggetto correlato a un'indagine o a una controversia legale. Una sospensione legale non ha una data di

scadenza, ma rimane in vigore finché non viene rimossa esplicitamente. Le sospensioni legali sono indipendenti dalla data di conservazione fino alla data di scadenza.



Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

Per i dettagli sulle impostazioni dell'oggetto, vedere ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#).

Impostazione di conservazione predefinita per i bucket

Se viene creato un bucket con S3 Object Lock abilitato, gli utenti possono facoltativamente specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita:** conformità o governance.
- **Periodo di conservazione predefinito:** per quanto tempo devono essere conservate le nuove versioni degli oggetti aggiunte a questo bucket, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non dispongono di impostazioni di conservazione proprie. Gli oggetti bucket esistenti non vengono modificati quando si aggiungono o si modificano queste impostazioni predefinite.

Vedere ["Crea un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco degli oggetti S3"](#).

Confronto tra S3 Object Lock e la conformità legacy

S3 Object Lock sostituisce la funzionalità Compliance disponibile nelle versioni precedenti StorageGRID. Poiché la funzionalità S3 Object Lock è conforme ai requisiti di Amazon S3, essa rende obsoleta la funzionalità proprietaria StorageGRID Compliance, ora denominata "legacy Compliance".



L'impostazione Conformità globale è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione Blocco oggetto S3 viene abilitata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per i dettagli, vedere ["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"](#).

Se hai utilizzato la funzionalità Conformità legacy in una versione precedente di StorageGRID, fai riferimento alla tabella seguente per scoprire come si confronta con la funzionalità Blocco oggetti S3 in StorageGRID.

	Blocco oggetto S3	Conformità (legacy)
Come viene abilitata la funzionalità a livello globale?	Da Grid Manager, seleziona CONFIGURAZIONE > Sistema > Blocco oggetto S3 .	Non più supportato.
Come si abilita la funzionalità per un bucket?	Gli utenti devono abilitare S3 Object Lock quando creano un nuovo bucket utilizzando Tenant Manager, Tenant Management API o S3 REST API.	Non più supportato.

	Blocco oggetto S3	Conformità (legacy)
È supportato il controllo delle versioni dei bucket?	Sì. Il controllo delle versioni del bucket è obbligatorio e viene abilitato automaticamente quando S3 Object Lock è abilitato per il bucket.	NO.
Come viene impostata la conservazione degli oggetti?	Gli utenti possono impostare una data di conservazione per ogni versione dell'oggetto oppure possono impostare un periodo di conservazione predefinito per ogni 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 di conformità, la data di conservazione per una versione di un oggetto può essere aumentata ma mai diminuita. • In modalità di governance, gli utenti con autorizzazioni speciali possono ridurre o addirittura rimuovere le impostazioni di conservazione di un oggetto.	Il periodo di conservazione di un bucket può essere aumentato, ma mai diminuito.
Dove viene controllata la conservazione legale?	Gli utenti possono applicare o rimuovere una sospensione legale per qualsiasi versione dell'oggetto nel bucket.	Viene applicata una sospensione legale al bucket che interessa tutti gli oggetti al suo interno.
Quando è possibile eliminare gli oggetti?	• In modalità di conformità, una versione dell'oggetto può essere eliminata dopo aver raggiunto la data di conservazione, a condizione che l'oggetto non sia soggetto a conservazione legale. • In modalità di governance, gli utenti con autorizzazioni speciali possono eliminare un oggetto prima che venga raggiunta la data di conservazione, a condizione che l'oggetto non sia soggetto a conservazione legale.	Un oggetto può essere eliminato dopo la scadenza del periodo di conservazione, a condizione che il bucket non sia sottoposto a conservazione legale. Gli oggetti possono essere eliminati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	Sì	NO

Attività di blocco degli oggetti S3

In qualità di amministratore della griglia, devi coordinarti strettamente con gli utenti tenant per garantire che gli oggetti siano protetti in modo da soddisfare i loro requisiti di conservazione.



L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato del nodo e delle operazioni di Cassandra.

Gli elenchi seguenti per gli amministratori della griglia e gli utenti tenant contengono le attività di alto livello per l'utilizzo della funzionalità S3 Object Lock.

Amministratore di rete

- Abilita l'impostazione globale di blocco degli oggetti S3 per l'intero sistema StorageGRID .
- Garantire che le politiche di gestione del ciclo di vita delle informazioni (ILM) siano *conformi*; ovvero, che soddisfino i ["requisiti dei bucket con S3 Object Lock abilitato"](#) .
- Se necessario, consentire a un tenant di utilizzare Conformità come modalità di conservazione. In caso contrario, è consentita solo la modalità Governance.
- Se necessario, impostare un periodo massimo di conservazione per un tenant.

Utente inquilino

- Esaminare le considerazioni relative a bucket e oggetti con S3 Object Lock.
- Se necessario, contattare l'amministratore della griglia per abilitare l'impostazione globale di blocco degli oggetti S3 e impostare le autorizzazioni.
- Crea bucket con S3 Object Lock abilitato.
- Facoltativamente, configura le impostazioni di conservazione predefinite per un bucket:
 - Modalità di conservazione predefinita: Governance o Conformità, se consentita dall'amministratore della rete.
 - Periodo di conservazione predefinito: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall'amministratore della griglia.
- Utilizzare l'applicazione client S3 per aggiungere oggetti e, facoltativamente, impostare la conservazione specifica dell'oggetto:
 - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore della rete.
 - Conserva fino alla data: deve essere inferiore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.

Requisiti per S3 Object Lock

È necessario esaminare i requisiti per abilitare l'impostazione globale S3 Object Lock, i requisiti per creare regole ILM e policy ILM conformi e le restrizioni che StorageGRID impone ai bucket e agli oggetti che utilizzano S3 Object Lock.

Requisiti per l'utilizzo dell'impostazione globale S3 Object Lock

- È necessario abilitare l'impostazione globale S3 Object Lock tramite Grid Manager o Grid Management API prima che un tenant S3 possa creare un bucket con S3 Object Lock abilitato.
- Abilitando l'impostazione globale S3 Object Lock, tutti gli account tenant S3 potranno creare bucket con S3

Object Lock abilitato.

- Dopo aver abilitato l'impostazione globale Blocco oggetti S3, non è possibile disabilitarla.
- Non è possibile abilitare il blocco oggetti S3 globale a meno che la regola predefinita in tutti i criteri ILM attivi non sia *conforme* (ovvero, la regola predefinita deve essere conforme ai requisiti dei bucket con blocco oggetti S3 abilitato).
- Quando l'impostazione globale Blocco oggetti S3 è abilitata, non è possibile creare un nuovo criterio ILM o attivarne uno esistente, a meno che la regola predefinita nel criterio non sia conforme. Dopo aver abilitato l'impostazione globale S3 Object Lock, le pagine Regole ILM e Criteri ILM indicano quali regole ILM sono conformi.

Requisiti per le regole ILM conformi

Se si desidera abilitare l'impostazione globale S3 Object Lock, è necessario assicurarsi che la regola predefinita in tutti i criteri ILM attivi sia conforme. Una regola conforme soddisfa i requisiti di entrambi i bucket con S3 Object Lock abilitato e di tutti i bucket esistenti con la conformità legacy abilitata:

- Deve creare almeno due copie replicate dell'oggetto o una copia con codice di cancellazione.
- Queste copie devono essere presenti sui nodi di archiviazione per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
- Le copie degli oggetti non possono essere salvate in un Cloud Storage Pool.
- Almeno una riga delle istruzioni di posizionamento deve iniziare dal giorno 0, utilizzando **Ingest time** come orario di riferimento.
- Almeno una riga delle istruzioni di posizionamento deve essere "per sempre".

Requisiti per le politiche ILM

Quando l'impostazione globale Blocco oggetti S3 è abilitata, i criteri ILM attivi e inattivi possono includere sia regole conformi che non conformi.

- La regola predefinita in una policy ILM attiva o inattiva deve essere conforme.
- Le regole non conformi si applicano solo agli oggetti nei bucket in cui non è abilitato S3 Object Lock o in cui non è abilitata la funzionalità legacy Compliance.
- Le regole conformi possono essere applicate agli oggetti in qualsiasi bucket; non è necessario abilitare S3 Object Lock o la conformità legacy per il bucket.

"Esempio di una policy ILM conforme per S3 Object Lock"

Requisiti per i bucket con S3 Object Lock abilitato

- Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID, è possibile utilizzare Tenant Manager, Tenant Management API o S3 REST API per creare bucket con S3 Object Lock abilitato.
- Se si prevede di utilizzare S3 Object Lock, è necessario abilitarlo quando si crea il bucket. Non è possibile abilitare S3 Object Lock per un bucket esistente.
- Quando S3 Object Lock è abilitato per un bucket, StorageGRID abilita automaticamente il controllo delle versioni per quel bucket. Non è possibile disattivare S3 Object Lock o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione predefinita e un periodo di conservazione per ciascun bucket utilizzando Tenant Manager, Tenant Management API o S3 REST API. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket.

che non dispongono di impostazioni di conservazione proprie. È possibile ignorare queste impostazioni predefinite specificando una modalità di conservazione e una data di conservazione per ogni versione dell'oggetto quando viene caricata.

- La configurazione del ciclo di vita del bucket è supportata per i bucket con S3 Object Lock abilitato.
- La replica CloudMirror non è supportata per i bucket con S3 Object Lock abilitato.

Requisiti per gli oggetti nei bucket con S3 Object Lock abilitato

- Per proteggere una versione dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure specificare le impostazioni di conservazione per ciascuna versione dell'oggetto. Le impostazioni di conservazione a livello di oggetto possono essere specificate tramite l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni degli oggetti. Una versione di un oggetto può avere sia un'impostazione di conservazione fino alla data di scadenza che un'impostazione di conservazione legale, una ma non l'altra, oppure nessuna delle due. Specificando un'impostazione di conservazione fino a data o di conservazione legale per un oggetto, si 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 abilitato

Ogni oggetto salvato in un bucket con S3 Object Lock abilitato attraversa queste fasi:

1. Ingestione di oggetti

Quando una versione di un oggetto viene aggiunta a un bucket in cui è abilitato il blocco degli oggetti S3, le impostazioni di conservazione vengono applicate come segue:

- Se per l'oggetto sono specificate impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.
- Se non vengono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se presenti.
- Se non vengono 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 sia tutti 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 di copie degli oggetti e le posizioni di archiviazione sono determinati dalle regole conformi nelle policy ILM attive. La possibilità di eliminare un oggetto protetto prima che venga raggiunta la data di conservazione dipende dalla sua modalità di conservazione.

- Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

Informazioni correlate

- ["Crea un bucket S3"](#)
- ["Aggiorna la conservazione predefinita del blocco degli oggetti S3"](#)
- ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#)

- ["Esempio 7: Politica ILM conforme per S3 Object Lock"](#)

Abilita 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 abilitare S3 Object Lock per l'intero sistema StorageGRID . Abilitando l'impostazione globale S3 Object Lock, qualsiasi utente tenant S3 può creare e gestire bucket e oggetti con S3 Object Lock.

Prima di iniziare

- Tu hai il ["Permesso di accesso root"](#) .
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai esaminato il flusso di lavoro di S3 Object Lock e ne hai compreso le considerazioni.
- Hai confermato che la regola predefinita nel criterio ILM attivo è conforme. Vedere ["Crea una regola ILM predefinita"](#) per i dettagli.

Informazioni su questo compito

Un amministratore di griglia deve abilitare l'impostazione globale S3 Object Lock per consentire agli utenti tenant di creare nuovi bucket con S3 Object Lock abilitato. Una volta abilitata, questa impostazione non può essere disabilitata.

Dopo aver abilitato l'impostazione globale Blocco oggetti S3, rivedere le impostazioni di conformità dei tenant esistenti. Quando si abilita questa impostazione, le impostazioni di S3 Object Lock per tenant dipendono dalla versione StorageGRID al momento della creazione del tenant.



L'impostazione Conformità globale è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione Blocco oggetto S3 viene abilitata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per i dettagli, vedere ["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"](#) .

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Blocco oggetto S3**.

Viene visualizzata la pagina Impostazioni blocco oggetti S3.

2. Selezionare **Abilita blocco oggetto S3**.

3. Selezionare **Applica**.

Viene visualizzata una finestra di dialogo di conferma che ricorda che non è possibile disattivare S3 Object Lock dopo averlo attivato.

4. Se sei sicuro di voler abilitare in modo permanente S3 Object Lock per l'intero sistema, seleziona **OK**.

Quando selezioni **OK**:

- Se la regola predefinita nel criterio ILM attivo è conforme, S3 Object Lock è ora abilitato per l'intera griglia e non può essere disabilitato.
- Se la regola predefinita non è conforme, viene visualizzato un errore. È necessario creare e attivare

una nuova policy ILM che includa una regola conforme come regola predefinita. Selezionare **OK**. Quindi, crea una nuova policy, simulala e attivala. Vedere ["Crea policy ILM"](#) per istruzioni.

Risolvi gli errori di coerenza durante l'aggiornamento del blocco degli oggetti S3 o della configurazione di conformità legacy

Se un sito del data center o più nodi di archiviazione in un sito diventano non disponibili, potrebbe essere necessario aiutare gli utenti del tenant S3 ad applicare le modifiche al blocco degli oggetti S3 o alla configurazione di conformità legacy.

Gli utenti tenant che dispongono di bucket con S3 Object Lock (o legacy Compliance) abilitato possono modificare determinate impostazioni. Ad esempio, un utente tenant che utilizza S3 Object Lock potrebbe dover mettere una versione dell'oggetto in conservazione legale.

Quando un utente tenant aggiorna le impostazioni per un bucket S3 o una versione di oggetto, StorageGRID tenta di aggiornare immediatamente i metadati del bucket o dell'oggetto in tutta la griglia. Se il sistema non riesce ad aggiornare i metadati perché un sito del data center o più nodi di archiviazione non sono disponibili, restituisce 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, segui questi passaggi:

1. Tentare di rendere nuovamente disponibili tutti i nodi o siti di archiviazione il prima possibile.
2. Se non riesci a rendere disponibili sufficienti nodi di archiviazione in ogni sito, contatta l'assistenza tecnica, che può aiutarti a ripristinare i nodi e a garantire che le modifiche vengano applicate in modo coerente in tutta la griglia.
3. Una volta risolto il problema di fondo, ricorda all'utente tenant di riprovare ad apportare le modifiche alla configurazione.

Informazioni correlate

- ["Utilizzare un account tenant"](#)
- ["Utilizzare l'API REST S3"](#)
- ["Recuperare e mantenere"](#)

Esempio di regole e policy ILM

Esempio 1: regole e policy ILM per l'archiviazione degli oggetti

È possibile utilizzare le seguenti regole e policy di esempio come punto di partenza per definire una policy ILM che soddisfi i requisiti di protezione e conservazione degli oggetti.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Regola ILM 1 per l'esempio 1: Copia i dati dell'oggetto in due siti

Questa regola ILM di esempio copia i dati degli oggetti nei pool di archiviazione in due siti.

Definizione della regola	Valore di esempio
Pool di archiviazione monosito	Due pool di archiviazione, ciascuno contenente siti diversi, denominati Sito 1 e Sito 2.
Nome della regola	Due copie due siti
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Dal giorno 0 all'infinito, conserva una copia replicata nel sito 1 e una copia replicata nel sito 2.

La sezione Analisi delle regole del diagramma di conservazione afferma:

- La protezione contro le perdite del sito StorageGRID sarà valida per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola non verranno eliminati da ILM.

Reference time ⓘ

Ingest time

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store forever

Store objects by replicating 1 copies at Site 1

and store objects by replicating 1 copies at Site 2

Add other type or location

Add another time period

Retention diagram

Replicated copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

1 replicated copy - Site 1

1 replicated copy - Site 2

Duration Forever

Regola ILM 2 per l'esempio 1: profilo di codifica di cancellazione con corrispondenza del bucket

Questa regola ILM di esempio utilizza un profilo di codifica di cancellazione e un bucket S3 per determinare dove e per quanto tempo l'oggetto viene archiviato.

705

Definizione della regola	Valore di esempio
Pool di archiviazione con più siti	• Un pool di archiviazione su tre siti (siti 1, 2, 3) • Utilizzare lo schema di codifica di cancellazione 6+3
Nome della regola	S3 Bucket finance-records
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Per gli oggetti nel bucket S3 denominato finance-records, creare una copia con codice di cancellazione nel pool specificato dal profilo di codifica di cancellazione. Conserva questa copia per sempre.

Time period and placements
Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1
From Day 0
store forever

Store objects by erasure coding using 6+3 EC scheme at Sites 1, 2, 3

Add other type or location

Add another time period

Retention diagram
Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: **Ingest time**

Day 0

Day 0 - forever
EC 6+3 - Sites 1, 2, 3

Duration
Forever

Politica ILM per esempio 1

Nella pratica, la maggior parte delle policy ILM sono semplici, anche se il sistema StorageGRID consente di progettare policy ILM sofisticate e complesse.

Una tipica policy ILM per una griglia multi-sito potrebbe includere regole ILM come le seguenti:

- Durante l'acquisizione, archivia tutti gli oggetti appartenenti al bucket S3 denominato `finance-records` in un pool di archiviazione 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 archiviare una copia di tale oggetto nel Sito 1 e una copia nel Sito 2.

Proposed policy name

Object Storage Policy

Reason for change

example 1

Manage rules

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

Select rules

Rule order	Rule name	Filters
1	S3 Bucket finance-records	Tenant is Finance Bucket name is finance-records
Default	Two Copies Two Data Centers	—

Informazioni correlate

- ["Utilizzare le policy ILM"](#)
- ["Creare policy ILM"](#)

Esempio 2: regole e policy ILM per il filtraggio delle dimensioni degli oggetti EC

È possibile utilizzare le seguenti regole e policy di esempio come punti di partenza per definire una policy ILM che filtri in base alle dimensioni dell'oggetto per soddisfare i requisiti EC consigliati.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Regola ILM 1 per l'esempio 2: utilizzare EC per oggetti maggiori di 1 MB

Questa regola ILM di esempio codifica gli oggetti di dimensioni superiori a 1 MB.



La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	Solo oggetti EC > 1 MB
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto maggiore di 1 MB

Definizione della regola	Valore di esempio
Posizionamenti	Crea una copia con codice di cancellazione 2+1 utilizzando tre siti

Filter group 1
Objects with all of following metadata will be evaluated by this rule:

Object size
greater than
1
MB

Regola ILM 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 la policy. Poiché la prima regola filtra tutti gli oggetti di dimensioni 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
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Nessuno
Posizionamenti	Dal giorno 0 all'infinito, conserva una copia replicata nel sito 1 e una copia replicata nel sito 2.

Criterio ILM per esempio 2: utilizzare EC per oggetti maggiori di 1 MB

Questo esempio di policy ILM include due regole ILM:

- La prima regola codifica tutti gli oggetti di dimensioni superiori a 1 MB.
- La seconda regola ILM (predefinita) crea due copie replicate. Poiché gli oggetti di dimensioni 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 immagine

È possibile utilizzare le seguenti regole e policy di esempio per garantire che le immagini di dimensioni superiori a 1 MB vengano codificate con cancellazione e che vengano realizzate due copie delle immagini più piccole.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Regola ILM 1 per esempio 3: utilizzare EC per file immagine superiori a 1 MB

Questa regola ILM di esempio utilizza un filtro avanzato per cancellare il codice di tutti i file immagine di dimensioni superiori a 1 MB.



La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	File immagine EC > 1 MB
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto maggiore di 1 MB
Filtri avanzati per la chiave	• Termina con .jpg • Termina con .png
Posizionamenti	Crea una copia con codice di cancellazione 2+1 utilizzando tre siti

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼

greater than ▼

1 ⬆ ⬇ ⬆

MB ▼ ✕

and Key ▼

ends with ▼

.jpg ✕

or Filter group 2 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼

greater than ▼

1 ⬆ ⬇ ⬆

MB ▼ ✕

and Key ▼

ends with ▼

.png ✕

Poiché questa regola è configurata come la prima regola del criterio, l'istruzione di posizionamento della codifica di cancellazione si applica solo ai file .jpg e .png di dimensioni superiori a 1 MB.

Regola ILM 2 per l'esempio 3: creare 2 copie replicate per tutti i file immagine rimanenti

Questa regola ILM di esempio utilizza un filtro avanzato per specificare che i file immagine più piccoli devono essere replicati. Poiché la prima regola del criterio ha già trovato corrispondenze con file immagine di dimensioni superiori a 1 MB, questa regola si applica ai file immagine di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Nome della regola	2 copie per i file immagine

709

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione
Filtri avanzati per la chiave	• Termina con .jpg • Termina con .png
Posizionamenti	Crea 2 copie replicate in due pool di archiviazione

Politica ILM per esempio 3: migliore protezione per i file immagine

Questo esempio di policy ILM include tre regole:

- La prima regola codifica tutti i file immagine di dimensioni superiori a 1 MB.
- La seconda regola crea due copie di tutti i file immagine rimanenti (ovvero immagini di dimensioni pari o inferiori a 1 MB).
- La regola predefinita si applica a tutti gli oggetti rimanenti (ovvero 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 e policy ILM per oggetti con versione S3

Se disponi di un bucket S3 con il controllo delle versioni abilitato, puoi gestire le versioni degli oggetti non correnti includendo regole nella policy ILM che utilizzano "Tempo non corrente" come tempo di riferimento.



Se si specifica un periodo di conservazione limitato per gli oggetti, tali oggetti verranno eliminati definitivamente una volta raggiunto il periodo di tempo specificato. Assicuratevi di aver capito per quanto tempo gli oggetti verranno conservati.

Come mostra questo esempio, è possibile controllare la quantità di spazio di archiviazione utilizzato dagli oggetti sottoposti a controllo di versione utilizzando diverse istruzioni di posizionamento per le versioni non correnti degli oggetti.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti 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 l'UUID e il CBID, utilizzare ["ricerca metadati oggetto"](#) mentre l'oggetto è ancora attuale.

Informazioni correlate

["Come vengono eliminati gli oggetti"](#)

Regola ILM 1 per esempio 4: Conservare 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 sottoposti a controllo di versione o meno.

Definizione della regola	Valore di esempio
Pool di stoccaggio	Tre pool di archiviazione, ciascuno composto da data center diversi, denominati Sito 1, Sito 2 e Sito 3.
Nome della regola	Tre copie dieci anni
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conservare tre copie replicate per 10 anni (3.652 giorni), una nel sito 1, una nel sito 2 e una nel sito 3. Dopo 10 anni, eliminare tutte le copie dell'oggetto.

Regola ILM 2 per esempio 4: Salvare due copie delle 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 tutte le versioni non correnti.

Per creare una regola che utilizzi "Tempo non corrente" come orario di riferimento, seleziona **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (in bucket S3 con controllo delle versioni abilitato)?" nel passaggio 1 (Immetti dettagli) della procedura guidata Crea una regola ILM. Selezionando **Sì**, *Tempo non corrente* viene automaticamente selezionato come orario di riferimento e non è possibile selezionare un orario di riferimento diverso.

1

Enter details

2

Define placements

3

Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)

Specify which tenant accounts and buckets this rule applies to.

Tenant accounts ?

Select tenant accounts

Bucket name ?

matches all

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? ?

☐ No☒ Yes

In questo esempio, vengono archiviate solo due copie delle versioni non correnti, che verranno conservate per due anni.

Definizione della regola	Valore di esempio
Pool di archiviazione	Due pool di archiviazione, ciascuno in data center diversi, Sito 1 e Sito 2.
Nome della regola	Versioni non correnti: due copie due anni
Tempo di riferimento	Tempo non corrente Selezionato automaticamente quando si seleziona Sì alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (in bucket S3 con controllo delle versioni abilitato)?" nella procedura guidata Crea una regola ILM.
Posizionamenti	Il giorno 0 relativo al tempo non corrente (ovvero a partire dal giorno in cui la versione dell'oggetto diventa la versione non corrente), conservare due copie replicate delle versioni dell'oggetto non corrente per 2 anni (730 giorni), una nel sito 1 e una nel sito 2. Dopo 2 anni, eliminare le versioni non correnti.

Criterio ILM per esempio 4: oggetti con versione S3

Se si desidera gestire le versioni precedenti di un oggetto in modo diverso rispetto alla versione corrente, le regole che utilizzano "Tempo non corrente" come orario di riferimento devono comparire nel criterio ILM prima delle regole che si applicano alla versione corrente dell'oggetto.

Una policy ILM per oggetti con versione S3 potrebbe includere regole ILM come le seguenti:

- Conservare tutte 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 comparire nel criterio prima delle regole che si applicano alla versione corrente dell'oggetto. In caso contrario, le versioni degli oggetti non correnti non verranno mai abbinate dalla regola "Tempo non corrente".

- Al momento dell'ingestione, creare tre copie replicate e conservarne una copia in ciascuno dei tre siti. Conservare copie della versione corrente dell'oggetto per 10 anni.

Quando si simula la policy di esempio, ci si aspetterebbe che gli oggetti di prova vengano valutati come segue:

- Tutte le versioni non correnti degli oggetti verrebbero confrontate con la prima regola. Se una versione non corrente di un oggetto è più vecchia di 2 anni, ILM la elimina definitivamente (tutte le copie della versione non corrente vengono rimosse dalla griglia).
- La versione corrente dell'oggetto verrebbe abbinata alla seconda regola. 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 dell'oggetto "non corrente". La prossima volta che si verifica la valutazione ILM, questa versione non corrente viene abbinata alla prima regola. Di conseguenza, la copia nel Sito 3 viene eliminata e le due copie nel Sito 1 e nel Sito 2 vengono conservate per altri 2 anni.

Esempio 5: regole e policy ILM per un comportamento di acquisizione rigoroso

È possibile utilizzare un filtro di posizione e il comportamento di acquisizione Rigoroso in una regola per impedire che gli oggetti vengano salvati in una posizione specifica del data center.

In questo esempio, un inquilino con sede a Parigi non vuole immagazzinare alcuni oggetti al di fuori dell'UE a causa di problemi normativi. Altri oggetti, compresi tutti gli oggetti provenienti da altri account tenant, possono essere archiviati nel data center di Parigi o in quello degli Stati Uniti.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Informazioni correlate

- ["Opzioni di acquisizione"](#)
- ["Crea regola ILM: seleziona il comportamento di acquisizione"](#)

Regola ILM 1 per esempio 5: Ingestione rigorosa per garantire il data center di Parigi

Questa regola ILM di esempio utilizza il comportamento di ingestione Strict per garantire che gli oggetti salvati da un tenant con sede a Parigi nei bucket S3 con la regione impostata su eu-west-3 (Parigi) non vengano mai

archiviati 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
Conto inquilino	inquilino di Parigi
Filtro avanzato	Il vincolo di posizione è uguale a eu-west-3
Pool di stoccaggio	Sito 1 (Parigi)
Nome della regola	Rigoroso inserimento per garantire il data center di Parigi
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre nel sito 1 (Parigi)
Comportamento di ingestione	Rigoroso. Utilizzare sempre i posizionamenti di questa regola durante l'acquisizione. L'acquisizione fallisce se non è possibile archiviare due copie dell'oggetto nel data center di Parigi.

Strict ingest to guarantee Paris data center

Compliant: Yes

Used in active policy: No

Used in proposed policy: No

Ingest behavior: Strict

Reference time: Ingest time

Clone

Edit

Remove

Filters

This rule applies if:

- Tenant is Paris tenant

And it only applies if objects have this metadata:

- Location constraint is eu-west-3

Time period and placements

Retention diagram

Placement instructions

Sort placements by

Time period

Storage pool

● Replicated copy

Rule analysis:

- StorageGRID site-loss protection will not apply from Day 0 - Forever.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Site 1

Duration

Forever

714

Regola ILM 2 per esempio 5: Ingestione bilanciata per altri oggetti

Questa regola ILM di esempio utilizza il comportamento di acquisizione bilanciato per garantire un'efficienza ILM ottimale per tutti gli oggetti non corrispondenti alla prima regola. Verranno conservate due copie di tutti gli oggetti che soddisfano questa regola: una nel centro dati degli Stati Uniti e una nel centro dati di Parigi. Se la regola non può essere soddisfatta immediatamente, vengono conservate copie provvisorie in qualsiasi posizione disponibile.

Questa regola si applica agli oggetti che appartengono a qualsiasi tenant e a qualsiasi regione.

Definizione della regola	Valore di esempio
Conto inquilino	Ignorare
Filtro avanzato	<i>Non specificato</i>
Pool di stoccaggio	Sito 1 (Parigi) e Sito 2 (Stati Uniti)
Nome della regola	2 copie 2 data center
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre in due data center
Comportamento di ingestione	Equilibrato. Se possibile, gli oggetti che corrispondono a questa regola vengono posizionati secondo le istruzioni di posizionamento della regola. In caso contrario, vengono effettuate copie provvisorie in qualsiasi luogo disponibile.

Politica ILM per l'esempio 5: combinazione di comportamenti di acquisizione

L'esempio di policy ILM include due regole con comportamenti di acquisizione diversi.

Una policy ILM che utilizza due diversi comportamenti di acquisizione potrebbe includere regole ILM come le seguenti:

- Archiviare 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. L'acquisizione non riesce se il data center di Parigi non è disponibile.
- Archiviare tutti gli altri oggetti (inclusi quelli che appartengono al tenant di Parigi ma che hanno una regione bucket diversa) sia nel data center statunitense che in quello di Parigi. Se non è possibile soddisfare le istruzioni di posizionamento, effettuare copie provvisorie in qualsiasi luogo disponibile.

Quando si simula la policy di esempio, ci si aspetta che gli oggetti di prova 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 vengono archiviati nel data center di Parigi. Poiché la prima regola utilizza l'acquisizione rigorosa, questi oggetti non vengono mai archiviati nel data center statunitense. Se i nodi di archiviazione nel data center di Parigi non sono disponibili, l'acquisizione fallisce.
- Tutti gli altri oggetti vengono abbinati dalla seconda regola, compresi gli oggetti che appartengono al tenant di Parigi e che non hanno la regione del bucket S3 impostata su eu-west-3. In ogni data center viene

salvata una copia di ogni oggetto. Tuttavia, poiché la seconda regola utilizza l'acquisizione bilanciata, se un data center non è disponibile, vengono salvate due copie provvisorie in qualsiasi posizione disponibile.

Esempio 6: Modificare una policy 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 ai posizionamenti ILM possono influire temporaneamente sulle prestazioni complessive di un sistema StorageGRID .

In questo esempio, è stato aggiunto un nuovo sito StorageGRID in un'espansione ed è necessario implementare una nuova policy ILM attiva per archiviare i dati nel nuovo sito. Per implementare una nuova politica attiva, prima **"creare una politica"** . Dopodiché, devi **"simulare"** poi **"attivare"** la nuova politica.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Come la modifica di una policy ILM influisce sulle prestazioni

Quando si attiva una nuova policy ILM, le prestazioni del sistema StorageGRID potrebbero essere temporaneamente compromesse, soprattutto se le istruzioni di posizionamento nella nuova policy richiedono lo spostamento di molti oggetti esistenti in nuove posizioni.

Quando si attiva una nuova policy ILM, StorageGRID la utilizza per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Prima di attivare una nuova policy ILM, rivedere tutte le modifiche apportate al posizionamento degli oggetti replicati e con codice di cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Per garantire che una nuova policy ILM non influisca sul posizionamento degli oggetti replicati e codificati per la cancellazione esistenti, è possibile **"creare una regola ILM con un filtro temporale di acquisizione"** . Ad esempio, **L'ora di ingestione è uguale o successiva <data e ora>**, in modo che la nuova regola si applichi solo agli oggetti ingeriti nella data e ora specificate o successivamente.

I tipi di modifiche ai criteri ILM che possono influire temporaneamente sulle prestazioni StorageGRID includono quanto segue:

- Applicazione di un profilo di codifica di cancellazione diverso agli oggetti con codifica di cancellazione esistenti.



StorageGRID considera ogni profilo di codifica di cancellazione come univoco e non riutilizza i frammenti di codifica di cancellazione quando viene utilizzato un nuovo profilo.

- Modifica del tipo di copie richieste per gli oggetti esistenti; ad esempio, convertendo una grande percentuale di oggetti replicati in oggetti con codice di cancellazione.
- Spostamento di copie di oggetti esistenti in una posizione completamente diversa; ad esempio, spostamento di un gran numero di oggetti da o verso un pool di archiviazione cloud o da o verso un sito remoto.

Criterio ILM attivo per 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.

Active policy

Policy history

Policy name:

Data Protection for Two Sites (2 rules)

Reason for change :

Data protection for two sites (using 2 rules)

Start date:

2022-10-11 10:37:11 MDT

Simulate

Policy rules

Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

In questa policy ILM, gli oggetti appartenenti al tenant A sono protetti tramite codifica di cancellazione 2+1 in un singolo sito, mentre gli oggetti appartenenti a tutti gli altri tenant sono protetti su due siti tramite replica a 2 copie.

Regola 1: Codifica di cancellazione in un unico sito per l'inquilino A

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione in un unico sito per l'inquilino A
Conto inquilino	Inquilino A
Pool di archiviazione	Sito 1
Posizionamenti	Codifica di cancellazione 2+1 nel sito 1 dal giorno 0 all'infinito

Regola 2: Replicazione a due siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a due siti per altri tenant
Conto inquilino	Ignorare
Pool di archiviazione	Sito 1 e Sito 2

Definizione della regola	Valore di esempio
Posizionamenti	Due copie replicate dal giorno 0 all'infinito: una copia nel Sito 1 e una copia nel Sito 2.

Politica 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 archiviazione: un pool di archiviazione per il sito 3 e un pool di archiviazione contenente tutti e tre i siti (diverso dal pool di archiviazione predefinito Tutti i nodi di archiviazione). Quindi, l'amministratore ha creato due nuove regole ILM e una nuova policy ILM, studiate per proteggere i dati in tutti e tre i siti.

Quando questa nuova policy ILM verrà attivata, gli oggetti appartenenti al Tenant A saranno protetti tramite codifica di cancellazione 2+1 in tre siti, mentre gli oggetti appartenenti ad altri tenant (e oggetti più piccoli appartenenti al Tenant A) saranno protetti in tre siti tramite replica a 3 copie.

Regola 1: Codifica di cancellazione a tre siti per l'inquilino A

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione a tre siti per l'inquilino A
Conto inquilino	Inquilino A
Pool di archiviazione	Tutti e 3 i siti (include il sito 1, il sito 2 e il sito 3)
Posizionamenti	Codifica di cancellazione 2+1 in tutti e 3 i siti dal giorno 0 all'infinito

Regola 2: Replicazione a tre siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a tre siti per altri tenant
Conto inquilino	Ignorare
Pool di archiviazione	Sito 1, Sito 2 e Sito 3
Posizionamenti	Tre copie replicate dal giorno 0 all'infinito: una copia nel Sito 1, una copia nel Sito 2 e una copia nel Sito 3.

Attivazione della politica ILM ad esempio 6

Quando si attiva una nuova policy ILM, gli oggetti esistenti potrebbero essere spostati in nuove posizioni oppure potrebbero essere create nuove copie degli oggetti esistenti, in base alle istruzioni di posizionamento contenute in eventuali regole nuove o aggiornate.



Gli errori in una policy 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 una nuova policy ILM, StorageGRID la utilizza per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Prima di attivare una nuova policy ILM, rivedere tutte le modifiche apportate al posizionamento degli oggetti replicati e con codice di cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Cosa succede quando cambiano le istruzioni di codifica di cancellazione

Nella policy ILM attualmente attiva per questo esempio, gli oggetti appartenenti al Tenant A sono protetti mediante la codifica di cancellazione 2+1 nel Sito 1. Nella nuova politica ILM, gli oggetti appartenenti al Tenant A saranno protetti mediante la codifica di cancellazione 2+1 nei siti 1, 2 e 3.

Quando viene attivata la nuova policy 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 conservato 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 ILM utilizzano un nuovo profilo di codifica di cancellazione, vengono creati e distribuiti ai tre siti frammenti completamente nuovi con codifica di cancellazione.



I frammenti 2+1 esistenti nel Sito 1 non vengono riutilizzati. StorageGRID considera ogni profilo di codifica di cancellazione come univoco e non riutilizza i frammenti di codifica di cancellazione quando viene utilizzato un nuovo profilo.

Cosa succede quando cambiano le istruzioni di replicazione

Nella policy ILM attualmente attiva per questo esempio, gli oggetti appartenenti ad altri tenant vengono protetti mediante due copie replicate nei pool di archiviazione nei siti 1 e 2. Nella nuova policy ILM, gli oggetti appartenenti ad altri tenant saranno protetti mediante tre copie replicate in pool di archiviazione nei siti 1, 2 e 3.

Quando viene attivata la nuova policy ILM, si verificano le seguenti operazioni ILM:

- Quando un tenant diverso dal tenant A acquisisce un nuovo oggetto, StorageGRID ne crea tre copie e ne salva una in ogni sito.
- Gli oggetti esistenti appartenenti a questi altri inquilini vengono rivalutati durante il processo di scansione ILM in corso. Poiché le copie degli oggetti esistenti nel Sito 1 e nel Sito 2 continuano a soddisfare i requisiti di replicazione della nuova regola ILM, StorageGRID deve creare solo una nuova copia dell'oggetto per il Sito 3.

Impatto sulle prestazioni dell'attivazione di questa policy

Quando viene attivata la policy ILM in questo esempio, le prestazioni complessive del sistema StorageGRID saranno temporaneamente compromesse. Saranno necessari livelli di risorse di rete superiori al normale per creare nuovi frammenti con codice di cancellazione per gli oggetti esistenti del Tenant A e nuove copie replicate nel Sito 3 per gli oggetti esistenti degli altri tenant.

A seguito della modifica della policy ILM, le richieste di lettura e scrittura dei client potrebbero temporaneamente presentare latenze superiori al normale. Le latenze torneranno ai livelli normali dopo che le

istruzioni di posizionamento saranno state completamente implementate nella griglia.

Per evitare problemi di risorse durante l'attivazione di un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Tempo di acquisizione in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare il tempo di acquisizione su un valore maggiore o uguale al momento approssimativo in cui la nuova policy entrerà in vigore, per garantire che gli oggetti esistenti non vengano spostati inutilmente.



Contattare l'assistenza tecnica se è necessario rallentare o aumentare la velocità di elaborazione degli oggetti dopo una modifica della policy ILM.

Esempio 7: Politica ILM conforme per S3 Object Lock

È possibile utilizzare il bucket S3, le regole ILM e la policy ILM in questo esempio come punto di partenza quando si definisce una policy ILM per soddisfare i requisiti di protezione e conservazione degli oggetti nei bucket con S3 Object Lock abilitato.



Se hai utilizzato la funzionalità di conformità legacy nelle versioni precedenti StorageGRID , puoi utilizzare questo esempio anche per gestire eventuali bucket esistenti in cui è abilitata la funzionalità di conformità legacy.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Informazioni correlate

- ["Gestisci gli oggetti con S3 Object Lock"](#)
- ["Creare una policy ILM"](#)

Esempio di bucket e oggetti per S3 Object Lock

In questo esempio, un account tenant S3 denominato Bank of ABC ha utilizzato Tenant Manager per creare un bucket con S3 Object Lock abilitato per archiviare i record bancari critici.

Definizione di bucket	Valore di esempio
Nome dell'account dell'inquilino	Banca ABC
Nome del bucket	registri bancari
Regione del bucket	us-east-1 (predefinito)

Ogni oggetto e versione dell'oggetto che viene aggiunto al bucket dei record bancari utilizzerà i seguenti valori per `retain-until-date` E `legal hold` impostazioni.

Impostazione per ogni oggetto	Valore di esempio
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 dicembre 2030) Ogni versione dell'oggetto ha la sua <code>retain-until-date</code> collocamento. Questa impostazione può essere aumentata, ma non diminuita.
<code>legal hold</code>	"OFF" (Non in vigore) È possibile applicare o rimuovere un blocco legale su qualsiasi versione dell'oggetto in qualsiasi momento durante il periodo di conservazione. Se un oggetto è sottoposto a una sospensione legale, l'oggetto non può essere eliminato anche se <code>retain-until-date</code> è stato raggiunto.

Regola ILM 1 per esempio di blocco oggetto S3: profilo di codifica di cancellazione con corrispondenza bucket

Questa regola ILM di esempio si applica solo al conto tenant S3 denominato Bank of ABC. Corrisponde a qualsiasi oggetto nel `bank-records` bucket e quindi utilizza la codifica di cancellazione per archiviare l'oggetto sui nodi di archiviazione in tre siti di data center utilizzando un profilo di codifica di cancellazione 6+3. Questa regola soddisfa i requisiti del bucket con S3 Object Lock abilitato: una copia viene conservata sui nodi di archiviazione dal giorno 0 all'infinito, utilizzando l'ora di ingestione come ora di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Regola conforme: Oggetti EC nel bucket dei registri bancari - Bank of ABC
Conto inquilino	Banca ABC
Nome del bucket	<code>bank-records</code>
Filtro avanzato	Dimensione oggetto (MB) maggiore di 1 Nota: questo filtro garantisce che la codifica di cancellazione non venga utilizzata per oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Dal giorno 0 conservalo per sempre
Profilo di codifica di cancellazione	• Creare una copia con codice di cancellazione sui nodi di archiviazione in tre siti di data center • Utilizza lo schema di codifica di cancellazione 6+3

Esempio di regola ILM 2 per blocco oggetto S3: regola non conforme

Questa regola ILM di esempio memorizza inizialmente due copie replicate dell'oggetto sui nodi di archiviazione. Dopo un anno, ne memorizza una copia per sempre su un Cloud Storage Pool. Poiché questa regola utilizza un Cloud Storage Pool, non è conforme e non verrà applicata agli oggetti nei bucket con S3 Object Lock abilitato.

Definizione della regola	Valore di esempio
Nome della regola	Regola non conforme: utilizzare Cloud Storage Pool
Conti degli inquilini	Non specificato
Nome del bucket	Non specificato, ma si applicherà solo ai bucket in cui non è abilitato S3 Object Lock (o la funzionalità legacy Compliance).
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione
Posizionamenti	• Il giorno 0, conserva due copie replicate sui nodi di archiviazione nel Data Center 1 e nel Data Center 2 per 365 giorni • Dopo 1 anno, conserva una copia replicata in un Cloud Storage Pool per sempre

Regola ILM 3 per esempio di blocco oggetto S3: regola predefinita

Questa regola ILM di esempio copia i dati degli oggetti nei pool di archiviazione in due data center. Questa regola conforme è concepita per essere la regola predefinita nella policy 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 dell'oggetto vengono conservate sui nodi di archiviazione dal giorno 0 all'infinito, utilizzando Ingest come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Regola di conformità predefinita: due copie, due data center
Conto inquilino	Non specificato
Nome del bucket	Non specificato
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione

Definizione della regola	Valore di esempio
Posizionamenti	Dal giorno 0 all'infinito, conserva due copie replicate: una sui nodi di archiviazione nel Data Center 1 e una sui nodi di archiviazione nel Data Center 2.

Esempio di policy ILM conforme per S3 Object Lock

Per creare una policy ILM che protegga efficacemente tutti gli oggetti nel sistema, compresi quelli nei bucket con S3 Object Lock abilitato, è necessario selezionare le regole ILM che soddisfano i requisiti di archiviazione per tutti gli oggetti. Quindi, è necessario simulare e attivare la policy.

Aggiungere regole alla policy

In questo esempio, la policy ILM include tre regole ILM, nel seguente ordine:

1. Una regola conforme che utilizza la codifica di cancellazione per proteggere gli oggetti di dimensioni superiori a 1 MB in un bucket specifico con S3 Object Lock abilitato. Gli oggetti vengono archiviati sui nodi di archiviazione dal giorno 0 all'infinito.
2. Una regola non conforme che crea due copie replicate dell'oggetto sui nodi di archiviazione per un anno e poi sposta una copia dell'oggetto in un pool di archiviazione cloud per sempre. Questa regola non si applica ai bucket con S3 Object Lock abilitato perché utilizza un Cloud Storage Pool.
3. La regola di conformità predefinita che crea due copie replicate degli oggetti sui nodi di archiviazione dal giorno 0 all'infinito.

Simulare la politica

Dopo aver aggiunto regole alla policy, scelto una regola conforme predefinita e organizzato le altre regole, dovresti simulare la policy testando gli oggetti dal bucket con S3 Object Lock abilitato e da altri bucket. Ad esempio, quando si simula la policy di esempio, ci si aspetterebbe che gli oggetti di prova vengano valutati come segue:

- La prima regola corrisponderà solo agli oggetti di prova che sono maggiori di 1 MB nel bucket bank-records per il tenant Bank of ABC.
- La seconda regola corrisponderà a tutti gli oggetti in tutti i bucket non conformi per tutti gli altri account tenant.
- La regola predefinita corrisponderà a questi oggetti:
 - Oggetti di dimensioni pari o inferiori a 1 MB nel bucket bank-records per il tenant Bank of ABC.
 - Oggetti in qualsiasi altro bucket in cui è abilitato il blocco oggetti S3 per tutti gli altri account tenant.

Attiva la politica

Quando sei completamente soddisfatto che la nuova policy protegga i dati degli oggetti come previsto, puoi attivarla.

Esempio 8: Priorità per il ciclo di vita del bucket S3 e policy 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 ciclo di vita del bucket che ha la priorità sulla policy ILM

Politica ILM

- Regola basata sul riferimento temporale non corrente: il giorno 0, conserva X copie per 20 giorni
- Regola basata sul riferimento al momento dell'acquisizione (predefinita): il giorno 0, conserva X copie per 50 giorni

Ciclo di vita del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 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 marcatore di eliminazione e "docs/text" diventa non corrente.
 - Dopo 5 giorni, per un totale di 105 giorni dall'acquisizione, "docs/text" viene eliminato.
 - Dopo 95 giorni, per un totale di 200 giorni dall'inserimento e 100 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.
- Viene acquisito un oggetto denominato "video/film". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
 - Dopo 50 giorni viene creato un marcatore di eliminazione e "video/film" diventa non corrente.
 - Dopo 20 giorni, ovvero 70 giorni in totale dall'acquisizione, "video/film" viene eliminato.
 - Dopo 30 giorni, per un totale di 100 giorni dall'inserimento e 50 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.

Esempio di ciclo di vita del bucket che mantiene implicitamente per sempre

Politica ILM

- Regola basata sul riferimento temporale non corrente: il giorno 0, conserva X copie per 20 giorni
- Regola basata sul riferimento al momento dell'acquisizione (predefinita): il giorno 0, conserva X copie per 50 giorni

Ciclo di vita del bucket

```
"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 il mantenimento di tutto il resto per sempre (a partire da "docs/").

I marcatori di eliminazione che iniziano con "docs/" vengono rimossi quando scadono.

- Viene acquisito un oggetto denominato "video/film". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
 - Dopo 50 giorni viene creato un marcatore di eliminazione e "video/film" diventa non corrente.

- Dopo 20 giorni, ovvero 70 giorni in totale dall'acquisizione, "video/film" viene eliminato.
- Dopo 30 giorni, per un totale di 100 giorni dall'inserimento e 50 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.

Esempio di utilizzo del ciclo di vita del bucket per duplicare ILM e ripulire i marcatori di eliminazione scaduti

Politica ILM

- Regola basata sul riferimento temporale non corrente: il giorno 0, conserva X copie per 20 giorni
- Regola basata sul riferimento al momento dell'acquisizione (predefinita): il giorno 0, conserva X copie per sempre

Ciclo di vita del bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Risultato

- La policy ILM viene duplicata nel ciclo di vita del bucket.
 - La regola "per sempre" della policy ILM è progettata per rimuovere manualmente gli oggetti e ripulire le versioni non correnti dopo 20 giorni. Di conseguenza, la regola ingest-time manterrà per sempre i marcatori di eliminazione scaduti.
 - Il ciclo di vita del bucket duplica il comportamento della policy ILM durante l'aggiunta `"ExpiredObjectDeleteMarker": true`, che rimuove i marcatori di eliminazione una volta scaduti
- Un oggetto viene ingerito. Nessun filtro significa che il ciclo di vita del bucket si applica a tutti gli oggetti e sostituisce le impostazioni di conservazione ILM.
 - Quando un tenant invia una richiesta di eliminazione di un oggetto, viene creato un marcatore di eliminazione e l'oggetto diventa non corrente.
 - Dopo 20 giorni, l'oggetto non corrente viene eliminato e il marcatore di eliminazione scade.
 - Poco dopo, il marcatore di eliminazione scaduto viene eliminato.

Rafforzamento del sistema

Considerazioni generali per il rafforzamento del sistema

Il rafforzamento del sistema è il processo di eliminazione del maggior numero possibile di rischi per la sicurezza da un sistema StorageGRID .

Durante l'installazione e la configurazione StorageGRID, utilizzare queste linee guida per soddisfare gli obiettivi di sicurezza prescritti in termini di riservatezza, integrità e disponibilità.

Dovresti già utilizzare le best practice standard del settore per il rafforzamento del sistema. Ad esempio, si utilizzano password complesse per StorageGRID, si utilizza HTTPS anziché HTTP e si abilita l'autenticazione basata su certificato, ove disponibile.

StorageGRID segue il ["Politica di gestione delle vulnerabilità NetApp"](#) . Le vulnerabilità segnalate vengono verificate e affrontate in base al processo di risposta agli incidenti di sicurezza del prodotto.

Quando si rafforza un sistema StorageGRID , tenere presente quanto segue:

- ***Quale delle tre reti StorageGRID * hai implementato?** Tutti i sistemi StorageGRID devono utilizzare la rete Grid, ma è possibile utilizzare anche la rete amministrativa, la rete client o entrambe. Ogni rete ha diverse considerazioni in materia di sicurezza.
- **Il tipo di piattaforme** utilizzate per i singoli nodi nel sistema StorageGRID . I nodi StorageGRID possono essere distribuiti su macchine virtuali VMware, all'interno di un motore di container su host Linux o come dispositivi hardware dedicati. Ogni tipo di piattaforma ha il suo insieme di best practice di rafforzamento.
- **Quanto sono affidabili gli account degli inquilini.** Se sei un fornitore di servizi con account tenant non attendibili, avrai problemi di sicurezza diversi rispetto a quando utilizzi solo tenant interni attendibili.
- **Quali requisiti e convenzioni di sicurezza** segue la tua organizzazione. Potrebbe essere necessario rispettare specifici requisiti normativi o aziendali.

Linee guida per il rafforzamento degli aggiornamenti software

Per difendersi dagli attacchi, è necessario mantenere aggiornati il sistema StorageGRID e i servizi correlati.

Aggiornamenti al software StorageGRID

Se possibile, è consigliabile aggiornare il software StorageGRID alla versione principale più recente o a quella precedente. Mantenere StorageGRID aggiornato aiuta a ridurre il tempo di attività delle vulnerabilità note e riduce la superficie complessiva di attacco. Inoltre, le versioni più recenti di StorageGRID spesso contengono funzionalità di rafforzamento della sicurezza non incluse nelle versioni precedenti.

Consultare il "[Strumento matrice di interoperabilità NetApp](#)" (IMT) per determinare quale versione del software StorageGRID dovresti utilizzare. Quando è necessario un hotfix, NetApp dà priorità alla creazione di aggiornamenti per le versioni più recenti. Alcune patch potrebbero non essere compatibili con le versioni precedenti.

- Per scaricare le versioni e gli hotfix più recenti StorageGRID , vai a "[Download NetApp : StorageGRID](#)" .
- Per aggiornare il software StorageGRID , vedere "[Istruzioni per l'aggiornamento](#)" .
- Per applicare un hotfix, vedere "[Procedura di hotfix di StorageGRID](#)" .

Aggiornamenti ai servizi esterni

I servizi esterni possono presentare vulnerabilità che influiscono indirettamente StorageGRID . È necessario assicurarsi 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 "[Strumento 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 "[Strumento matrice di interoperabilità NetApp](#)" .

Aggiornamenti ai nodi Linux

Se i nodi StorageGRID utilizzano piattaforme host Linux, è necessario assicurarsi che gli aggiornamenti di sicurezza e del kernel vengano 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 ["Strumento matrice di interoperabilità NetApp"](#) .

Linee guida per il rafforzamento delle reti StorageGRID

Il sistema StorageGRID supporta fino a tre interfacce di rete per nodo della griglia, consentendo di configurare la rete per ogni singolo nodo della griglia in base ai requisiti di sicurezza e accesso.

Per informazioni dettagliate sulle reti StorageGRID , vedere ["Tipi di rete StorageGRID"](#) .

Linee guida per la rete Grid

È necessario configurare una rete Grid per tutto il traffico StorageGRID interno. Tutti i nodi della griglia sono sulla rete Grid e devono essere in grado di comunicare con tutti gli altri nodi.

Durante la configurazione della rete Grid, seguire queste linee guida:

- Assicurarsi che la rete sia protetta da client non attendibili, come quelli presenti su Internet.
- Se possibile, utilizzare la rete Grid esclusivamente per il traffico interno. Sia la rete amministrativa che la rete client presentano ulteriori restrizioni firewall che bloccano il traffico esterno verso i servizi interni. È supportato l'utilizzo della Grid Network per il traffico client esterno, ma questo utilizzo offre meno livelli di protezione.
- Se la distribuzione StorageGRID si estende su più data center, utilizzare una rete privata virtuale (VPN) o equivalente sulla rete Grid per fornire ulteriore protezione al 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 di amministrazione

La rete di amministrazione viene in genere utilizzata per attività amministrative (dipendenti fidati che utilizzano Grid Manager o SSH) e per comunicare con altri servizi fidati quali LDAP, DNS, NTP o KMS (o server KMIP). Tuttavia, StorageGRID non impone questo utilizzo internamente.

Se si utilizza Admin Network, seguire queste linee guida:

- Bloccare tutte le porte di traffico interno sulla rete di amministrazione. Vedi il ["elenco delle porte interne"](#) .
- Se i client non attendibili riescono ad accedere alla rete di amministrazione, bloccare l'accesso a StorageGRID sulla rete di amministrazione con un firewall esterno.

Linee guida per la rete clienti

La rete client viene in genere utilizzata per i tenant e per comunicare con servizi esterni, come il servizio di replica CloudMirror o un altro servizio della piattaforma. Tuttavia, StorageGRID non impone questo utilizzo internamente.

Se si utilizza la rete client, seguire queste linee guida:

- Blocca tutte le porte di traffico interno sulla rete client. Vedi il ["elenco delle porte interne"](#) .
- Accetta il traffico client in entrata solo sugli endpoint configurati in modo esplicito. Vedi le informazioni su ["gestione dei controlli del firewall"](#) .

Linee guida per il rafforzamento dei nodi StorageGRID

I nodi StorageGRID possono essere distribuiti su macchine virtuali VMware, all'interno di un motore di container su host Linux o come dispositivi hardware dedicati. Ogni tipo di piattaforma e ogni tipo di nodo ha il suo insieme di best practice di rafforzamento.

Controllare l'accesso IPMI remoto a BMC

È possibile abilitare o disabilitare l'accesso IPMI remoto per tutti gli apparecchi che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello ai dispositivi StorageGRID a chiunque disponga di un account e di una password BMC. Se non è necessario l'accesso IPMI remoto al BMC, disabilitare questa opzione.

- Per controllare l'accesso IPMI remoto al BMC in Grid Manager, andare su **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza > Appliance**:
 - Deselezionare la casella di controllo **Abilita accesso IPMI remoto** per disabilitare l'accesso IPMI al BMC.
 - Selezionare la casella di controllo **Abilita accesso IPMI remoto** per abilitare l'accesso IPMI al BMC.

Configurazione del firewall

Come parte del processo di rafforzamento del sistema, è necessario rivedere le configurazioni del firewall esterno e modificarle in modo che il traffico venga accettato solo dagli indirizzi IP e sulle porte da cui è strettamente necessario.

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della griglia consentendo di controllare l'accesso di rete al nodo. Dovresti ["gestire i controlli del firewall interno"](#) per impedire l'accesso alla rete su tutte le porte, eccetto quelle necessarie per la distribuzione specifica della griglia. Le modifiche alla configurazione apportate nella pagina di controllo del firewall vengono distribuite a ciascun nodo.

Nello specifico, puoi gestire queste aree:

- **Indirizzi privilegiati**: puoi consentire a determinati indirizzi IP o subnet di accedere alle porte chiuse dalle impostazioni nella scheda Gestisci accesso esterno.
- **Gestisci accesso esterno**: puoi chiudere le porte aperte per impostazione predefinita o riaprire quelle chiuse in precedenza.
- **Rete client non attendibile**: è possibile specificare se un nodo si fida del traffico in entrata dalla rete client, nonché delle porte aggiuntive che si desidera aprire quando è configurata la rete client non attendibile.

Sebbene questo firewall interno fornisca 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"](#).

Disabilitare i servizi non utilizzati

Per tutti i nodi StorageGRID, è necessario disabilitare o bloccare l'accesso ai servizi non utilizzati. Ad esempio, se non si prevede di utilizzare DHCP, utilizzare Grid Manager per chiudere la porta 68. Selezionare **CONFIGURAZIONE > Controllo firewall > Gestisci accesso esterno**. Quindi modifica l'interruttore di stato per la porta 68 da **Aperto** a **Chiuso**.

Virtualizzazione, container e hardware condiviso

Per tutti i nodi StorageGRID , evitare di eseguire StorageGRID sullo stesso hardware fisico di software non attendibile. Non dare per scontato che le protezioni dell'hypervisor impediscano al malware di accedere ai dati protetti StorageGRID se sia StorageGRID che il malware sono presenti sullo stesso hardware fisico. Ad esempio, gli attacchi Meltdown e Spectre sfruttano vulnerabilità critiche nei processori moderni e consentono ai programmi di rubare dati nella memoria dello stesso computer.

Proteggere i nodi durante l'installazione

Non consentire agli utenti non attendibili di accedere ai nodi StorageGRID tramite la rete durante l'installazione dei nodi. I nodi non sono completamente sicuri finché non vengono uniti alla griglia.

Linee guida per i nodi di amministrazione

I nodi amministrativi forniscono servizi di gestione quali configurazione del sistema, monitoraggio e registrazione. Quando accedi a Grid Manager o a Tenant Manager, ti stai connettendo a un nodo di amministrazione.

Seguire queste linee guida per proteggere i nodi amministrativi nel sistema StorageGRID :

- Proteggere tutti i nodi amministrativi da client non attendibili, come quelli presenti su Internet aperto. Assicurarsi che nessun client non attendibile possa accedere a nessun nodo di amministrazione sulla rete Grid, sulla rete di amministrazione o sulla rete client.
- I gruppi StorageGRID controllano l'accesso alle funzionalità Grid Manager e Tenant Manager. Concedi a ciascun gruppo di utenti le autorizzazioni minime richieste per il loro ruolo e utilizza la modalità di accesso di sola lettura per impedire agli utenti di modificare la configurazione.
- Quando si utilizzano endpoint del bilanciamento del carico StorageGRID , utilizzare nodi gateway anziché nodi amministrativi per il traffico client non attendibile.
- Se hai tenant non attendibili, non consentire loro di accedere direttamente a Tenant Manager o all'API Tenant Management. In alternativa, fai in modo che tutti gli inquilini non attendibili utilizzino un portale per gli inquilini o un sistema di gestione degli inquilini esterno, che interagisca con l'API di gestione degli inquilini.
- Facoltativamente, utilizzare un proxy di amministrazione per un maggiore controllo sulla comunicazione AutoSupport dai nodi di amministrazione al supporto NetApp . Vedi i passaggi per ["creazione di un proxy amministratore"](#) .
- Facoltativamente, utilizzare le porte riservate 8443 e 9443 per separare le comunicazioni tra Grid Manager e Tenant Manager. Per una maggiore protezione, bloccare la porta condivisa 443 e limitare le richieste dei tenant alla porta 9443.
- Facoltativamente, utilizzare nodi amministrativi separati per gli amministratori della griglia e gli utenti tenant.

Per maggiori informazioni, consultare le istruzioni per ["amministrazione di StorageGRID"](#) .

Linee guida per i nodi di archiviazione

I nodi di archiviazione gestiscono e archiviano dati e metadati degli oggetti. Seguire queste linee guida per proteggere i nodi di archiviazione nel sistema StorageGRID .

- Non consentire ai client non attendibili di connettersi direttamente ai nodi di archiviazione. 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 i tenant non attendibili. Ad esempio, quando si crea un account per un tenant non attendibile, non consentire al tenant di utilizzare la propria origine identità e non consentire l'utilizzo dei servizi della piattaforma. Vedi i passaggi per ["creazione di un account inquilino"](#) .
- Utilizzare un bilanciatore del carico di terze parti per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre maggiore controllo e ulteriori livelli di protezione contro gli attacchi.
- Facoltativamente, utilizzare un proxy di archiviazione per un maggiore controllo sui pool di archiviazione cloud e sulla comunicazione dei servizi della piattaforma dai nodi di archiviazione ai servizi esterni. Vedi i passaggi per ["creazione di un proxy di archiviazione"](#) .
- Facoltativamente, è possibile connettersi ai servizi esterni tramite la rete client. Quindi, selezionare **CONFIGURAZIONE > Sicurezza > Controllo firewall > Reti client non attendibili** e indicare che la rete client sul nodo di archiviazione non è attendibile. Il nodo di archiviazione non accetta più traffico in entrata sulla rete client, ma continua a consentire richieste in uscita per i servizi della piattaforma.

Linee guida per i nodi gateway

I nodi gateway forniscono un'interfaccia di bilanciamento del carico opzionale che le applicazioni client possono utilizzare per connettersi a StorageGRID. Seguire queste linee guida per proteggere tutti i nodi gateway nel sistema StorageGRID :

- Configurare e utilizzare gli endpoint del bilanciatore del carico. Vedere ["Considerazioni sul bilanciamento del carico"](#) .
- Utilizzare un bilanciatore del carico di terze parti tra il client e il nodo gateway o i nodi di archiviazione per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre maggiore controllo e ulteriori livelli di protezione contro gli attacchi. Se si utilizza un bilanciatore del carico di terze parti, è comunque possibile configurare il traffico di rete in modo che passi attraverso un endpoint del bilanciatore del carico interno o venga inviato direttamente ai nodi di archiviazione.
- Se si utilizzano endpoint di bilanciamento del carico, è possibile fare in modo che i client si connettano tramite la rete client. Quindi, selezionare **CONFIGURAZIONE > Sicurezza > Controllo firewall > 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 configurate esplicitamente come endpoint del bilanciatore del carico.

Linee guida per i nodi degli apparecchi hardware

Gli apparecchi hardware StorageGRID sono progettati specificamente per l'uso in un sistema StorageGRID . Alcuni dispositivi possono essere utilizzati come nodi di archiviazione. Altri dispositivi possono essere utilizzati come nodi amministrativi o nodi gateway. È possibile combinare nodi appliance con nodi basati su software oppure implementare griglie completamente progettate per tutti gli appliance.

Seguire queste linee guida per proteggere tutti i nodi degli apparecchi hardware nel sistema StorageGRID :

- Se l'appliance utilizza SANtricity System Manager per la gestione del controller di archiviazione, impedire ai client non attendibili di accedere a SANtricity System Manager tramite la rete.
- Se l'appliance è dotata di un controller di gestione della scheda base (BMC), tenere presente che la porta di gestione BMC consente l'accesso hardware di basso livello. Collegare la porta di gestione BMC solo a una rete di gestione interna sicura e affidabile. Se non è disponibile alcuna rete di questo tipo, lasciare la porta di gestione BMC scollegata o bloccata, a meno che il supporto tecnico non richieda una connessione BMC .
- Se l'appliance supporta la gestione remota dell'hardware del controller tramite Ethernet utilizzando lo standard Intelligent Platform Management Interface (IPMI), bloccare il traffico non attendibile sulla porta 623.



È possibile abilitare o disabilitare l'accesso IPMI remoto per tutti gli apparecchi che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello ai dispositivi StorageGRID a chiunque disponga di un account e di una password BMC. Se non è necessario l'accesso IPMI remoto al BMC, disabilitare questa opzione utilizzando uno dei seguenti metodi:

- + In Grid Manager, andare su **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza > Appliance** e deselezionare la casella di controllo **Abilita accesso IPMI remoto**.
- + Nell'API di gestione della griglia, utilizzare l'endpoint privato: `PUT /private/bmc`.

- Per i modelli di appliance contenenti unità SED, FDE o FIPS NL-SAS gestite con SANtricity System Manager, ["abilitare e configurare SANtricity Drive Security"](#).
- Per i modelli di appliance contenenti SSD SED o FIPS NVMe gestiti tramite StorageGRID Appliance Installer e Grid Manager, ["abilitare e configurare la crittografia dell'unità StorageGRID"](#).
- Per gli apparecchi senza unità SED, FDE o FIPS, abilitare e configurare la crittografia del nodo software StorageGRID ["utilizzando un server di gestione delle chiavi \(KMS\)"](#).

Linee guida per il rafforzamento di TLS e SSH

È necessario sostituire i certificati predefiniti creati durante l'installazione e selezionare la policy di sicurezza appropriata per le connessioni TLS e SSH.

Linee guida per il rafforzamento dei certificati

Dovresti sostituire i certificati predefiniti creati durante l'installazione con i tuoi 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 firmato da una CA da utilizzare per l'autenticazione StorageGRID.

Nello specifico, dovresti utilizzare certificati server personalizzati anziché questi 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:** utilizzato per proteggere l'accesso ai nodi di archiviazione e ai nodi gateway, che le applicazioni client S3 utilizzano 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 bilanciatore del carico. Per configurare i certificati del bilanciatore del carico, vedere ["Configurare gli endpoint del bilanciatore del carico"](#).

Quando si utilizzano certificati server personalizzati, seguire queste linee guida:

- I certificati dovrebbero avere un `subjectAltName` che corrisponde alle voci DNS per StorageGRID. Per i dettagli, vedere la sezione 4.2.1.6, "Nome alternativo dell'oggetto", in ["RFC 5280: Certificato PKIX e profilo CRL"](#).
- Se possibile, evitare l'uso di certificati jolly. Un'eccezione a questa linea guida è il certificato per un endpoint in stile host virtuale S3, che richiede l'uso di un carattere jolly se i nomi dei bucket non sono noti in anticipo.
- Quando è necessario utilizzare caratteri jolly nei certificati, è opportuno adottare misure aggiuntive per

ridurre i rischi. Utilizzare un modello jolly come `*.s3.example.com` e non usare il `s3.example.com` suffisso per altre applicazioni. Questo modello funziona anche con l'accesso S3 in stile percorso, come `dc1-s1.s3.example.com/mybucket`.

- Imposta tempi di scadenza dei certificati brevi (ad esempio, 2 mesi) e utilizza l'API Grid Management per automatizzare la rotazione dei certificati. Ciò è particolarmente importante per i certificati jolly.

Inoltre, i client devono utilizzare un controllo rigoroso del nome host quando comunicano con StorageGRID.

Linee guida per il rafforzamento della politica TLS e SSH

È possibile selezionare una policy di sicurezza per determinare quali protocolli e cifrari vengono utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure con i servizi StorageGRID interni.

La policy di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. Come buona pratica, dovresti disabilitare le opzioni di crittografia non necessarie per la compatibilità dell'applicazione. Utilizzare il criterio Modern predefinito, a meno che il sistema non debba essere conforme ai Common Criteria o non sia necessario utilizzare altri cifrari.

Vedere "[Gestire la politica TLS e SSH](#)" per dettagli e istruzioni.

Altre linee guida per il rafforzamento

Oltre a seguire le linee guida di rafforzamento per le reti e i nodi StorageGRID, è necessario seguire anche le linee guida di rafforzamento per altre aree del sistema StorageGRID.

Password di installazione temporanea

Per proteggere il sistema StorageGRID durante l'installazione, impostare una password nella pagina della password temporanea del programma di installazione nell'interfaccia utente di installazione StorageGRID o nell'API di installazione. Se impostata, questa password si applica a tutti i metodi di installazione StorageGRID, inclusa l'interfaccia utente, l'API di installazione e `configure-storagegrid.py` sceneggiatura.

Per maggiori informazioni, fare riferimento a:

- "[Installa StorageGRID su Red Hat Enterprise Linux](#)"
- "[Installa StorageGRID su Ubuntu o Debian](#)"
- "[Installa StorageGRID su VMware](#)"
- "[Installare l'appliance StorageGRID](#)"

Registri e messaggi di controllo

Proteggere sempre in modo sicuro i registri StorageGRID e l'output dei messaggi di controllo. I registri e i messaggi di controllo StorageGRID forniscono informazioni preziose dal punto di vista del supporto e della disponibilità del sistema. Inoltre, le informazioni e i dettagli contenuti nei log StorageGRID e nell'output dei messaggi di controllo 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.

Vedi il "[Riferimento ai file di registro](#)" per ulteriori informazioni sui log StorageGRID. Vedere "[Messaggi di](#)

[controllo](#)" per ulteriori informazioni sui messaggi di controllo StorageGRID .

AutoSupport NetApp

La funzionalità AutoSupport di StorageGRID consente di monitorare in modo proattivo lo stato del sistema e di inviare automaticamente pacchetti al sito di supporto NetApp , al team di supporto interno della tua organizzazione o a un partner di supporto. Per impostazione predefinita, l'invio di pacchetti AutoSupport a NetApp è abilitato quando StorageGRID viene configurato per la prima volta.

La funzione AutoSupport può essere disattivata. Tuttavia, NetApp consiglia di abilitarlo perché AutoSupport aiuta ad accelerare l'identificazione e la risoluzione dei problemi nel caso in cui si verifichino 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 dei pacchetti AutoSupport a NetApp.

Condivisione delle risorse tra origini (CORS)

È possibile configurare la condivisione delle risorse tra origini (CORS) per un bucket S3 se si desidera che il bucket e gli oggetti in esso contenuti siano accessibili alle applicazioni Web in altri domini. In generale, non abilitare CORS a meno che non sia necessario. Se CORS è richiesto, limitarlo alle origini attendibili.

Vedi i passaggi per "[configurazione della condivisione delle risorse tra origini \(CORS\)](#)" .

Dispositivi di sicurezza esterni

Una soluzione di rafforzamento completa deve tenere conto dei meccanismi di sicurezza esterni a StorageGRID. L'utilizzo di dispositivi infrastrutturali aggiuntivi per filtrare e limitare l'accesso a StorageGRID è un modo efficace per stabilire e mantenere un rigoroso livello di sicurezza. 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 l'uso di un bilanciatore del carico di terze parti. Il bilanciamento del carico di terze parti offre maggiore controllo e ulteriori livelli di protezione contro gli attacchi.

Mitigazione del ransomware

Aiuta a proteggere i dati dei tuoi oggetti dagli attacchi ransomware seguendo i consigli in "[Difesa dal ransomware con StorageGRID](#)" .

Configurare StorageGRID per FabricPool

Configurare StorageGRID per FabricPool

Se si utilizza il software NetApp ONTAP , è possibile utilizzare NetApp FabricPool per suddividere i dati inattivi in un sistema di archiviazione di oggetti NetApp StorageGRID .

Utilizzare 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 archiviazione di oggetti StorageGRID per l'utilizzo con FabricPool.

- Scopri come fornire i valori richiesti a ONTAP quando colleghi StorageGRID come livello cloud FabricPool .

Guida rapida per la configurazione di StorageGRID per FabricPool

1

Pianifica la tua configurazione

- Decidi quale criterio di suddivisione in livelli del volume FabricPool utilizzerai per suddividere in livelli i dati ONTAP inattivi in StorageGRID.
- Pianifica e installa un sistema StorageGRID per soddisfare le tue esigenze di capacità di archiviazione e prestazioni.
- Acquisire familiarità con il software di sistema StorageGRID , incluso il ["Responsabile della griglia"](#) e il ["Responsabile degli inquilini"](#) .
- Esaminare le best practice di FabricPool per ["gruppi HA"](#) , ["bilanciamento del carico"](#) , ["ILM"](#) , E ["Di più"](#) .
- Consultare queste risorse aggiuntive, che forniscono dettagli sull'utilizzo e la configurazione ONTAP e FabricPool:

["TR-4598: Migliori pratiche FabricPool in ONTAP"](#)

["Documentazione ONTAP per FabricPool"](#)

2

Eeguire le attività prerequisito

Ottieni il ["informazioni necessarie per collegare StorageGRID come livello cloud"](#) , tra cui:

- indirizzi IP
- Nomi di dominio
- Certificato SSL

Facoltativamente, configurare ["federazione di identità"](#) E ["accesso unico"](#) .

3

Configurare le impostazioni StorageGRID

Utilizzare StorageGRID per ottenere i valori di cui ONTAP ha bisogno per connettersi alla rete.

Utilizzando il ["Procedura guidata di configurazione FabricPool"](#) è il metodo consigliato e più veloce per configurare tutti gli elementi, ma è anche possibile configurare manualmente ogni entità, se necessario.

4

Configurare ONTAP e DNS

Utilizzare ONTAP per ["aggiungere un livello cloud"](#) che utilizza i valori StorageGRID . Poi, ["configurare le voci DNS"](#) per associare gli indirizzi IP a qualsiasi nome di dominio che intendi utilizzare.

5

Monitorare e gestire

Quando il sistema è attivo e funzionante, esegui attività continue in ONTAP e StorageGRID per gestire e monitorare la suddivisione in livelli dei dati FabricPool nel tempo.

Che cos'è FabricPool?

FabricPool è una soluzione di storage ibrida ONTAP che utilizza un aggregato flash ad alte prestazioni come livello di prestazioni e un archivio di oggetti come livello cloud. Utilizzando aggregati abilitati per FabricPool è possibile ridurre i costi di archiviazione senza compromettere prestazioni, efficienza o protezione.

FabricPool associa un livello cloud (un archivio di oggetti esterno, come StorageGRID) a un livello locale (un aggregato di archiviazione ONTAP) per creare una raccolta composita di dischi. I volumi all'interno di FabricPool possono quindi sfruttare la suddivisione in livelli mantenendo i dati attivi (hot) su un archivio ad alte prestazioni (il livello locale) e disattivando i dati (cold) nell'archivio oggetti esterno (il livello cloud).

Non sono necessarie modifiche architettoniche e puoi continuare a gestire i tuoi dati e l'ambiente applicativo dal sistema di archiviazione centrale ONTAP.

Che cos'è StorageGRID?

NetApp StorageGRID è un'architettura di storage che gestisce i dati come oggetti, a differenza di altre architetture di storage come l'archiviazione di file o di blocchi. Gli oggetti vengono conservati all'interno di un singolo contenitore (ad esempio un bucket) e non sono annidati come file all'interno di una directory all'interno di altre directory. Sebbene l'archiviazione di oggetti offra generalmente prestazioni inferiori rispetto all'archiviazione di file o blocchi, è significativamente più scalabile. I bucket StorageGRID possono contenere petabyte di dati e miliardi di oggetti.

Perché utilizzare StorageGRID come livello cloud FabricPool ?

FabricPool può suddividere i dati ONTAP in livelli per diversi provider di archiviazione di oggetti, tra cui StorageGRID. A differenza dei cloud pubblici che potrebbero impostare un numero massimo di operazioni di input/output supportate al secondo (IOPS) a livello di bucket o contenitore, le prestazioni StorageGRID variano in base al numero di nodi in un sistema. Utilizzando StorageGRID come livello cloud FabricPool puoi conservare i tuoi dati inattivi nel tuo cloud privato, per ottenere le massime prestazioni e il controllo completo sui tuoi dati.

Inoltre, non è richiesta una licenza FabricPool quando si utilizza StorageGRID come livello cloud.

Informazioni necessarie per collegare StorageGRID come livello 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?

Nella tabella seguente vengono mostrati i valori che è necessario configurare in StorageGRID e come 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 bilanciatore del carico	ONTAP System Manager > Aggiungi livello cloud

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Certificato SSL	StorageGRID > Endpoint del bilanciatore del carico	ONTAP System Manager > Aggiungi livello cloud
Nome del server (FQDN)	StorageGRID > Endpoint del bilanciatore del carico	voce DNS
ID chiave di accesso e chiave di accesso segreta	StorageGRID > Tenant e bucket	ONTAP System Manager > Aggiungi livello cloud
Nome del bucket/contenitore	StorageGRID > Tenant e bucket	ONTAP System Manager > Aggiungi livello cloud

Come posso ottenere questi valori?

A seconda delle tue esigenze, puoi procedere in uno dei seguenti modi per ottenere le informazioni di cui hai bisogno:

- Utilizzare il ["Procedura guidata di configurazione FabricPool"](#) . La procedura guidata di configurazione FabricPool consente di configurare rapidamente i valori richiesti in StorageGRID e genera un file che è possibile utilizzare per configurare ONTAP System Manager. La procedura guidata ti guida attraverso i passaggi necessari e ti aiuta a verificare che le tue impostazioni siano conformi alle best practice StorageGRID e FabricPool .
- Configurare manualmente ogni elemento. Quindi, immettere i valori in ONTAP System Manager o in ONTAP CLI. Segui questi passaggi:
 - a. ["Configurare un gruppo ad alta disponibilità \(HA\) per FabricPool"](#) .
 - b. ["Creare un endpoint del bilanciatore del carico per FabricPool"](#) .
 - c. ["Crea un account tenant per FabricPool"](#) .
 - d. Sign in all'account tenant e ["creare il bucket e le chiavi di accesso per l'utente root"](#) .
 - e. Crea una regola ILM per i dati FabricPool e aggiungila ai tuoi criteri ILM attivi. Vedere ["Configurare ILM per i dati FabricPool"](#) .
 - f. Facoltativamente, ["creare una politica di classificazione del traffico per FabricPool"](#) .

Utilizzare la procedura guidata di configurazione FabricPool

Utilizzare la procedura guidata di configurazione FabricPool : considerazioni e requisiti

È possibile utilizzare la procedura guidata di configurazione FabricPool per configurare StorageGRID come sistema di archiviazione degli oggetti per un livello cloud FabricPool . Dopo aver completato la procedura guidata di configurazione, è possibile immettere i dettagli richiesti in ONTAP System Manager.

Quando utilizzare la procedura guidata di configurazione FabricPool

La procedura guidata di configurazione FabricPool ti guida attraverso ogni fase della configurazione di StorageGRID per l'utilizzo con FabricPool e configura automaticamente determinate entità, come ILM e criteri di classificazione del traffico. Per completare la procedura guidata, è necessario scaricare un file che è

possibile utilizzare per immettere valori in ONTAP System Manager. Utilizza la procedura guidata per configurare il sistema più rapidamente e per assicurarti che le impostazioni siano conformi alle best practice StorageGRID e FabricPool .

Supponendo di disporre dell'autorizzazione di accesso Root, è possibile completare la procedura guidata di configurazione FabricPool quando si inizia a utilizzare StorageGRID Grid Manager oppure è possibile accedere e completare la procedura guidata in qualsiasi momento successivo. A seconda delle esigenze, è anche possibile configurare manualmente alcuni o tutti gli elementi richiesti e quindi utilizzare la procedura guidata per assemblare i valori di cui ONTAP ha bisogno in un unico file.



Utilizzare la procedura guidata di configurazione FabricPool a meno che non si abbiano requisiti particolari o che l'implementazione richieda una personalizzazione significativa.

Prima di utilizzare la procedura guidata

Conferma di aver completato questi passaggi preliminari.

Esaminare le migliori pratiche

- Hai una comprensione generale del ["informazioni necessarie per collegare StorageGRID come livello cloud"](#) .
- Hai esaminato le best practice FabricPool per:
 - ["Gruppi ad alta disponibilità \(HA\)"](#)
 - ["Bilanciamento del carico"](#)
 - ["Regole e politica ILM"](#)

Ottenere indirizzi IP e configurare le interfacce VLAN

Se si configura un gruppo HA, si sa a quali nodi si conetterà ONTAP e quale rete StorageGRID verrà utilizzata. Si sa anche quali valori immettere per il CIDR della subnet, l'indirizzo IP del gateway e gli indirizzi IP virtuali (VIP).

Se si prevede di utilizzare una LAN virtuale per separare il traffico FabricPool , è già stata configurata l'interfaccia VLAN. Vedere ["Configurare le interfacce VLAN"](#) .

Configurare la federazione delle identità e SSO

Se intendi utilizzare la federazione delle identità o l'accesso singolo (SSO) per il tuo sistema StorageGRID , hai abilitato queste funzionalità. Si sa anche quale gruppo federato dovrebbe avere accesso root per l'account tenant che ONTAP utilizzerà. Vedere ["Utilizzare la federazione delle identità"](#) E ["Configurare l'accesso singolo"](#) .

Ottieni e configura i nomi di dominio

- Sai quale nome di dominio completo (FQDN) utilizzare per StorageGRID. Le voci del server dei nomi di dominio (DNS) mapperanno questo FQDN agli indirizzi IP virtuali (VIP) del gruppo HA creato tramite la procedura guidata. Vedere ["Configurare il server DNS"](#) .
- Se si prevede di utilizzare richieste in stile host virtuale S3, è necessario ["nomi di dominio endpoint S3 configurati"](#) . Per impostazione predefinita, ONTAP utilizza URL in stile percorso, ma si consiglia di utilizzare richieste in stile virtual hosted.

Esaminare i requisiti del bilanciatore del carico e del certificato di sicurezza

Se si prevede di utilizzare il bilanciatore del carico StorageGRID , è necessario aver esaminato le informazioni generali ["considerazioni per il bilanciamento del carico"](#) . Hai i certificati che caricherai o i valori necessari per generare un certificato.

Se si prevede di utilizzare un endpoint di bilanciamento del carico esterno (di terze parti), è necessario disporre del nome di dominio completo (FQDN), della porta e del certificato per tale bilanciatore del carico.

Confermare la configurazione del pool di archiviazione ILM

se inizialmente hai installato StorageGRID 11.6 o una versione precedente, hai configurato il pool di archiviazione che utilizzerai. In generale, dovresti creare un pool di archiviazione per ogni sito StorageGRID che utilizzerai per archiviare i dati ONTAP .



Questo prerequisito non si applica se inizialmente è stato installato StorageGRID 11.7 o 11.8. Quando si installa inizialmente una di queste versioni, vengono creati automaticamente dei pool di archiviazione per ogni sito.

Relazione tra ONTAP e il livello cloud StorageGRID

La procedura guidata FabricPool ti guida attraverso il processo di creazione di un singolo livello cloud StorageGRID che include un tenant StorageGRID , un set di chiavi di accesso e un bucket StorageGRID . È possibile collegare questo livello cloud StorageGRID a uno o più livelli locali ONTAP .

La prassi migliore in generale è quella di collegare un singolo livello cloud a più livelli locali in un cluster. Tuttavia, a seconda delle esigenze, potresti voler utilizzare più di un bucket o addirittura più di un tenant StorageGRID per i livelli locali in un singolo cluster. L'utilizzo di bucket e tenant diversi consente di isolare i dati e l'accesso ai dati tra i livelli locali ONTAP , ma è un po' più complesso da configurare e gestire.

NetApp sconsiglia di collegare un singolo livello cloud a livelli locali in più cluster.



Per le best practice per l'utilizzo di StorageGRID con NetApp MetroCluster™ e FabricPool Mirror, vedere ["TR-4598: Migliori pratiche FabricPool in ONTAP"](#) .

Facoltativo: utilizzare un bucket diverso per ogni livello locale

Per utilizzare più di un bucket per i livelli locali in un cluster ONTAP , aggiungere più di un livello cloud StorageGRID in ONTAP. Ogni livello cloud condivide lo stesso gruppo HA, endpoint del bilanciatore del carico, tenant e chiavi di accesso, ma utilizza un contenitore diverso (bucket StorageGRID). Seguire questi passaggi generali:

1. Da StorageGRID Grid Manager, completare la procedura guidata di configurazione FabricPool per il primo livello cloud.
2. Da ONTAP System Manager, aggiungi un livello cloud e utilizza il file scaricato da StorageGRID per fornire i valori richiesti.
3. Da StorageGRID Tenant Manager, accedi al tenant creato dalla procedura guidata e crea un secondo bucket.
4. Completare nuovamente la procedura guidata FabricPool . Selezionare il gruppo HA esistente, l'endpoint del bilanciatore del carico e il tenant. Quindi, seleziona il nuovo bucket che hai creato manualmente. Crea una nuova regola ILM per il nuovo bucket e attiva un criterio ILM per includere tale regola.
5. Da ONTAP, aggiungi un secondo livello cloud ma fornisci il nome del nuovo bucket.

Facoltativo: utilizzare un tenant e un bucket diversi per ogni livello locale

Per utilizzare più di un tenant e diversi set di chiavi di accesso per i livelli locali in un cluster ONTAP , aggiungere più di un livello cloud StorageGRID in ONTAP. Ogni livello cloud condivide lo stesso gruppo HA, lo stesso endpoint del bilanciatore del carico, ma utilizza un tenant, chiavi di accesso e un contenitore (bucket StorageGRID) diversi. Seguire questi passaggi generali:

1. Da StorageGRID Grid Manager, completare la procedura guidata di configurazione FabricPool per il primo livello cloud.
2. Da ONTAP System Manager, 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 bilanciatore del carico. Crea un nuovo tenant e un nuovo bucket. Crea una nuova regola ILM per il nuovo bucket e attiva 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.

Accedi e completa la procedura guidata di configurazione FabricPool

È possibile utilizzare la procedura guidata di configurazione FabricPool per configurare StorageGRID come sistema di archiviazione degli oggetti per un livello cloud FabricPool .

Prima di iniziare

- Hai esaminato il "[considerazioni e requisiti](#)" per utilizzare la procedura guidata di configurazione FabricPool .



Se si desidera configurare StorageGRID per l'utilizzo con qualsiasi altra applicazione client S3, andare a "[Utilizzare la procedura guidata di configurazione S3](#)" .

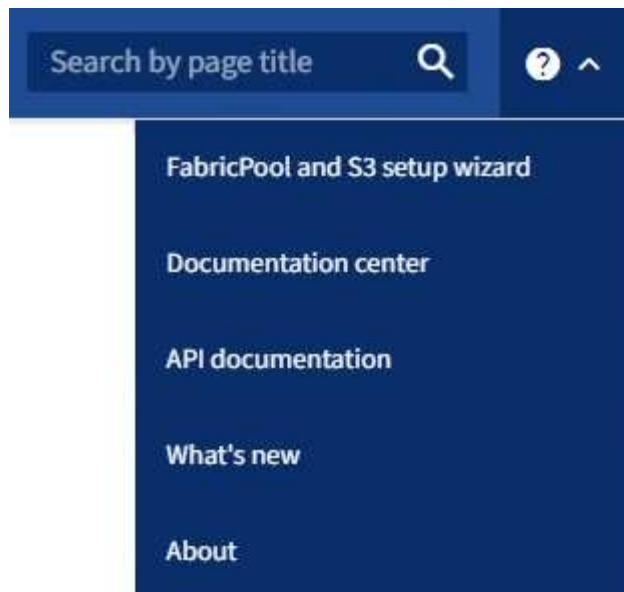
- Tu hai il "[Permesso di accesso root](#)" .

Accedi alla procedura guidata

È possibile completare la procedura guidata di configurazione FabricPool quando si inizia a utilizzare StorageGRID Grid Manager oppure è possibile accedere e completare la procedura guidata in qualsiasi momento successivo.

Passi

1. Sign in a Grid Manager utilizzando un "[browser web supportato](#)" .
2. Se nella dashboard viene visualizzato il banner **Procedura guidata di configurazione FabricPool e S3**, selezionare il collegamento nel banner. Se il banner non viene più visualizzato, seleziona l'icona della guida dalla barra dell'intestazione in Grid Manager e seleziona **Procedura guidata di configurazione di FabricPool e S3**.



3. Nella sezione FabricPool della pagina della procedura guidata di configurazione FabricPool e S3, seleziona **Configura ora**.

Viene visualizzato **Passaggio 1 di 9: Configura gruppo HA**.

Passaggio 1 di 9: configurare il gruppo HA

Un gruppo ad alta disponibilità (HA) è una raccolta di nodi, ciascuno dei quali contiene il servizio StorageGRID Load Balancer. Un gruppo HA può contenere nodi gateway, nodi amministrativi 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 fallisce, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool

Per i dettagli su questa attività, vedere "[Gestire gruppi ad alta disponibilità](#)" E "[Procedure consigliate per i gruppi ad alta disponibilità](#)".

Passi

1. Se si prevede di utilizzare un bilanciatore del carico esterno, non è necessario creare un gruppo HA. Seleziona **Salta questo passaggio** e vai a [Passaggio 2 di 9: configurare l'endpoint del bilanciatore del carico](#) .
2. Per utilizzare il bilanciatore del carico StorageGRID , creare un nuovo gruppo HA o utilizzare un gruppo HA esistente.

Crea gruppo HA

- a. Per creare un nuovo gruppo HA, seleziona **Crea gruppo HA**.
- b. Per la fase **Inserisci dettagli**, compila i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome visualizzato univoco per questo gruppo HA.
Descrizione (facoltativa)	Descrizione di questo gruppo HA.

- c. Per il passaggio **Aggiungi interfacce**, seleziona le interfacce del nodo che desideri utilizzare in questo gruppo HA.

Utilizzare le intestazioni di colonna per ordinare le righe oppure immettere un termine di ricerca per individuare più rapidamente le interfacce.

È possibile selezionare uno o più nodi, ma è possibile selezionare solo un'interfaccia per ciascun nodo.

- d. Per il passaggio **Assegna priorità alle interfacce**, determinare l'interfaccia primaria e tutte 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 primaria 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 funziona, gli indirizzi IP virtuali (VIP) vengono spostati sulla prima interfaccia di backup in ordine di priorità. Se tale interfaccia non funziona, gli indirizzi VIP vengono spostati alla successiva interfaccia di backup e così via. Una volta risolti i guasti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

- e. Per il passaggio **Inserisci indirizzi IP**, compila i seguenti campi.

Campo	Descrizione
CIDR di sottorete	L'indirizzo della subnet VIP in notazione CIDR: un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere alcun bit host impostato. Ad esempio, 192.16.0.0/22.
Indirizzo IP del gateway (facoltativo)	Opzionale. Se gli indirizzi IP ONTAP utilizzati per accedere a StorageGRID non si trovano sulla stessa subnet degli indirizzi VIP StorageGRID, immettere l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve essere all'interno della subnet VIP.

Campo	Descrizione
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 saranno tutti attivi contemporaneamente sull'interfaccia attiva. Almeno un indirizzo deve essere IPv4. Facoltativamente, è possibile specificare indirizzi IPv4 e IPv6 aggiuntivi.

f. Selezionare **Crea gruppo HA** e quindi **Fine** per tornare alla procedura guidata di configurazione FabricPool .

g. Selezionare **Continua** per passare alla fase di bilanciamento del carico.

Utilizzare il gruppo HA esistente

a. Per utilizzare un gruppo HA esistente, seleziona il nome del gruppo HA dall'elenco a discesa **Seleziona un gruppo HA**.

b. Selezionare **Continua** per passare alla fase di bilanciamento del carico.

Passaggio 2 di 9: configurare l'endpoint del bilanciatore del carico

StorageGRID utilizza un bilanciatore 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 su più nodi di archiviazione.

È possibile utilizzare il servizio StorageGRID Load Balancer, presente su tutti i nodi gateway e amministrativi, oppure connettersi a un bilanciatore del carico esterno (di terze parti). Si consiglia di utilizzare il bilanciatore del carico StorageGRID .

Per i dettagli su questa attività, vedere la sezione generale ["considerazioni per il bilanciamento del carico"](#) e il ["best practice per il bilanciamento del carico per FabricPool"](#) .

Passi

1. Selezionare o creare un endpoint del bilanciatore del carico StorageGRID oppure utilizzare un bilanciatore del carico esterno.

Crea endpoint

- a. Selezionare **Crea endpoint**.
- b. Per il passaggio **Inserisci i dettagli dell'endpoint**, compila 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 impostato su 10433 per il primo endpoint creato, ma è possibile immettere qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, perché queste porte sono riservate sui nodi amministrativi. Nota: non sono consentite le porte utilizzate da altri servizi di rete. Vedi il "Riferimento porta di rete" .
Tipo di cliente	Deve essere S3 .
Protocollo di rete	Selezionare HTTPS. Nota: la comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

- c. Per il passaggio **Seleziona modalità di associazione**, specificare la modalità di associazione. La modalità di associazione controlla il modo in cui si accede all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (predefinito)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo HA su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione Globale (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 il corrispondente FQDN) di un gruppo HA. Gli endpoint con questa modalità di associazione possono utilizzare tutti lo stesso numero di porta, purché i gruppi HA selezionati per gli endpoint non si sovrappongano.
Interfacce dei nodi	Per accedere a questo endpoint, i client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionati.

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 oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway per accedere a questo endpoint.

d. Per il passaggio **Accesso tenant**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket. Consenti tutti i tenant è quasi sempre l'opzione appropriata per l'endpoint del bilanciatore del carico utilizzato per FabricPool. È necessario selezionare questa opzione se si utilizza la procedura guidata di configurazione FabricPool per un nuovo sistema StorageGRID e non è ancora stato creato alcun account tenant.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai propri bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

e. Per il passaggio **Allega certificato**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Carica il certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato da una CA, una chiave privata del certificato e un bundle CA facoltativo.
Genera certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciatore del carico" per i dettagli su cosa inserire.
Utilizzare il certificato StorageGRID S3	Questa opzione è disponibile solo se hai già caricato o generato una versione personalizzata del certificato globale StorageGRID . Vedere "Configurare i certificati API S3" per i dettagli.

f. Selezionare **Fine** per tornare alla procedura guidata di configurazione FabricPool .

g. Selezionare **Continua** per passare alla fase tenant e bucket.



Le modifiche al certificato di un endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Utilizzare l'endpoint del bilanciatore del carico esistente

- a. Selezionare il nome di un endpoint esistente dall'elenco a discesa **Seleziona un endpoint del bilanciatore del carico**.
- b. Selezionare **Continua** per passare alla fase tenant e bucket.

Utilizzare un bilanciatore di carico esterno

- a. Compilare i seguenti campi per il bilanciatore del carico esterno.

Campo	Descrizione
Nome di dominio completo	Nome di dominio completo (FQDN) del bilanciatore del carico esterno.
Porta	Numero di porta che FabricPool utilizzerà per connettersi al bilanciatore del carico esterno.
Certificato	Copiare il certificato del server per il bilanciatore del carico esterno e incollarlo in questo campo.

- b. Selezionare **Continua** per passare alla fase tenant e bucket.

Fase 3 di 9: Inquilino e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per archiviare e recuperare oggetti in StorageGRID. Ogni tenant ha i propri 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 verrà utilizzato FabricPool .

Un bucket è un contenitore utilizzato per archiviare gli oggetti e i metadati degli oggetti di un tenant. Sebbene alcuni tenant possano avere molti bucket, la procedura guidata consente di creare o selezionare solo un tenant e un bucket alla volta. In seguito potrai utilizzare Tenant Manager per aggiungere altri bucket di cui hai bisogno.

È possibile creare un nuovo tenant e un nuovo bucket da utilizzare in 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 i dettagli su questa attività, vedere ["Crea un account tenant per FabricPool"](#) E ["Crea un bucket S3 e ottieni una chiave di accesso"](#) .

Passi

Crea un nuovo tenant e un nuovo bucket oppure seleziona un tenant esistente.

Nuovo inquilino e secchio

1. Per creare un nuovo tenant e un nuovo bucket, immettere un **Nome tenant**. Ad esempio, `FabricPool tenant`.
2. Definisci l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del sistema StorageGRID "federazione di identità", "accesso unico (SSO)", o entrambi.

Opzione	Fai questo
Se la federazione delle identità non è abilitata	Specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se la federazione delle identità è abilitata	a. Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se sono abilitati sia la federazione delle identità che il Single Sign-On (SSO)	Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. Nessun utente locale può effettuare l'accesso.

3. Per **Nome bucket**, immettere il nome del bucket che FabricPool utilizzerà per archiviare i dati ONTAP. Ad esempio, `fabricpool-bucket`.



Non è possibile modificare il nome del bucket dopo averlo creato.

4. Seleziona la **Regione** per questo bucket.

Utilizza la regione predefinita (`us-east-1`) a meno che non si preveda di utilizzare ILM in futuro per filtrare gli oggetti in base alla regione del bucket.

5. Selezionare **Crea e continua** per creare il tenant e il bucket e per passare alla fase di download dei dati

Seleziona inquilino e bucket

L'account tenant esistente deve avere almeno un bucket in cui non è abilitato il controllo delle versioni. Non è possibile selezionare un account tenant esistente se non esiste alcun bucket per quel tenant.

1. Selezionare il tenant esistente dall'elenco a discesa **Nome del tenant**.
2. Selezionare il bucket esistente dall'elenco a discesa **Nome bucket**.

FabricPool non supporta il controllo delle versioni degli oggetti, pertanto i bucket in cui il controllo delle versioni è abilitato non vengono visualizzati.



Non selezionare un bucket in cui è abilitato S3 Object Lock per l'utilizzo con FabricPool.

3. Selezionare **Continua** per passare alla fase di download dei dati.

Passaggio 4 di 9: Scarica le impostazioni ONTAP

Durante questa fase, scaricherai un file che potrai utilizzare per immettere valori in ONTAP System Manager.

Passi

1. Facoltativamente, seleziona 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 scaricato, ma potresti volerli salvare 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 archiviazione degli oggetti per un livello cloud FabricPool , tra cui:

- Dettagli sulla connessione del bilanciatore del carico, inclusi il nome del server (FQDN), la porta e il certificato
- Nome del bucket
- ID 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 un luogo sicuro.



Non chiudere questa pagina finché non hai copiato entrambe le chiavi di accesso, scaricato le impostazioni ONTAP o entrambe le cose. Le chiavi non saranno più disponibili dopo aver chiuso questa pagina. Assicuratevi di salvare queste informazioni in un luogo sicuro, perché possono essere utilizzate per ottenere dati dal vostro sistema StorageGRID .

4. Seleziona 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 al passaggio relativo al pool di archiviazione ILM.

Passaggio 5 di 9: selezionare un pool di archiviazione

Un pool di archiviazione è un gruppo di nodi di archiviazione. Quando si seleziona un pool di archiviazione, si determinano quali nodi StorageGRID utilizzerà per archiviare i dati suddivisi in livelli da ONTAP.

Per i dettagli su questo passaggio, vedere ["Creare un pool di archiviazione"](#) .

Passi

1. Dall'elenco a discesa **Sito**, seleziona il sito StorageGRID che desideri utilizzare per i dati suddivisi in livelli da ONTAP.
2. Dall'elenco a discesa **Pool di archiviazione**, selezionare il pool di archiviazione per quel sito.

Il pool di archiviazione per un sito include tutti i nodi di archiviazione presenti in quel sito.

3. Selezionare **Continua** per passare alla fase della regola ILM.

Passaggio 6 di 9: rivedere la regola ILM per FabricPool

Le regole di gestione del ciclo di vita delle informazioni (ILM) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel sistema StorageGRID .

La procedura guidata di configurazione FabricPool crea automaticamente la regola ILM consigliata per l'utilizzo FabricPool . Questa regola si applica solo al bucket specificato. Utilizza la codifica di cancellazione 2+1 in un singolo sito per memorizzare i dati suddivisi in livelli da ONTAP.

Per i dettagli su questo passaggio, vedere ["Crea regola ILM"](#) E ["Procedure consigliate per l'utilizzo di ILM con i dati FabricPool"](#) .

Passi

1. Rivedi i dettagli della regola.

Campo	Descrizione
Nome della regola	Generato automaticamente e non può essere modificato
Descrizione	Generato automaticamente e non può essere modificato
Filtro	Il nome del bucket Questa regola si applica solo agli oggetti salvati nel bucket specificato.
Tempo di riferimento	Tempo di ingestione Le istruzioni di posizionamento iniziano quando gli oggetti vengono salvati inizialmente nel bucket.
Istruzioni per il posizionamento	Utilizzare la codifica di cancellazione 2+1

2. Ordinare il diagramma di conservazione in base a **Periodo di tempo** e **Pool di archiviazione** per confermare le istruzioni di posizionamento.
 - Il **periodo di tempo** per la regola è **Giorno 0 - per sempre**. **Giorno 0** significa che la regola viene applicata quando i dati vengono suddivisi in livelli da ONTAP. **Per sempre** significa che StorageGRID ILM non eliminerà i dati che sono stati suddivisi in livelli da ONTAP.
 - Il **pool di archiviazione** per la regola è il pool di archiviazione selezionato. **EC 2+1** significa 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 archiviazione in un unico sito.
3. Selezionare **Crea e continua** per creare questa regola e passare alla fase relativa alla policy ILM.

Passaggio 7 di 9: rivedere e attivare la policy ILM

Dopo che la procedura guidata di configurazione FabricPool ha creato la regola ILM per l'utilizzo FabricPool , crea un criterio ILM. È necessario simulare e rivedere attentamente questa politica prima di attivarla.

Per i dettagli su questo passaggio, vedere ["Crea policy ILM"](#) E ["Procedure consigliate per l'utilizzo di ILM con i dati FabricPool"](#) .



Quando si attiva una nuova policy ILM, StorageGRID utilizza tale policy 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 una nuova policy può comportare lo spostamento di oggetti esistenti in nuove posizioni.



Per evitare la perdita di dati, non utilizzare una regola ILM che farà scadere o eliminerà i dati del livello cloud FabricPool. Impostare il periodo di conservazione su **per sempre** per garantire che gli oggetti FabricPool non vengano eliminati da StorageGRID ILM.

Passi

1. Facoltativamente, aggiornare il **Nome criterio** generato dal sistema. Per impostazione predefinita, il sistema aggiunge "+ FabricPool" al nome della policy attiva o inattiva, ma è possibile specificare un nome personalizzato.
2. Esaminare l'elenco delle regole nella policy inattiva.
 - 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 in alto.
 - Se la griglia ha già 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 la policy inattiva contiene regole diverse o un ordine diverso rispetto alla policy attiva, la procedura guidata crea una nuova policy inattiva clonando la policy attiva e aggiungendo la nuova regola in alto.
3. Rivedere l'ordine delle regole nella nuova policy inattiva.

Poiché la regola FabricPool è la prima regola, tutti gli oggetti nel bucket FabricPool vengono posizionati prima che vengano valutate le altre regole nel criterio. Gli oggetti in qualsiasi altro bucket vengono inseriti dalle regole successive nella policy.

4. Esaminare il diagramma di conservazione per scoprire come verranno conservati 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 archiviazione** per esaminare il diagramma di conservazione. Verificare che tutte le regole applicate al bucket o al tenant FabricPool conservino gli oggetti **per sempre**.
5. Dopo aver esaminato la policy inattiva, seleziona **Attiva e continua** per attivare la policy e passare alla fase di classificazione del traffico.



Gli errori in una policy ILM possono causare una perdita irreparabile di dati. Prima di attivarla, leggere attentamente la policy.

Passaggio 8 di 9: creare una policy di classificazione del traffico

Come opzione, la procedura guidata di configurazione FabricPool può creare un criterio di classificazione del traffico che è possibile utilizzare per monitorare il carico di lavoro FabricPool. Il criterio creato dal sistema utilizza una regola di corrispondenza per identificare tutto il traffico di rete correlato al bucket creato. Questa policy monitora solo il traffico; non limita il traffico per FabricPool o altri client.

Per i dettagli su questo passaggio, vedere ["Creare una policy di classificazione del traffico per FabricPool"](#).

Passi

1. Rivedi la politica.

2. Se si desidera creare questa policy di classificazione del traffico, selezionare **Crea e continua**.

Non appena FabricPool inizia a suddividere i dati in livelli per StorageGRID, è possibile accedere alla pagina Criteri di classificazione del traffico per visualizzare le metriche del traffico di rete per questo criterio. In seguito, è anche possibile aggiungere regole per limitare altri carichi di lavoro e garantire che il carico di lavoro FabricPool disponga della maggior parte della larghezza di banda.

3. Altrimenti, seleziona **Salta questo passaggio**.

Fase 9 di 9: Riepilogo della revisione

Il riepilogo fornisce dettagli sugli elementi configurati, tra cui il nome del bilanciatore del carico, del tenant e del bucket, la policy di classificazione del traffico e la policy ILM attiva.

Passi

1. Rivedi il riepilogo.
2. Selezionare **Fine**.

Prossimi passi

Dopo aver completato la procedura guidata FabricPool, eseguire questi passaggi aggiuntivi.

Passi

1. Vai a ["Configurare ONTAP System Manager"](#) per immettere 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 i criteri di suddivisione in livelli del volume.
2. Vai a ["Configurare il server DNS"](#) e assicurati che il DNS includa un record per associare il nome del server StorageGRID (nome di dominio completo) a ciascun indirizzo IP StorageGRID che utilizzerai.
3. Vai a ["Altre best practice per StorageGRID e FabricPool"](#) per apprendere le best practice per i log di controllo 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 una raccolta di nodi, ognuno dei quali contiene il servizio StorageGRID Load Balancer. Un gruppo HA può contenere nodi gateway, nodi amministrativi 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 fallisce, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool.

Per i dettagli su questa attività, vedere ["Gestire gruppi ad alta disponibilità"](#). Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#).

Prima di iniziare

- Hai esaminato il ["best practice per gruppi ad alta disponibilità"](#).

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .
- Se si prevede di utilizzare una VLAN, è stata creata l'interfaccia VLAN. Vedere ["Configurare le interfacce VLAN"](#) .

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Gruppi ad alta disponibilità**.
2. Seleziona **Crea**.
3. Per la fase **Inserisci dettagli**, compila i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome visualizzato univoco per questo gruppo HA.
Descrizione (facoltativa)	Descrizione di questo gruppo HA.

4. Per il passaggio **Aggiungi interfacce**, seleziona le interfacce del nodo che desideri utilizzare in questo gruppo HA.

Utilizzare le intestazioni di colonna per ordinare le righe oppure immettere un termine di ricerca per individuare più rapidamente le interfacce.

È possibile selezionare uno o più nodi, ma è possibile selezionare solo un'interfaccia per ciascun nodo.

5. Per il passaggio **Assegna priorità alle interfacce**, determinare l'interfaccia primaria e tutte 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 primaria 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 funziona, gli indirizzi IP virtuali (VIP) vengono spostati sulla prima interfaccia di backup in ordine di priorità. Se tale interfaccia non funziona, gli indirizzi VIP vengono spostati alla successiva interfaccia di backup e così via. Una volta risolti i guasti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

6. Per il passaggio **Inserisci indirizzi IP**, compila i seguenti campi.

Campo	Descrizione
CIDR di sottorete	L'indirizzo della subnet VIP in notazione CIDR: un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere alcun bit host impostato. Ad esempio, 192.16.0.0/22 .

Campo	Descrizione
Indirizzo IP del gateway (facoltativo)	Opzionale. Se gli indirizzi IP ONTAP utilizzati per accedere a StorageGRID non si trovano sulla stessa subnet degli indirizzi VIP StorageGRID , immettere l'indirizzo IP del gateway locale VIP StorageGRID . L'indirizzo IP del gateway locale deve essere all'interno della subnet VIP.
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. Facoltativamente, è possibile specificare indirizzi IPv4 e IPv6 aggiuntivi.

7. Selezionare **Crea gruppo HA** e quindi selezionare **Fine**.

Creare un endpoint del bilanciatore del carico per FabricPool

StorageGRID utilizza un bilanciatore 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 su più nodi di archiviazione.

Quando si configura StorageGRID per l'utilizzo con FabricPool, è necessario configurare un endpoint del bilanciatore del carico e caricare o generare un certificato dell'endpoint del bilanciatore del carico, che viene utilizzato per proteggere la connessione tra ONTAP e StorageGRID.

Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#) .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso 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"](#) .

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Endpoint del bilanciatore del carico**.
2. Seleziona **Crea**.
3. Per il passaggio **Inserisci i dettagli dell'endpoint**, compila 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 impostato su 10433 per il primo endpoint creato, ma è possibile immettere 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 amministrativi. Nota: non sono consentite le porte utilizzate da altri servizi di rete. Vedi il "Riferimento porta di rete". Fornirai questo numero a ONTAP quando collegherai StorageGRID come livello cloud FabricPool.
Tipo di cliente	Selezionare S3 .
Protocollo di rete	Selezionare HTTPS. Nota: la comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

4. Per il passaggio **Seleziona modalità di associazione**, specificare la modalità di associazione. La modalità di associazione controlla il modo in cui si accede all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (predefinito)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo HA su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione Globale (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 il corrispondente FQDN) di un gruppo HA. Gli endpoint con questa modalità di associazione possono utilizzare tutti lo stesso numero di porta, purché i gruppi HA selezionati per gli endpoint non si sovrappongano.
Interfacce dei nodi	Per accedere a questo endpoint, i client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionati.
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 oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway per accedere a questo endpoint.

5. Per il passaggio **Accesso tenant**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket. Consenti tutti i tenant è quasi sempre l'opzione appropriata per l'endpoint del bilanciamento del carico utilizzato per FabricPool. È necessario selezionare questa opzione se non è ancora stato creato alcun account tenant.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai propri bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

6. Per il passaggio **Allega certificato**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Carica il certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato da una CA, una chiave privata del certificato e un bundle CA facoltativo.
Genera certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciamento del carico" per i dettagli su cosa inserire.
Utilizzare il certificato StorageGRID S3	Questa opzione è disponibile solo se hai già caricato o generato una versione personalizzata del certificato globale StorageGRID . Vedere "Configurare i certificati API S3" per i dettagli.

7. Seleziona **Crea**.



Le modifiche al certificato di un endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Crea un account tenant per FabricPool

Per utilizzare FabricPool è necessario creare un account tenant in Grid Manager.

Gli account tenant consentono alle applicazioni client di archiviare e recuperare oggetti su StorageGRID. Ogni account tenant ha il proprio ID account, gruppi e utenti autorizzati, bucket e oggetti.

Per i dettagli su questa attività, vedere ["Crea un account inquilino"](#) . Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#) .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Passi

1. Selezionare **INQUILINI**.
2. Seleziona **Crea**.
3. Per i passaggi Inserisci dettagli, inserisci le seguenti informazioni.

Campo	Descrizione
Nome	Un nome per l'account del tenant. I nomi degli inquilini non devono essere univoci. Quando viene creato l'account tenant, questo riceve un ID account numerico univoco.
Descrizione (facoltativa)	Una descrizione che aiuti a identificare l'inquilino.
Tipo di cliente	Deve essere S3 per FabricPool.
Quota di archiviazione (facoltativa)	Lasciare vuoto questo campo per FabricPool.

4. Per il passaggio Seleziona autorizzazioni:

- a. Non selezionare **Consenti servizi di piattaforma**.

In genere, i tenant FabricPool non hanno bisogno di utilizzare servizi di piattaforma, come la replica di CloudMirror.

- b. Facoltativamente, seleziona **Usa la tua fonte di identità**.

- c. Non selezionare **Consenti selezione S3**.

In genere, i tenant FabricPool non hanno bisogno di utilizzare S3 Select.

- d. Facoltativamente, seleziona **Usa connessione federazione griglia** per consentire al tenant di utilizzare una ["collegamento della federazione di rete"](#) per la clonazione dell'account e la replica tra griglie. Quindi, seleziona la connessione di federazione della griglia da utilizzare.

5. Per il passaggio Definisci accesso root, specificare quale utente avrà l'autorizzazione di accesso root iniziale per l'account tenant, in base al fatto che il sistema StorageGRID utilizzi ["federazione di identità"](#) , ["accesso unico \(SSO\)"](#) , o entrambi.

Opzione	Fai questo
Se la federazione delle identità non è abilitata	Specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se la federazione delle identità è abilitata	a. Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si accede al tenant come utente root locale.

Opzione	Fai questo
Se sono abilitati sia la federazione delle identità che il Single Sign-On (SSO)	Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. Nessun utente locale può effettuare l'accesso.

6. Selezionare **Crea tenant**.

Crea un bucket S3 e ottieni 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 verrà utilizzato per FabricPool.

Per i dettagli su questa attività, vedere ["Crea bucket S3"](#) E ["Crea le tue chiavi di accesso S3"](#) . Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#) .

Prima di iniziare

- Hai creato un account tenant per l'utilizzo FabricPool .
- Hai accesso Root all'account tenant.

Passi

1. Sign in a Tenant Manager.

Puoi procedere in uno dei seguenti modi:

- Dalla pagina Account tenant in Grid Manager, seleziona il link * Sign in* per il tenant e inserisci le tue credenziali.
- Inserisci l'URL dell'account tenant in un browser Web e inserisci le tue credenziali.

2. Crea un bucket S3 per i dati FabricPool .

È necessario creare un bucket univoco per ogni cluster ONTAP che si intende utilizzare.

- Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
- Seleziona **Crea bucket**.
- 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. Seleziona la regione per questo bucket.

Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione.

e. Selezionare **Continua**.

f. Seleziona **Crea bucket**.



Non selezionare **Abilita controllo delle versioni degli oggetti** per il bucket FabricPool . Allo stesso modo, non modificare un bucket FabricPool per utilizzare **Disponibile** o una coerenza non predefinita. La coerenza 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.

- Selezionare **ARCHIVIAZIONE (S3) > Le mie chiavi di accesso**.
- Seleziona **Crea chiave**.
- Seleziona **Crea chiave di accesso**.
- Copiare l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di 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 genera una nuova chiave di accesso e una chiave di accesso segreta in StorageGRID , immettere 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

È possibile utilizzare questo semplice esempio di policy come punto di partenza per le proprie regole e policy ILM.

In questo esempio si presuppone che si stiano progettando le regole ILM e una policy ILM per un sistema StorageGRID dotato di quattro nodi di archiviazione in un unico 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 molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita. Per saperne di più, vedere ["Gestire gli oggetti con ILM"](#) .



Per evitare la perdita di dati, non utilizzare una regola ILM che farà scadere o eliminerà i dati del livello cloud FabricPool . Impostare il periodo di conservazione su **per sempre** per garantire che gli oggetti FabricPool non vengano eliminati da StorageGRID ILM.

Prima di iniziare

- Hai esaminato il ["best practice per l'utilizzo di ILM con dati FabricPool"](#) .
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di accesso ILM o Root"](#) .
- Se hai eseguito l'aggiornamento a StorageGRID 11.9 da una versione precedente StorageGRID , hai configurato il pool di archiviazione che utilizzerai. In generale, dovresti creare un pool di archiviazione per ogni sito StorageGRID che utilizzerai per archiviare i dati.



Questo prerequisito non si applica se inizialmente è stato installato StorageGRID 11.7 o 11.8. Quando si installa inizialmente una di queste versioni, vengono creati automaticamente dei pool di archiviazione per ogni sito.

Passi

1. Creare una regola ILM che si applica solo ai dati in `fabricpool-bucket`. Questa regola di esempio crea copie con codice di cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione 2 + 1 per i dati FabricPool
Nome del bucket	<code>fabricpool-bucket</code> È anche possibile filtrare in base all'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 ingestione
Periodo di tempo e collocamenti	Dal giorno 0 conservalo per sempre Memorizzare gli oggetti tramite codifica di cancellazione utilizzando lo schema EC 2+1 a Denver e conservare tali oggetti in StorageGRID per sempre.  Per evitare la perdita di dati, non utilizzare una regola ILM che farà scadere o eliminerà i dati del livello cloud FabricPool .
Comportamento di ingestione	Equilibrato

2. Crea una regola ILM predefinita che creerà due copie replicate di tutti gli oggetti non corrispondenti alla prima regola. Non selezionare un filtro di base (account tenant o nome bucket) né filtri avanzati.

Definizione della regola	Valore di esempio
Nome della regola	Due copie replicate
Nome del bucket	<i>nessuno</i>
Filtri avanzati	<i>nessuno</i>
Tempo di riferimento	Tempo di ingestione

Definizione della regola	Valore di esempio
Periodo di tempo e collocamenti	Dal giorno 0 conservalo per sempre Conserva gli oggetti replicandone 2 copie a Denver.
Comportamento di ingestione	Equilibrato

3. Creare una policy ILM e selezionare le due regole. Poiché la regola di replica non utilizza alcun filtro, può essere la regola predefinita (ultima) per il criterio.
4. Inserire gli oggetti di prova nella griglia.
5. Simulare la policy con gli oggetti di prova per verificarne il comportamento.
6. Attiva la policy.

Quando questa policy è attivata, StorageGRID posiziona i dati degli oggetti come segue:

- I dati suddivisi in livelli da FabricPool in `fabricpool-bucket` verrà codificato con cancellazione utilizzando lo schema di codifica 2+1. Due frammenti di dati e un frammento di parità verranno posizionati su tre nodi di archiviazione diversi.
- Tutti gli oggetti in tutti gli altri bucket verranno replicati. Verranno create due copie e posizionate su due nodi di archiviazione diversi.
- Le copie verranno conservate in StorageGRID per sempre. StorageGRID ILM non eliminerà questi oggetti.

Creare una policy di classificazione del traffico per FabricPool

Facoltativamente, è possibile progettare una policy di classificazione del traffico StorageGRID per ottimizzare la qualità del servizio per il carico di lavoro FabricPool .

Per i dettagli su questa attività, vedere ["Gestire le policy di classificazione del traffico"](#) . Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#) .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .

Informazioni su questo compito

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 livelli su StorageGRID, è necessario assicurarsi che il carico di lavoro FabricPool disponga della 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, è più importante dare priorità alle operazioni di lettura FabricPool rispetto alle operazioni di scrittura.

Ad esempio, se altri client S3 utilizzano questo sistema StorageGRID , è necessario creare una policy di classificazione del traffico. È possibile limitare il traffico di rete per gli altri bucket, tenant, subnet IP o

endpoint del bilanciatore del carico.

- In genere, non dovresti imporre limiti alla qualità del servizio su alcun carico di lavoro FabricPool ; dovresti limitare solo gli altri carichi di lavoro.
- I limiti imposti ad altri carichi di lavoro dovrebbero tenere conto del comportamento di tali carichi di lavoro. I limiti imposti varieranno anche in base alle dimensioni e alle capacità della rete e al livello di utilizzo previsto.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.
2. Seleziona **Crea**.
3. Inserisci un nome e una descrizione (facoltativa) per la policy e seleziona **Continua**.
4. Per il passaggio Aggiungi regole di corrispondenza, aggiungere almeno una regola.
 - a. Seleziona **Aggiungi regola**
 - b. Per Tipo, seleziona **Endpoint del bilanciatore del carico** e seleziona l'endpoint del bilanciatore del carico creato per FabricPool.

È anche possibile selezionare l'account tenant o il bucket FabricPool .
 - c. Se si desidera che questa policy del traffico limiti il traffico per gli altri endpoint, selezionare **Corrispondenza inversa**.
5. Facoltativamente, aggiungi uno o più limiti per controllare il traffico di rete a cui corrisponde la regola.



StorageGRID raccoglie le metriche anche se non si aggiungono limiti, in modo da poter comprendere le tendenze del traffico.

- a. Seleziona **Aggiungi un limite**.
 - b. Seleziona il tipo di traffico che vuoi limitare e il limite da applicare.
6. Selezionare **Continua**.
 7. Leggere e rivedere la politica di classificazione del traffico. Utilizzare il pulsante **Precedente** per tornare indietro e apportare le modifiche desiderate. Quando sei soddisfatto della policy, seleziona **Salva e continua**.

Dopo aver finito

["Visualizza le metriche del traffico di rete"](#) per verificare che le norme rispettino i limiti di traffico previsti.

Configurare ONTAP System Manager

Dopo aver ottenuto le informazioni StorageGRID richieste, puoi andare su ONTAP per aggiungere StorageGRID come livello cloud.

Prima di iniziare

- Se hai completato la procedura guidata di configurazione FabricPool , hai `ONTAP_FabricPool_settings_bucketname.txt` file che hai scaricato.
- Se hai configurato StorageGRID manualmente, disponi del nome di dominio completo (FQDN) che stai utilizzando per StorageGRID o dell'indirizzo IP virtuale (VIP) per il gruppo StorageGRID HA, del numero di porta per l'endpoint del bilanciatore del carico, del certificato del bilanciatore del carico, dell'ID della chiave di accesso e della chiave segreta per l'utente root dell'account tenant e del nome del bucket che ONTAP

utilizzerà in quel tenant.

Access ONTAP System Manager

Queste istruzioni descrivono come utilizzare ONTAP System Manager per aggiungere StorageGRID come livello cloud. È possibile completare la stessa configurazione utilizzando ONTAP CLI. Per le istruzioni, vai a ["Documentazione ONTAP per FabricPool"](#) .

Passi

1. Accedi a System Manager per il cluster ONTAP che desideri suddividere in livelli su StorageGRID.
2. Sign in come amministratore per il cluster.
3. Vai a **ARCHIVIAZIONE > Livelli > Aggiungi livello cloud**.
4. Selezionare * StorageGRID* dall'elenco dei provider di archiviazione oggetti.

Inserisci i valori StorageGRID

Vedere ["Documentazione ONTAP per FabricPool"](#) per maggiori informazioni.

Passi

1. Completa il modulo Aggiungi livello cloud, utilizzando `ONTAP_FabricPool_settings_bucketname.txt` file o i valori ottenuti manualmente.

Campo	Descrizione
Nome	Inserisci un nome univoco per questo livello cloud. È possibile accettare il valore predefinito.
Stile URL	Se tu "nomi di dominio endpoint S3 configurati" , seleziona URL in stile ospitato virtuale. Path-Style URL è l'impostazione predefinita per ONTAP, ma per StorageGRID si consiglia di utilizzare richieste in stile virtual hosted. È necessario utilizzare URL stile percorso se si fornisce un indirizzo IP anziché un nome di dominio per il campo Nome server (FQDN).
Nome del 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, <code>s3.storagegrid.company.com</code> . Notare quanto segue: • L'indirizzo IP o il nome di dominio specificato qui deve corrispondere al certificato caricato o generato per l'endpoint del bilanciatore del carico StorageGRID . • Se si fornisce un nome di dominio, il record DNS deve essere mappato su ciascun indirizzo IP che si utilizzerà per connettersi a StorageGRID. Vedere "Configurare il server DNS" .
SSL	Abilitato (predefinito).

Campo	Descrizione
Certificato di archiviazione degli oggetti	Incolla il certificato PEM che stai utilizzando per l'endpoint del bilanciatore del carico StorageGRID , inclusi: -----BEGIN CERTIFICATE----- E -----END CERTIFICATE----- . Nota: se una CA intermedia ha emesso il certificato StorageGRID , è necessario fornire il certificato della CA intermedia. Se il certificato StorageGRID è stato emesso direttamente dalla CA radice, è necessario fornire il certificato della CA radice.
Porta	Immettere la porta utilizzata dall'endpoint del bilanciatore del carico StorageGRID . ONTAP utilizzerà questa porta quando si conatterà 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 genera una nuova chiave di accesso e una chiave di accesso segreta in StorageGRID , immettere 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 contenitore	Inserisci il nome del bucket StorageGRID creato per l'utilizzo con questo livello ONTAP .

2. Completare la configurazione finale FabricPool in ONTAP.
 - a. Collegare uno o più aggregati al livello cloud.
 - b. Facoltativamente, creare una politica di suddivisione in livelli del volume.

Configurare il server DNS

Dopo aver configurato i gruppi ad alta disponibilità, gli endpoint del bilanciatore 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 ogni nome nel certificato di sicurezza e per ogni indirizzo IP che si desidera utilizzare.

Vedere ["Considerazioni sul 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 verrà utilizzato. Gli indirizzi IP immessi nel DNS dipendono dall'utilizzo o meno di un gruppo HA di nodi di bilanciamento del carico:

- Se è stato configurato un gruppo HA, ONTAP si conatterà agli indirizzi IP virtuali di quel gruppo HA.
- Se non si utilizza un gruppo HA, ONTAP può conatterci al servizio StorageGRID Load Balancer utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo.
- Se il nome del server si risolve in più di un indirizzo IP, ONTAP stabilisce connessioni client con tutti gli

indirizzi IP (fino a un massimo di 16 indirizzi IP). Gli indirizzi IP vengono rilevati tramite un metodo round-robin quando vengono stabilite le connessioni.

Voci DNS per richieste in stile ospitato virtuale

Se hai definito "[Nomi di dominio endpoint S3](#)" e utilizzerai richieste in stile virtual hosted, aggiungerai voci DNS per tutti i nomi di dominio degli endpoint S3 richiesti, inclusi eventuali nomi jolly.

Le migliori pratiche StorageGRID per FabricPool

Procedure consigliate per i gruppi ad alta disponibilità (HA)

Prima di collegare StorageGRID come livello cloud FabricPool , informati sui gruppi ad alta disponibilità (HA) StorageGRID e rivedi le best practice per l'utilizzo dei gruppi HA con FabricPool.

Che cos'è un gruppo HA?

Un gruppo ad alta disponibilità (HA) è una raccolta di interfacce provenienti 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 fallisce, 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 sui nodi gateway o sia sui nodi amministrativi che sui nodi gateway fornisce un accesso altamente disponibile al servizio Load Balancer condiviso.

Per saperne di più sui gruppi ad alta disponibilità, vedere "[Gestire gruppi ad alta disponibilità \(HA\)](#)".

Utilizzo di gruppi HA

Le procedure consigliate 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 interruzioni nel recupero dei dati.
- Se si prevede di utilizzare la politica di suddivisione in livelli del volume basata solo su snapshot FabricPool o livelli di prestazioni locali non primari (ad esempio, posizioni di disaster recovery o destinazioni NetApp SnapMirror), è possibile configurare un gruppo HA con un solo nodo.

Queste istruzioni descrivono come impostare un gruppo HA per HA Active-Backup (un nodo è attivo e l'altro è di backup). Tuttavia, potresti preferire utilizzare DNS Round Robin o Active-Active HA. Per conoscere i 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 collegare StorageGRID come livello cloud FabricPool , rivedere le best practice per l'utilizzo dei bilanciatori del carico con FabricPool.

Per informazioni generali sul bilanciatore del carico StorageGRID e sul certificato del bilanciatore del carico, vedere "[Considerazioni sul bilanciamento del carico](#)".

Procedure consigliate per l'accesso del tenant all'endpoint del bilanciatore del carico utilizzato per FabricPool

È possibile controllare quali tenant possono utilizzare uno specifico endpoint del bilanciatore del carico per accedere ai propri bucket. È possibile consentire l'accesso a tutti gli inquilini, ad alcuni o bloccarne alcuni. Quando si crea un endpoint di bilanciamento del carico per l'utilizzo FabricPool, selezionare **Consenti tutti i tenant**. ONTAP crittografa i dati inseriti nei bucket StorageGRID, pertanto questo livello di sicurezza aggiuntivo garantirebbe poca sicurezza aggiuntiva.

Buone pratiche per il certificato di sicurezza

Quando si crea un endpoint del bilanciatore del carico StorageGRID per l'utilizzo in 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 dovrebbe utilizzare la crittografia Transport Layer Security (TLS). L'utilizzo di FabricPool senza crittografia TLS è supportato ma non consigliato. Quando si seleziona il protocollo di rete per l'endpoint del bilanciatore del carico StorageGRID, selezionare **HTTPS**. Quindi fornire il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

Per saperne di più sul certificato del server per un endpoint di bilanciamento del carico:

- ["Gestire i certificati di sicurezza"](#)
- ["Considerazioni sul bilanciamento del carico"](#)
- ["Linee guida per il rafforzamento dei certificati del server"](#)

Aggiungi certificato a ONTAP

Quando si aggiunge StorageGRID come livello cloud FabricPool, è necessario installare lo stesso certificato sul cluster ONTAP, inclusi i certificati radice e tutti i certificati dell'autorità di certificazione (CA) subordinata.

Gestisci 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 suddivisi in livelli su StorageGRID.

Per evitare problemi di scadenza dei certificati, seguire queste best practice:

- Monitorare attentamente tutti gli avvisi che segnalano l'avvicinarsi della data di scadenza dei certificati, come gli avvisi **Scadenza del certificato dell'endpoint del bilanciatore del carico** e **Scadenza del certificato del server globale per l'API S3**.
- Mantenere sempre sincronizzate le versioni StorageGRID e ONTAP del certificato. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint del bilanciatore del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato da ONTAP per il livello cloud.
- Utilizzare un certificato CA firmato pubblicamente. Se si utilizza un certificato firmato da una CA, è possibile utilizzare l'API Grid Management per automatizzare la rotazione dei certificati. Ciò consente di sostituire i certificati prossimi alla scadenza senza interruzioni.
- Se hai generato un certificato StorageGRID autofirmato e tale certificato sta per scadere, devi sostituirlo manualmente sia in StorageGRID che in ONTAP prima che scada il 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 NetApp : come configurare un nuovo certificato server autofirmato StorageGRID"](#)

su una distribuzione ONTAP FabricPool esistente" per istruzioni.

Procedure consigliate per l'utilizzo di ILM con i dati FabricPool

Se si utilizza FabricPool per suddividere i dati in livelli per StorageGRID, è necessario comprendere i requisiti per l'utilizzo della gestione del ciclo di vita delle informazioni (ILM) StorageGRID con i dati FabricPool .



FabricPool non ha alcuna conoscenza delle regole o delle policy ILM StorageGRID . Se la policy StorageGRID ILM non è configurata correttamente, si può verificare una perdita di dati. Per informazioni dettagliate, vedere ["Utilizzare le regole ILM per gestire gli oggetti"](#) E ["Creare policy ILM"](#) .

Linee guida per l'utilizzo di ILM con FabricPool

Quando si utilizza la procedura guidata di configurazione FabricPool , questa crea automaticamente una nuova regola ILM per ogni bucket S3 creato e aggiunge tale regola a un criterio inattivo. Ti verrà chiesto di attivare la policy. La regola creata automaticamente segue le best practice consigliate: utilizza la codifica di cancellazione 2+1 in un singolo sito.

Se si configura StorageGRID manualmente anziché utilizzare la procedura guidata di configurazione FabricPool , consultare queste linee guida per assicurarsi che le regole e i criteri ILM siano adatti ai dati FabricPool e ai requisiti aziendali. Potrebbe essere necessario creare nuove regole e aggiornare le policy ILM attive per soddisfare queste linee guida.

- È possibile utilizzare qualsiasi combinazione di regole di replicazione e di codifica di cancellazione per proteggere i dati del livello cloud.

La migliore pratica consigliata è quella di utilizzare la codifica di cancellazione 2+1 all'interno di un sito per una protezione dei dati conveniente. La codifica di cancellazione utilizza più CPU, ma offre una capacità di archiviazione notevolmente inferiore rispetto alla replicazione. Gli schemi 4+1 e 6+1 utilizzano meno capacità rispetto allo schema 2+1. Tuttavia, gli schemi 4+1 e 6+1 sono meno flessibili se è necessario aggiungere nodi di archiviazione durante l'espansione della griglia. Per maggiori dettagli, vedere ["Aggiungere capacità di archiviazione per oggetti con codice di cancellazione"](#) .

- Ogni regola applicata ai dati FabricPool deve utilizzare la codifica di cancellazione oppure deve creare almeno due copie replicate.



Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

- Se hai bisogno di ["rimuovere i dati FabricPool da StorageGRID"](#) , utilizzare ONTAP per recuperare tutti i dati per il volume FabricPool e promuoverlo al livello di prestazioni.



Per evitare la perdita di dati, non utilizzare una regola ILM che farà scadere o eliminerà i dati del livello cloud FabricPool . Impostare il periodo di conservazione in ogni regola ILM su **per sempre** per garantire che gli oggetti FabricPool non vengano eliminati da StorageGRID ILM.

- Non creare regole che sposteranno i dati del livello cloud FabricPool dal bucket a un'altra posizione. Non è

possibile utilizzare un Cloud Storage Pool per spostare i dati FabricPool in un altro archivio oggetti.



L'utilizzo di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva necessaria per recuperare un oggetto dalla destinazione di Cloud Storage Pool.

- A partire da ONTAP 9.8, è possibile creare facoltativamente tag di oggetti per facilitare la classificazione e l'ordinamento dei dati a livelli, semplificandone la gestione. Ad esempio, è possibile impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Quindi, quando si creano regole ILM in StorageGRID, è possibile utilizzare il filtro avanzato Object Tag per selezionare e posizionare 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 StorageGRID. Prima di modificare un'impostazione globale, valutare l'impatto della modifica sulle altre applicazioni S3.

Destinazioni dei messaggi di controllo e dei registri

I carichi di lavoro FabricPool presentano spesso un elevato tasso di operazioni di lettura, che può generare un volume elevato di messaggi di audit.

- Se non è necessario un record delle operazioni di lettura del client per FabricPool o qualsiasi altra applicazione S3, è possibile passare facoltativamente a **CONFIGURAZIONE > Monitoraggio > Server di audit e 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 controllo e le destinazioni dei registri"](#) per i dettagli.
- Se si dispone di una griglia di grandi dimensioni, 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 sulle prestazioni della registrazione dei messaggi di controllo senza ridurre la completezza dei dati di controllo. Vedere ["Considerazioni per il server syslog esterno"](#) per i dettagli.

Crittografia degli oggetti

Durante la configurazione di StorageGRID, è possibile abilitare facoltativamente ["opzione globale per la crittografia degli oggetti memorizzati"](#) se è richiesta la crittografia dei dati per altri client StorageGRID. I dati suddivisi in livelli da FabricPool a StorageGRID sono già crittografati, pertanto non è necessario abilitare l'impostazione StorageGRID. Le chiavi di crittografia lato client sono di proprietà di ONTAP.

Compressione degli oggetti

Quando si configura StorageGRID, non abilitare ["opzione globale per comprimere gli oggetti memorizzati"](#). I dati suddivisi in livelli da FabricPool a StorageGRID sono già compressi. L'utilizzo dell'opzione StorageGRID non ridurrà ulteriormente le dimensioni di un oggetto.

Consistenza del secchio

Per i bucket FabricPool, la coerenza consigliata è **Read-after-new-write**, che è la coerenza predefinita per un nuovo bucket. Non modificare i bucket FabricPool per utilizzare **Disponibile** o **Strong-site**.

Struttura a FabricPool

Se un nodo StorageGRID utilizza storage assegnato da un sistema NetApp ONTAP, verificare che il volume

non abbia un criterio di suddivisione in livelli FabricPool abilitato. Ad esempio, se un nodo StorageGRID è in esecuzione su un host VMware, assicurarsi che il volume che supporta il datastore per il nodo StorageGRID non abbia un criterio di suddivisione in livelli FabricPool abilitato. La disattivazione della suddivisione in livelli FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di archiviazione.



Non utilizzare mai FabricPool per riportare i dati relativi a StorageGRID a StorageGRID stesso. Il riordino dei dati StorageGRID su StorageGRID aumenta la complessità operativa e la risoluzione dei problemi.

Rimuovere i dati FabricPool da StorageGRID

Se è necessario rimuovere i dati FabricPool attualmente archiviati in StorageGRID, è necessario utilizzare ONTAP per recuperare tutti i dati per il volume FabricPool e promuoverli al livello di prestazioni.

Prima di iniziare

- Hai esaminato le istruzioni e le considerazioni in ["Promuovi i dati al livello di prestazioni"](#) .
- Stai utilizzando ONTAP 9.8 o versione successiva.
- Stai utilizzando un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti StorageGRID per l'account tenant FabricPool che ha ["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#) .

Informazioni su questo compito

Queste istruzioni spiegano come spostare i dati da StorageGRID a FabricPool. Questa procedura viene eseguita utilizzando ONTAP e StorageGRID Tenant Manager.

Passi

1. Da ONTAP, emettere il `volume modify` comando.

Impostato `tiering-policy` A `none` per fermare la nuova suddivisione in livelli e impostare `cloud-retrieval-policy` A `promote` per restituire tutti i dati precedentemente suddivisi in livelli su StorageGRID.

Vedere ["Promuovi tutti i dati da un volume FabricPool al livello di prestazioni"](#) .

2. Attendere il completamento dell'operazione.

Puoi usare il `volume object-store` comando con il `tiering` opzione per ["verificare lo stato della promozione del livello di performance"](#) .

3. Una volta completata l'operazione di promozione, accedi a StorageGRID Tenant Manager per l'account tenant FabricPool .
4. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
5. Verificare che il bucket FabricPool sia ora vuoto.
6. Se il secchio è vuoto, ["elimina il bucket"](#) .

Dopo aver finito

Quando si elimina il bucket, la suddivisione in livelli da FabricPool a StorageGRID non può più continuare.

Tuttavia, poiché il livello locale è ancora collegato al livello cloud StorageGRID , ONTAP System Manager restituirà messaggi di errore che indicano che il bucket non è accessibile.

Per evitare questi messaggi di errore, procedere in uno dei seguenti modi:

- Utilizzare FabricPool Mirror per collegare un livello cloud diverso all'aggregato.
- Spostare i dati dall'aggregato FabricPool a un aggregato non FabricPool , quindi eliminare l'aggregato non utilizzato.

Vedi il "[Documentazione ONTAP per FabricPool](#)" per istruzioni.

Utilizzare i tenant e i client StorageGRID

Utilizzare un account tenant

Utilizzare un account tenant

Un account tenant consente di utilizzare l'API REST Simple Storage Service (S3) o l'API REST Swift per archiviare e recuperare oggetti in un sistema StorageGRID .

Che cos'è un conto inquilino?

Ogni account tenant ha i propri gruppi federati o locali, utenti, bucket S3 o contenitori Swift e oggetti.

Gli account tenant possono essere utilizzati per separare gli oggetti archiviati da entità diverse. Ad esempio, è possibile utilizzare più account tenant per uno qualsiasi di questi casi d'uso:

- **Caso d'uso aziendale:** se il sistema StorageGRID viene utilizzato all'interno di un'azienda, l'archiviazione degli oggetti della griglia potrebbe essere segregata dai diversi reparti dell'organizzazione. Ad esempio, potrebbero esserci 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 anche i bucket S3 e i criteri dei bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario creare account tenant separati. Vedi le istruzioni per l'implementazione "[Bucket S3 e policy dei bucket](#)" per maggiori informazioni.

- **Caso d'uso del fornitore di servizi:** se il sistema StorageGRID viene utilizzato da un fornitore di servizi, l'archiviazione degli oggetti della griglia potrebbe essere segregata dalle diverse entità che affittano l'archiviazione. Ad esempio, potrebbero esserci conti inquilino per la Società A, la Società B, la Società C e così via.

Come creare un account tenant

Gli account degli inquilini vengono creati da un "[Amministratore della griglia StorageGRID che utilizza Grid Manager](#)". 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) e la quota di archiviazione facoltativa.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine identità, utilizzare S3 Select o utilizzare una connessione di federazione di griglia.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione delle identità o Single Sign-On (SSO).

Inoltre, gli amministratori della griglia possono abilitare l'impostazione S3 Object Lock per il sistema StorageGRID se gli account tenant S3 devono essere conformi ai requisiti normativi. Quando S3 Object Lock è abilitato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

Configurare i tenant S3

Dopo un "[L'account tenant S3 è stato creato](#)", puoi accedere al Tenant Manager per eseguire attività come le seguenti:

- Impostare la federazione delle identità (a meno che l'origine dell'identità non sia condivisa con la griglia)
- Gestisci gruppi e utenti
- Utilizzare la federazione di griglia per la clonazione degli account e la replica tra griglie
- Gestisci le chiavi di accesso S3
- Crea e gestisci bucket S3
- Utilizzare i servizi della piattaforma S3
- Utilizzare S3 Select
- Monitorare l'utilizzo dello spazio di archiviazione



Sebbene sia possibile creare e gestire bucket S3 con Tenant Manager, è necessario utilizzare un ["Cliente S3"](#) o un ["Console S3"](#) per ingerire e gestire oggetti.

Come accedere e uscire

Sign in a Tenant Manager

Si accede al Tenant Manager inserendo l'URL del tenant nella barra degli indirizzi di un ["browser web supportato"](#).

Prima di iniziare

- Hai le tue credenziali di accesso.
- Hai un URL per accedere a Tenant Manager, fornito dall'amministratore della tua griglia. L'URL sarà simile a uno di questi 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 di amministrazione o l'indirizzo IP virtuale di un gruppo HA di nodi di amministrazione. Potrebbe includere anche un numero di porta, l'ID dell'account tenant a 20 cifre o entrambi.

- Se l'URL non include l'ID account di 20 cifre del tenant, si dispone di questo ID account.
- Stai utilizzando un ["browser web supportato"](#).
- I cookie sono abilitati nel tuo browser web.
- Appartieni a un gruppo di utenti che ha ["autorizzazioni di accesso specifiche"](#).

Passi

1. Lanciare un ["browser web supportato"](#).
2. Nella barra degli indirizzi del browser, inserisci l'URL per accedere a Tenant Manager.
3. Se viene visualizzato un avviso di sicurezza, installare il certificato utilizzando la procedura guidata di installazione del browser.

4. Sign in a Tenant Manager.

La schermata di accesso visualizzata dipende dall'URL immesso e dal fatto che sia stato configurato l'accesso singolo (SSO) per StorageGRID.

Non si utilizza SSO

Se StorageGRID non utilizza SSO, viene visualizzata una delle seguenti schermate:

- La pagina di accesso di Grid Manager. Selezionare il link **Accesso tenant**.



NetApp StorageGRID®

Grid Manager

Username

Password

[Sign in](#)

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

- La pagina di accesso del Tenant Manager. Il campo **Account** potrebbe essere già compilato, come mostrato di seguito.

The screenshot shows the NetApp StorageGRID Tenant Manager login interface. At the top is the NetApp StorageGRID logo. Below it is the title 'Tenant Manager'. The form includes a 'Recent' dropdown menu currently showing '-- Optional --'. Below that is an 'Account' text field containing the ID '64600207336181242061'. This is followed by 'Username' and 'Password' text fields. A blue 'Sign in' button is positioned below the password field. At the bottom of the form are links for 'NetApp support' and 'NetApp.com'.

- i. Se l'ID account di 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account del tenant se appare nell'elenco degli account recenti oppure immettere l'ID account.
- ii. Inserisci il tuo nome utente e la tua password.
- iii. Seleziona * Sign in*.

Viene visualizzata la dashboard del Tenant Manager.

- iv. Se hai ricevuto una password iniziale da qualcun altro, seleziona **username** > **Cambia password** per proteggere il tuo account.

Utilizzo di SSO

Se StorageGRID utilizza SSO, viene visualizzata una delle seguenti schermate:

- La pagina SSO della tua organizzazione. Per esempio:

Sign in with your organizational account

someone@example.com

Password

Sign in

Inserisci le tue credenziali SSO standard e seleziona * Sign in*.

- Pagina di accesso SSO del Tenant Manager.

NetApp StorageGRID®

Tenant Manager

Recent

S3 tenant ▼

Account

62984032838045582045

Sign in

[NetApp support](#) | [NetApp.com](#)

- Se l'ID account di 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account del tenant se appare nell'elenco degli account recenti oppure immettere l'ID account.
- Seleziona * Sign in*.
- Sign in con le tue credenziali SSO standard alla pagina di accesso SSO della tua organizzazione.

Viene visualizzata la dashboard del Tenant Manager.

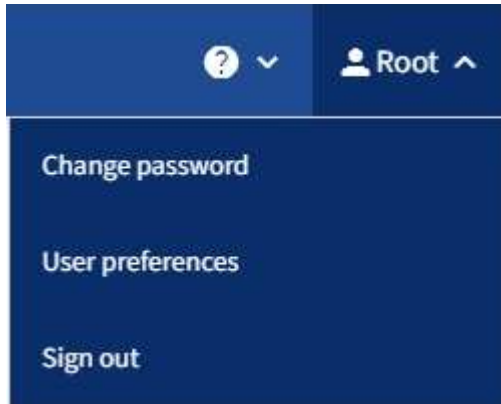
Esci da Tenant Manager

Una volta terminato di lavorare con Tenant Manager, è necessario disconnettersi per

impedire agli utenti non autorizzati di accedere al sistema StorageGRID . In base alle impostazioni dei cookie del browser, la chiusura del browser potrebbe non comportare la disconnessione dal sistema.

Passi

1. Individua il menu a discesa del nome utente nell'angolo in alto a destra dell'interfaccia utente.



2. Seleziona il nome utente e poi seleziona **Esci**.

- Se SSO non è in uso:

Hai effettuato la disconnessione dal nodo di amministrazione. Viene visualizzata la pagina di accesso del Tenant Manager.



Se hai effettuato l'accesso a più di un nodo di amministrazione, devi disconnetterti da ciascun nodo.

- Se SSO è abilitato:

Hai effettuato l'uscita da tutti i nodi amministrativi a cui stavi accedendo. Viene visualizzata la pagina Sign in a StorageGRID . Il nome dell'account tenant a cui hai appena avuto accesso è elencato come predefinito nel menu a discesa **Account recenti** e viene visualizzato l'**ID account** del tenant.



Se l'SSO è abilitato e hai effettuato l'accesso anche a Grid Manager, devi anche disconnetterti da Grid Manager per uscire dall'SSO.

Comprendere la dashboard di Tenant Manager

La dashboard di Tenant Manager fornisce una panoramica della configurazione di un account tenant e della quantità di spazio utilizzata dagli oggetti nei bucket (S3) o nei contenitori (Swift) del tenant. Se il tenant ha una quota, la dashboard mostra quanta quota è utilizzata e quanta ne rimane. Se si verificano errori relativi all'account del tenant, gli errori vengono visualizzati nella dashboard.



I valori dello spazio utilizzato sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo.

Una volta caricati gli oggetti, la dashboard apparirà come nell'esempio seguente:

Dashboard

16**Buckets**[View buckets](#)**2****Platform services****endpoints**[View endpoints](#)**0****Groups**[View groups](#)**1****User**[View users](#)

Storage usage ?

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage ?

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details ?

Name: Tenant02

ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Informazioni sull'account dell'inquilino

Nella parte superiore della dashboard viene visualizzato il numero di bucket o contenitori, gruppi e utenti configurati. Visualizza anche il numero di endpoint dei servizi della piattaforma, se ne sono stati configurati. Selezionare i link per visualizzare i dettagli.

A seconda del "[permessi di gestione degli inquilini](#)" di cui disponi e le opzioni che hai configurato, il resto della dashboard visualizza varie combinazioni di linee guida, utilizzo dello storage, informazioni sugli oggetti e dettagli sui tenant.

Utilizzo di spazio di archiviazione e quote

Il pannello Utilizzo dello spazio di archiviazione contiene le seguenti informazioni:

- La quantità di dati oggetto per il tenant.

Questo valore indica la quantità totale di dati degli oggetti caricati e non rappresenta lo spazio utilizzato per archiviare copie di tali oggetti e dei relativi metadati.

- Se è 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 possono essere acquisiti.



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 inizia a caricare oggetti e rifiuta nuovi ingest 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 finché non viene ricalcolato l'utilizzo della quota. I calcoli dell'utilizzo delle quote possono richiedere 10 minuti o più.

- Un grafico a barre che rappresenta le dimensioni relative dei contenitori o dei bucket più grandi.

È possibile posizionare il cursore su uno qualsiasi dei segmenti del grafico per visualizzare lo spazio totale occupato da quel bucket o contenitore.



- Per far corrispondere il grafico a barre, un elenco dei bucket o contenitori più grandi, inclusa la quantità totale di dati degli oggetti e il numero di oggetti per ciascun bucket o contenitore.

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 l'inquilino ha più di nove bucket o contenitori, tutti gli altri bucket o contenitori vengono combinati in un'unica voce in fondo all'elenco.



Per modificare le unità per i valori di archiviazione visualizzati in Tenant Manager, selezionare il menu a discesa dell'utente in alto a destra di Tenant Manager, quindi selezionare **Preferenze utente**.

Avvisi sull'utilizzo delle quote

Se in Grid Manager sono stati abilitati gli avvisi sull'utilizzo delle quote, questi avvisi verranno 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 **Utilizzo elevato della quota del tenant**.

Si consiglia di chiedere all'amministratore della rete di aumentare la quota.

- Se superi la tua quota, una notifica ti informa che non puoi caricare nuovi oggetti.

Limite di utilizzo della capacità

Se hai impostato un limite di capacità per i tuoi bucket, la dashboard di Tenant Manager visualizza un elenco dei bucket principali in base all'utilizzo del limite di capacità.

Se non viene impostato alcun limite per un bucket, la sua capacità è illimitata. Tuttavia, se il tuo account tenant ha una quota di archiviazione totale e tale quota viene raggiunta, non potrai acquisire altri oggetti indipendentemente dal limite di capacità rimanente su un bucket.

Errori di 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.



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.

Per vedere i dettagli su "errori dell'endpoint dei servizi della piattaforma", seleziona **Endpoint** per visualizzare la pagina Endpoint.

API di gestione degli inquilini

Comprendere l'API di gestione degli inquilini

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Tenant Management anziché l'interfaccia utente di Tenant Manager. Ad esempio, potresti voler utilizzare l'API per automatizzare le operazioni o per creare più entità, come gli utenti, più rapidamente.

API di gestione degli inquilini:

- Utilizza la piattaforma API open source Swagger. Swagger fornisce un'interfaccia utente intuitiva che consente agli sviluppatori e ai non sviluppatori di interagire con l'API. L'interfaccia utente di Swagger fornisce dettagli e documentazione completi per ogni operazione API.
- Usi "controllo delle versioni per supportare aggiornamenti non distruttivi".

Per accedere alla documentazione Swagger per l'API di gestione tenant:

1. Sign in a Tenant Manager.
2. Nella parte superiore di Tenant Manager, seleziona l'icona della guida e seleziona **Documentazione API**.

operazioni API

L'API di gestione degli inquilini organizza le operazioni API disponibili nelle seguenti sezioni:

- **account:** Operazioni sull'account del tenant corrente, incluso l'ottenimento di informazioni sull'utilizzo dello spazio di archiviazione.
- **auth:** Operazioni per eseguire l'autenticazione della sessione utente.

L'API di gestione tenant supporta lo schema di autenticazione Bearer Token. Per l'accesso del tenant, è necessario fornire un nome utente, una password e un accountId 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 successive richieste API ("Authorization: Bearer token").

Per informazioni su come migliorare la sicurezza dell'autenticazione, vedere ["Protezione contro la falsificazione delle richieste tra siti"](#).



Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), è necessario eseguire passaggi diversi per l'autenticazione. Vedi il ["istruzioni per l'utilizzo dell'API di gestione della griglia"](#).

- **config:** Operazioni relative alla versione del prodotto e alle versioni dell'API di gestione tenant. È possibile elencare la versione del prodotto e le principali versioni dell'API supportate da tale versione.
- **contenitori:** operazioni su bucket S3 o contenitori Swift.
- **deactivated-features:** Operazioni per visualizzare le funzionalità 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 StorageGRID CloudMirror.
- **grid-federation-connections:** Operazioni sulle connessioni della federazione di griglia e sulla replicazione tra griglie.
- **gruppi:** operazioni per gestire gruppi di tenant locali e per recuperare gruppi di tenant federati da una fonte di identità esterna.
- **identity-source:** Operazioni per configurare una fonte di identità esterna e per sincronizzare manualmente le informazioni sui gruppi federati e sugli utenti.
- **ilm:** Operazioni sulle impostazioni di gestione del ciclo di vita delle informazioni (ILM).
- **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 tenant.
- **s3-object-lock:** Operazioni sulle impostazioni globali di S3 Object Lock, utilizzate per supportare la conformità normativa.
- **utenti:** operazioni per visualizzare e gestire gli utenti tenant.

Dettagli dell'operazione

Espandendo ogni operazione API, è possibile visualizzare la relativa azione HTTP, l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (quando richiesto) e le possibili risposte.

groups
Operations on groups

GET
/org/groups
Lists Tenant User Groups

Parameters
Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses
Response content type
application/json

Code	Description
200	Example Value Model <pre> { "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.1" } </pre>

Inviare richieste API



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

Passi

1. Selezionare l'azione HTTP per visualizzare i dettagli della richiesta.
2. Determina se la richiesta richiede parametri aggiuntivi, come un gruppo o un ID utente. Quindi, ottieni questi valori. Potrebbe essere necessario inviare prima una richiesta API diversa per ottenere le informazioni necessarie.
3. Determina se è necessario modificare il corpo della richiesta di esempio. In tal caso, puoi selezionare **Modello** per conoscere i requisiti per ciascun campo.

4. Seleziona **Provalo**.
5. Fornire tutti i parametri richiesti o modificare il corpo della richiesta come richiesto.
6. Selezionare **Esegui**.
7. Esaminare il codice di risposta per determinare se la richiesta è andata a buon fine.

Versionamento dell'API di gestione degli inquilini

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 aggiornata quando vengono apportate modifiche che non sono compatibili con le versioni precedenti. La versione secondaria dell'API viene aggiornata quando vengono apportate modifiche *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o nuove proprietà.

L'esempio seguente illustra come la versione dell'API viene aumentata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Vecchia versione	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con le versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene abilitata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova versione delle funzionalità di StorageGRID, si continua ad avere accesso alla versione API precedente per almeno una versione delle funzionalità StorageGRID.



È possibile configurare le versioni supportate. Consultare la sezione **config** della documentazione dell'API Swagger per "[API di gestione della griglia](#)" per maggiori informazioni. Dopo aver aggiornato tutti i client API per utilizzare la versione più recente, è necessario disattivare il supporto per la versione precedente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Obsoleto: vero"
- Il corpo della risposta JSON include "deprecated": true
- Un avviso obsoleto è stato aggiunto a nms.log. Per esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determina quali versioni API sono supportate nella versione corrente

Utilizzare il GET `/versions` Richiesta API per restituire un elenco delle principali versioni 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 API utilizzando un parametro di percorso(`/api/v4`) o un'intestazione(`Api-Version: 4`). Se si specificano 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 falsificazione delle richieste tra siti (CSRF)

È possibile contribuire a proteggersi dagli attacchi CSRF (Cross-Site Request Forgery) 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 abilitarla o meno al momento dell'accesso.

Un aggressore in grado di attivare una richiesta a un sito diverso (ad esempio con un modulo HTTP POST) può far sì che determinate richieste vengano effettuate utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggersi dagli attacchi CSRF utilizzando i token CSRF. Se abilitato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro del corpo POST specifico.

Per abilitare 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 è impostato con un valore casuale per gli accessi a Grid Manager e `AccountCsrfToken` il cookie viene impostato con un valore casuale per gli accessi al Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere uno dei seguenti elementi:

- IL `X-Csrf-Token` intestazione, con il valore dell'intestazione impostato sul valore del cookie token CSRF.
- Per gli endpoint che accettano un corpo codificato in formato: A `csrfToken` parametro del corpo della richiesta codificato nel modulo.

Per configurare la protezione CSRF, utilizzare ["API di gestione della griglia"](#) O ["API di gestione degli inquilini"](#) .



Le richieste che hanno impostato un 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 rete

Clona gruppi tenant e utenti

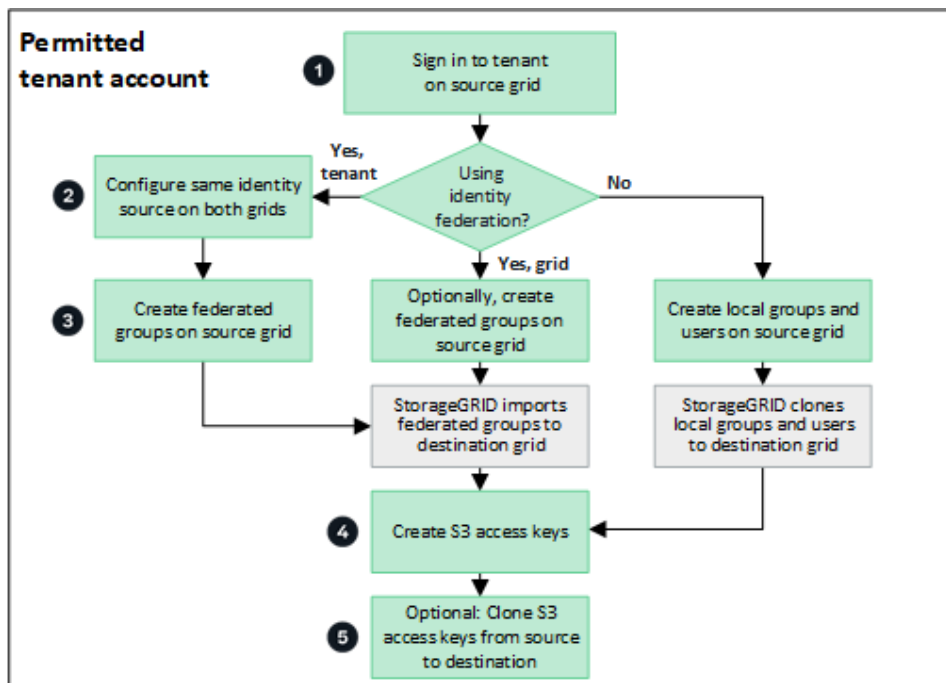
Se un tenant è stato creato o modificato per utilizzare una connessione di federazione della griglia, tale tenant viene replicato da un sistema StorageGRID (il tenant di origine) a un altro sistema StorageGRID (il tenant di replica). Dopo che il tenant è stato replicato, tutti i gruppi e gli utenti aggiunti al tenant di origine vengono clonati nel tenant replica.

Il sistema StorageGRID in cui il tenant viene creato originariamente è la *griglia sorgente* 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 archiviazione e autorizzazioni assegnate, ma il tenant di destinazione inizialmente non ha una password utente root. Per i dettagli, vedere ["Che cosa è il clone dell'account"](#) E ["Gestire gli inquilini autorizzati"](#) .

La clonazione delle informazioni dell'account dell'inquilino è richiesta per ["replicazione cross-grid"](#) di oggetti secchio. Avere gli stessi gruppi di tenant e utenti su entrambe le griglie garantisce l'accesso ai bucket e agli oggetti corrispondenti su entrambe le griglie.

Flusso di lavoro del tenant per la clonazione dell'account

Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, rivedi il diagramma del flusso di lavoro per vedere i passaggi da eseguire per clonare gruppi, utenti e chiavi di accesso S3.



Questi sono i passaggi principali del flusso di lavoro:

1

Sign in al tenant

Sign in all'account del tenant sulla griglia di origine (la griglia in cui è stato inizialmente creato il tenant).

2

Facoltativamente, configurare la federazione delle identità

Se il tuo account tenant dispone dell'autorizzazione **Usa la propria origine identità** per utilizzare gruppi e utenti federati, configura la stessa origine identità (con le stesse impostazioni) sia per l'account tenant di origine che per quello di destinazione. I gruppi e gli utenti federati non possono essere clonati a meno che entrambe le griglie non utilizzino la stessa origine identità. Per le istruzioni, vedere ["Utilizzare la federazione delle identità"](#).

3

Crea gruppi e utenti

Quando si creano gruppi e utenti, iniziare sempre dalla griglia di origine del tenant. Quando aggiungi un nuovo gruppo, StorageGRID lo clona automaticamente nella griglia di destinazione.

- Se la federazione delle identità è configurata per l'intero sistema StorageGRID o per il tuo account tenant, ["creare nuovi gruppi di tenant"](#) importando gruppi federati dalla fonte dell'identità.
- Se non si utilizza la federazione delle identità, ["creare nuovi gruppi locali"](#) poi ["creare utenti locali"](#).

4

Crea chiavi di accesso S3

Puoi ["crea le tue chiavi di accesso"](#) o ["creare le chiavi di accesso di un altro utente"](#) sulla griglia di origine o sulla griglia di destinazione per accedere ai bucket su quella griglia.

Facoltativamente, clona le chiavi di accesso S3

Se devi accedere ai bucket con le stesse chiavi di accesso su entrambe le griglie, crea le chiavi di accesso sulla griglia di origine e poi usa l'API Tenant Manager per clonarle manualmente sulla griglia di destinazione. Per le istruzioni, vedere ["Clona le chiavi di accesso S3 utilizzando l'API"](#).

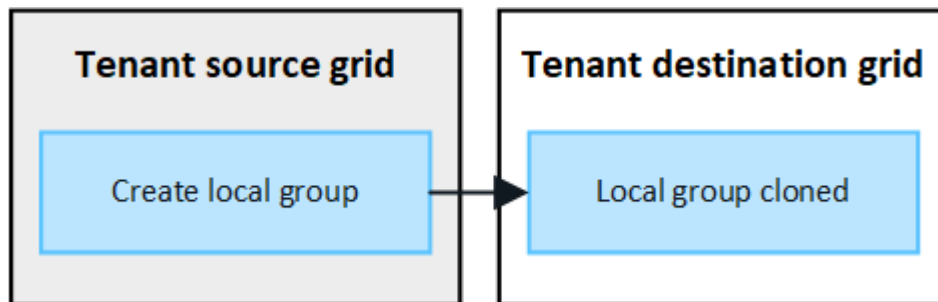
Come vengono clonati gruppi, utenti e chiavi di accesso S3?

Esaminare questa sezione per comprendere come gruppi, utenti e chiavi di accesso S3 vengono clonati 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 che un account tenant è stato creato e replicato nella griglia di destinazione, StorageGRID clona automaticamente tutti i gruppi locali aggiunti alla griglia di origine del tenant nella griglia di destinazione del tenant.

Sia il gruppo originale che il suo clone hanno la stessa modalità di accesso, le stesse autorizzazioni di gruppo e la stessa policy di gruppo S3. Per le istruzioni, vedere ["Crea gruppi per il tenant S3"](#).

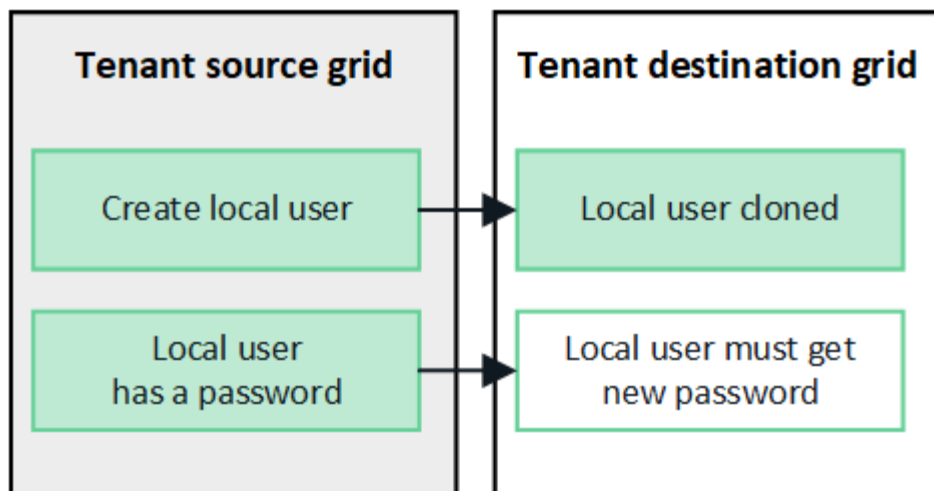


Tutti gli utenti selezionati quando si crea un gruppo locale nella griglia di origine non vengono inclusi quando il gruppo viene clonato nella griglia di destinazione. Per questo motivo, non selezionare gli utenti quando crei il gruppo. In alternativa, seleziona il gruppo quando crei gli utenti.

Gli utenti locali creati sulla griglia di origine vengono clonati

Quando si crea un nuovo utente locale sulla griglia di origine, StorageGRID clona automaticamente tale utente nella griglia di destinazione. Sia l'utente originale che il suo clone hanno lo stesso nome completo, lo stesso nome utente e l'impostazione **Nega accesso**. Entrambi gli utenti appartengono anche agli stessi gruppi. Per le istruzioni, vedere ["Gestisci 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 sulla griglia di destinazione, l'utente root dell'account tenant deve aggiungere una password per tale utente sulla griglia di destinazione. Per le istruzioni, vedere ["Gestisci gli utenti locali"](#).

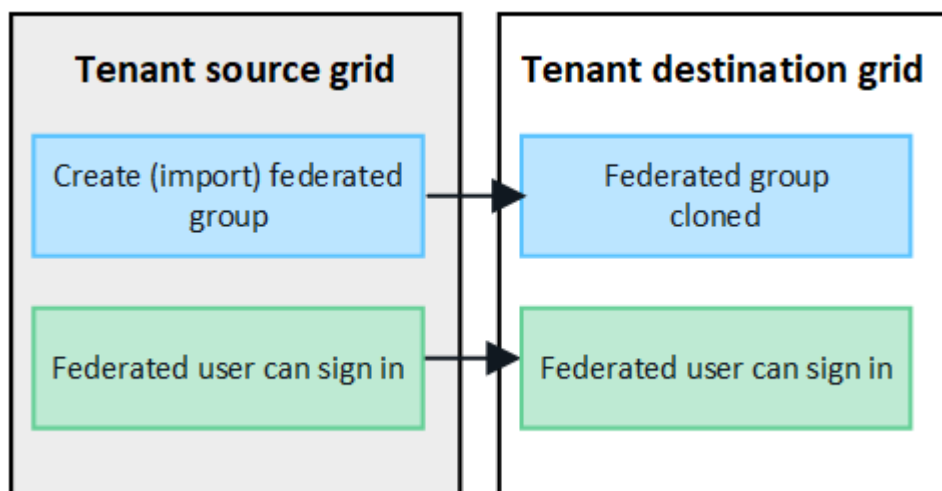


I gruppi federati creati sulla griglia di origine vengono clonati

Supponendo che i requisiti per l'utilizzo del clone dell'account con ["accesso unico"](#) E ["federazione di identità"](#) sono stati soddisfatti, i gruppi federati creati (importati) per il tenant nella griglia di origine vengono automaticamente clonati nel tenant nella griglia di destinazione.

Entrambi i gruppi hanno la stessa modalità di accesso, le stesse autorizzazioni di gruppo e la stessa policy di gruppo S3.

Dopo che i gruppi federati sono stati creati per il tenant di origine e clonati nel tenant di destinazione, gli utenti federati possono accedere al tenant su entrambe le griglie.

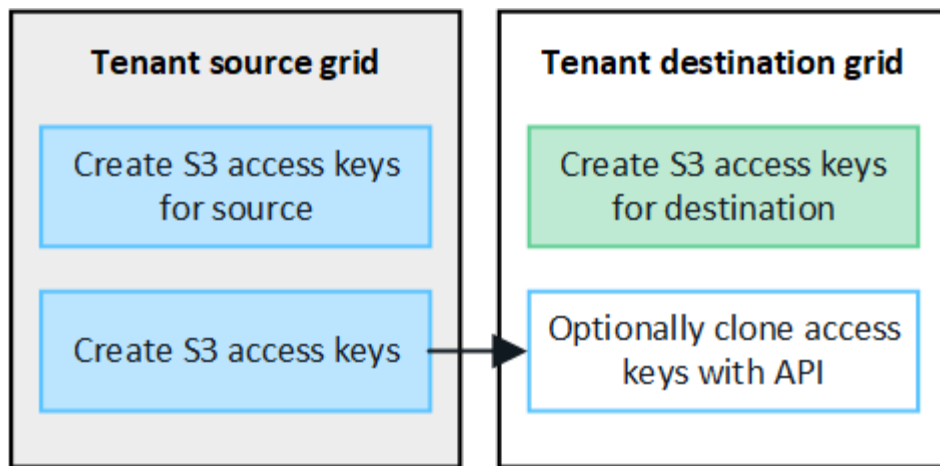


Le chiavi di accesso S3 possono essere clonate manualmente

StorageGRID non clona automaticamente le chiavi di accesso S3 perché la sicurezza è migliorata dalla presenza di chiavi diverse su ogni griglia.

Per gestire le chiavi di accesso sulle due griglie, puoi procedere in uno dei seguenti modi:

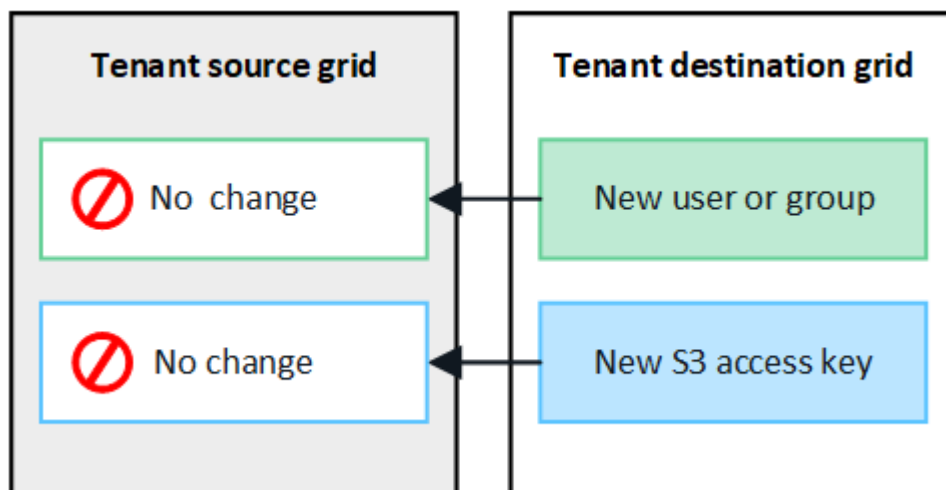
- Se non hai bisogno di usare le stesse chiavi per ogni griglia, puoi ["crea le tue chiavi di accesso"](#) O ["creare le chiavi di accesso di un altro utente"](#) su ogni griglia.
- Se devi utilizzare le stesse chiavi su entrambe le griglie, puoi creare chiavi sulla griglia di origine e quindi utilizzare l'API Tenant Manager per crearle manualmente ["clonare le chiavi"](#) alla griglia di destinazione.



Quando si clonano le chiavi di accesso S3 per un utente federato, sia l'utente sia le chiavi di accesso S3 vengono clonati nel tenant di destinazione.

I gruppi e gli utenti aggiunti alla griglia di destinazione non vengono clonati

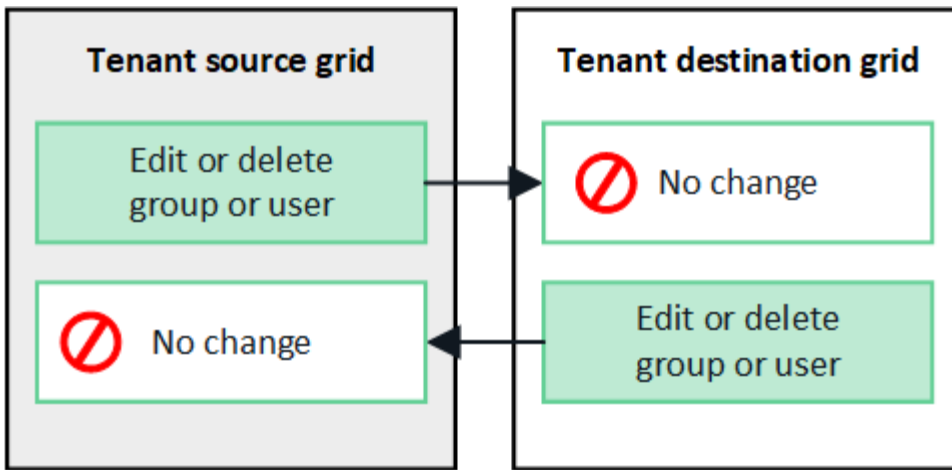
La clonazione avviene solo dalla griglia di origine del tenant alla griglia di destinazione del tenant. Se si creano o si importano gruppi e utenti nella griglia di destinazione del tenant, StorageGRID non clonerà questi elementi nella griglia di origine del tenant.



I gruppi, gli utenti e le chiavi di accesso modificati o eliminati non vengono clonati

La clonazione avviene solo quando si creano nuovi gruppi e utenti.

Se modifichi o elimini gruppi, utenti o chiavi di accesso su una delle due griglie, le modifiche non verranno clonate nell'altra griglia.



Clona le chiavi di accesso S3 utilizzando l'API

Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, puoi 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 ha l'autorizzazione **Usa connessione federata alla griglia**.
- La connessione della federazione di rete ha uno **Stato di connessione** pari a **Connesso**.
- Hai effettuato l'accesso al Tenant Manager sulla griglia di origine del tenant utilizzando un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["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 sia le chiavi di accesso S3 vengono aggiunti al tenant di destinazione.

Clona le tue chiavi di accesso

Puoi clonare le tue chiavi di accesso se hai bisogno di accedere agli stessi bucket su entrambe le griglie.

Passi

1. Utilizzando Tenant Manager sulla griglia di origine, ["crea le tue chiavi di accesso"](#) e scarica il `.csv` file.
2. Nella parte superiore di Tenant Manager, seleziona l'icona della guida e seleziona **Documentazione API**.
3. Nella sezione **s3**, seleziona il seguente endpoint:

```
POST /org/users/current-user/replicate-s3-access-key
```

POST

`/org/users/current-user/replicate-s3-access-key` Clone the current user's S3 key to the other grids.



4. Seleziona **Provalo**.
5. Nella casella di testo **corpo**, sostituisci le voci di esempio per **accessKey** e **secretAccessKey** con i valori del file `.csv` scaricato.

Assicuratevi di mantenere le virgolette doppie attorno a ciascuna stringa.



```
{
  "accessKey": "AKIAIOSFODNN7EXAMPLE",
  "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
  "expires": "2028-09-04T00:00:00.000Z"
}
```

6. Se la chiave scadrà, sostituire la voce di esempio per **expires** con la data e l'ora di scadenza come stringa nel formato data-ora ISO 8601 (ad esempio, 2024-02-28T22:46:33-08:00). Se la chiave non scade, immettere **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.

Clona le chiavi di accesso di un altro utente

È possibile clonare le chiavi di accesso di un altro utente se quest'ultimo ha bisogno di accedere agli stessi bucket su entrambe le griglie.

Passi

1. Utilizzando Tenant Manager sulla griglia di origine, "[creare le chiavi di accesso S3 dell'altro utente](#)" e scarica il .csv file.
2. Nella parte superiore di Tenant Manager, seleziona l'icona della guida e seleziona **Documentazione API**.
3. Ottieni l'ID utente. Questo valore ti servirà per clonare le chiavi di accesso dell'altro utente.
 - a. Dalla sezione **utenti**, seleziona il seguente endpoint:

```
GET /org/users
```
 - b. Seleziona **Provalo**.
 - c. Specificare i parametri che si desidera utilizzare durante la ricerca degli utenti.
 - d. Selezionare **Esegui**.
 - e. Trova l'utente di cui vuoi clonare le chiavi e copia il numero nel campo **id**.
4. Nella sezione **s3**, seleziona il seguente endpoint:

```
POST /org/users/{userId}/replicate-s3-access-key
```



```
POST /org/users/{userId}/replicate-s3-access-key Clone an S3 key to the other grids.
```

5. Seleziona **Provalo**.
6. Nella casella di testo **userId**, incolla l'ID utente che hai copiato.
7. Nella casella di testo **corpo**, sostituire le voci di esempio per **chiave di accesso di esempio** e **chiave di accesso segreta** con i valori del file .csv per quell'utente.

Assicuratevi di mantenere le virgolette doppie attorno alla stringa.

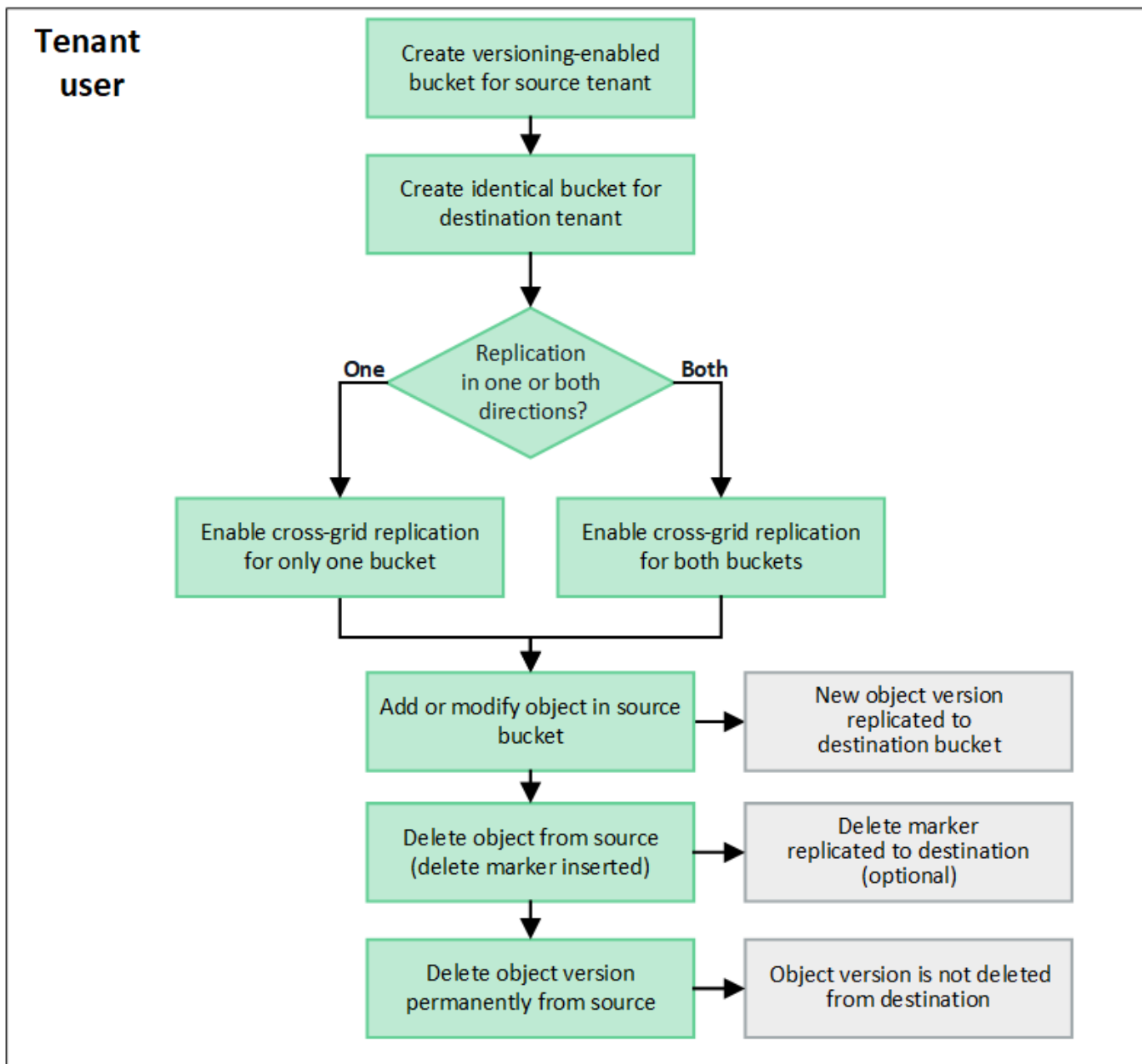
8. Se la chiave scadrà, sostituire la voce di esempio per **expires** con la data e l'ora di scadenza come stringa nel formato data-ora ISO 8601 (ad esempio, 2023-02-28T22:46:33-08:00). Se la chiave non scade, immettere **null** come valore per la voce **expires** (oppure rimuovere la riga **Expires** 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 replicazione tra griglie

Se al momento della creazione dell'account tenant è stata assegnata l'autorizzazione **Usa connessione federazione griglia**, è possibile utilizzare la replica tra griglie per replicare automaticamente gli oggetti tra i bucket sulla griglia di origine del tenant e i bucket sulla griglia di destinazione del tenant. La replicazione tra griglie può avvenire in una o entrambe le direzioni.

Flusso di lavoro per la replicazione tra griglie

Il diagramma del flusso di lavoro riassume i passaggi da eseguire per configurare la replica tra griglie tra bucket su due griglie. Questi passaggi sono descritti più dettagliatamente di seguito.



Configurare la replicazione tra griglie

Prima di poter utilizzare la replica tra griglie, è necessario accedere agli account tenant corrispondenti su ciascuna griglia e creare bucket identici. Quindi, è possibile abilitare la replica tra griglie su uno o entrambi i bucket.

Prima di iniziare

- Hai esaminato i requisiti per la replicazione tra griglie. Vedere ["Che cosa è la replicazione cross-grid"](#).
- Stai utilizzando un ["browser web supportato"](#).
- L'account tenant ha l'autorizzazione **Usa connessione federata di griglia** e su entrambe le griglie esistono account tenant identici. Vedere ["Gestire gli inquilini autorizzati per la connessione alla federazione di rete"](#).
- L'utente tenant con cui effettuerai l'accesso esiste già su entrambe le griglie e appartiene a un gruppo di utenti che ha ["Permesso di accesso root"](#).

- Se effettuerai l'accesso alla griglia di destinazione del tenant come utente locale, l'utente root dell'account tenant avrà impostato una password per il tuo account utente su quella griglia.

Crea due bucket identici

Come primo passo, accedi agli account tenant corrispondenti su ciascuna griglia e crea bucket identici.

Passi

1. Partendo da una delle due griglie nella connessione di federazione delle griglie, crea un nuovo bucket:
 - a. Sign in all'account tenant utilizzando le credenziali di un utente tenant presente su entrambe le griglie.



Se non riesci ad accedere alla griglia di destinazione del tenant come utente locale, verifica che l'utente root dell'account tenant abbia impostato una password per il tuo account utente.

- b. Seguire le istruzioni per ["creare un bucket S3"](#).
 - c. Nella scheda **Gestisci impostazioni oggetto**, seleziona **Abilita controllo delle versioni degli oggetti**.
 - d. Se S3 Object Lock è abilitato per il sistema StorageGRID, non abilitare S3 Object Lock per il bucket.
 - e. Seleziona **Crea bucket**.
 - f. Selezionare **Fine**.
2. Ripetere questi passaggi per creare un bucket identico per lo stesso account tenant sull'altra griglia nella connessione di federazione della griglia.



A seconda delle necessità, ogni bucket può utilizzare una regione diversa.

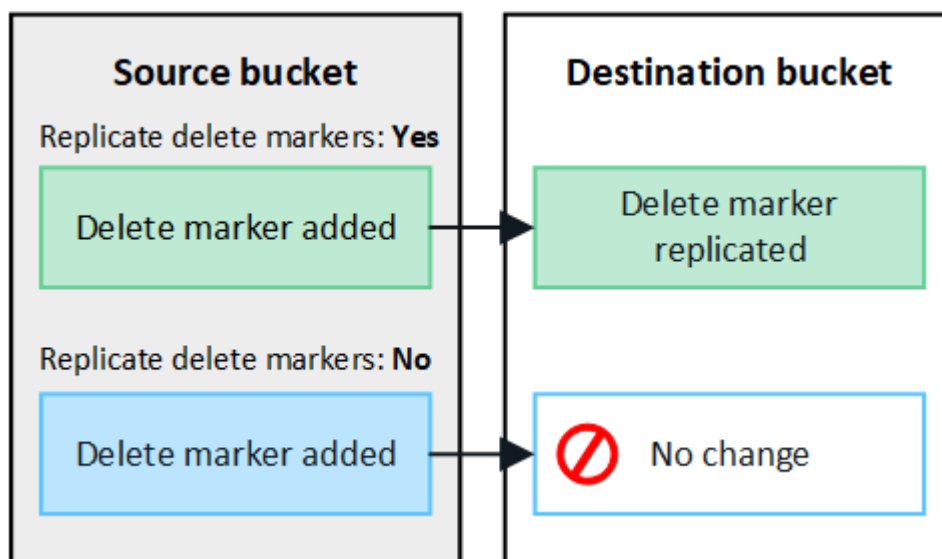
Abilita la replicazione tra griglie

È necessario eseguire questi passaggi prima di aggiungere oggetti a uno dei due bucket.

Passi

1. Partendo da una griglia di cui vuoi replicare gli oggetti, abilita ["replicazione cross-grid in una direzione"](#):
 - a. Sign in all'account tenant per il bucket.
 - b. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
 - c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
 - d. Selezionare la scheda **Replica tra griglie**.
 - e. Selezionare **Abilita** e rivedere l'elenco dei requisiti.
 - f. Se tutti i requisiti sono stati soddisfatti, selezionare la connessione di federazione di rete che si desidera utilizzare.
 - g. Facoltativamente, modifica l'impostazione di **Replica marcatori di eliminazione** per determinare cosa accade sulla griglia di destinazione se un client S3 invia una richiesta di eliminazione alla griglia di origine che non include un ID versione:
 - **Sì** (predefinito): 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 versione, la versione dell'oggetto viene rimossa definitivamente dal bucket di origine. StorageGRID non replica le richieste di eliminazione che includono un ID versione, pertanto la stessa versione dell'oggetto non viene eliminata dalla destinazione.

Vedere ["Che cosa è la replicazione cross-grid"](#) per i dettagli.

- Facoltativamente, modificare l'impostazione della categoria di controllo **Replica tra griglie** per gestire il volume dei messaggi di controllo:
 - **Errore** (predefinito): nell'output di controllo vengono incluse solo le richieste di replica tra griglie non riuscite.
 - **Normale**: vengono incluse tutte le richieste di replica tra griglie, il che aumenta significativamente il volume dell'output di audit.
- Rivedi le tue selezioni. Non è possibile modificare queste impostazioni a meno che entrambi i bucket non siano vuoti.
- Seleziona **Abilita e prova**.

Dopo qualche istante, verrà visualizzato un messaggio di conferma dell'operazione. Gli oggetti aggiunti a questo bucket verranno ora replicati automaticamente nell'altra griglia. **La replica tra griglie** è visualizzata come funzionalità abilitata nella pagina dei dettagli del bucket.

- Facoltativamente, vai al bucket corrispondente sull'altra griglia e ["abilitare la replicazione cross-grid in entrambe le direzioni"](#).

Test di replicazione tra griglie

Se la replica tra griglie è abilitata per un bucket, potrebbe essere necessario verificare che la connessione e la replica tra griglie funzionino correttamente e che i bucket di origine e di destinazione soddisfino ancora tutti i requisiti (ad esempio, che il controllo delle versioni sia ancora abilitato).

Prima di iniziare

- Stai utilizzando un ["browser web supportato"](#).

- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#) .

Passi

1. Sign in all'account tenant per il bucket.
2. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
3. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
4. Selezionare la scheda **Replica tra griglie**.
5. Selezionare **Test connessione**.

Se la connessione è funzionante, viene visualizzato un banner di conferma. In caso contrario, verrà visualizzato un messaggio di errore che tu e l'amministratore della griglia potrete utilizzare per risolvere il problema. Per maggiori dettagli, vedere ["Risolvere gli errori di federazione della griglia"](#) .

6. Se la replica tra griglie è configurata per verificarsi in entrambe le direzioni, andare al bucket corrispondente sull'altra griglia e selezionare **Test connessione** per verificare che la replica tra griglie funzioni nell'altra direzione.

Disabilita la replicazione tra griglie

È possibile interrompere definitivamente la replica tra griglie se non si desidera più copiare oggetti nell'altra griglia.

Prima di disattivare la replica tra griglie, tenere presente quanto segue:

- La disattivazione della replica tra griglie non rimuove gli oggetti già copiati tra le griglie. Ad esempio, oggetti in my-bucket sulla Griglia 1 che sono stati copiati in my-bucket sulla Griglia 2 non vengono rimossi se si disabilita la replica tra griglie per quel bucket. Se si desidera eliminare questi oggetti, è necessario rimuoverli manualmente.
- Se la replica tra griglie è stata abilitata per ciascuno dei bucket (ovvero, se la replica avviene in entrambe le direzioni), è possibile disabilitare la replica tra griglie per uno o entrambi i bucket. Ad esempio, potresti voler disabilitare la replica degli oggetti da my-bucket sulla griglia 1 a my-bucket sulla Griglia 2, continuando a replicare oggetti da my-bucket sulla griglia 2 a my-bucket sulla griglia 1.
- È necessario disabilitare la replica tra griglie prima di poter rimuovere l'autorizzazione di un tenant a utilizzare la connessione federata della griglia. Vedere ["Gestire gli inquilini autorizzati"](#) .
- Se si disabilita la replica tra griglie per un bucket contenente oggetti, non sarà possibile riabilitarla a meno che non si eliminino tutti gli oggetti sia dal bucket di origine che da quello di destinazione.



Non è possibile riattivare la replica a meno che entrambi i bucket non siano vuoti.

Prima di iniziare

- Stai utilizzando un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#) .

Passi

1. A partire dalla griglia i cui oggetti non vuoi più replicare, interrompi la replica tra griglie per il bucket:
 - a. Sign in all'account tenant per il bucket.
 - b. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
 - c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.

- d. Selezionare la scheda **Replica tra griglie**.
- e. Selezionare **Disabilita replicazione**.
- f. Se sei sicuro di voler disabilitare la replica tra griglie per questo bucket, digita **Sì** nella casella di testo e seleziona **Disabilita**.

Dopo qualche istante, verrà visualizzato un messaggio di conferma dell'operazione. I nuovi oggetti aggiunti a questo bucket non possono più essere replicati automaticamente nell'altra griglia. La **replica tra griglie** non è più visualizzata come funzionalità abilitata nella pagina Bucket.

2. Se la replica tra griglie è stata configurata per essere eseguita in entrambe le direzioni, passare al bucket corrispondente sull'altra griglia e interrompere la replica tra griglie nell'altra direzione.

Visualizza le connessioni della federazione di griglia

Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federata alla griglia**, puoi visualizzare le connessioni consentite.

Prima di iniziare

- L'account tenant ha l'autorizzazione **Usa connessione federata alla griglia**.
- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#).

Passi

1. Selezionare **STORAGE (S3) > Connessioni federazione di rete**.

Viene visualizzata la pagina di connessione della federazione Grid, che include una tabella che riassume le seguenti informazioni:

Colonna	Descrizione
Nome della connessione	Le connessioni della federazione di rete che questo tenant è autorizzato a utilizzare.
Bucket con replicazione cross-grid	Per ogni connessione di federazione di griglia, i bucket tenant che hanno abilitata la replica tra griglie. Gli oggetti aggiunti a questi bucket verranno replicati nell'altra griglia nella connessione.
Ultimo errore	Per ogni connessione di federazione di griglia, l'errore più recente verificatosi, se presente, durante la replica dei dati sull'altra griglia. Vedere Cancella l'ultimo errore .

2. Facoltativamente, seleziona un nome bucket per ["visualizza i dettagli del bucket"](#).

Cancella l'ultimo errore

Potrebbe apparire un errore nella colonna **Ultimo errore** per uno dei seguenti motivi:

- La versione dell'oggetto sorgente non è stata trovata.
- Il bucket di origine non è stato trovato.

- Il bucket di destinazione è stato eliminato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il controllo delle versioni del bucket di destinazione è sospeso.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più sottoposto a controllo di versione.



Questa colonna mostra solo l'ultimo errore di replicazione tra griglie verificatosi; gli errori precedenti che potrebbero essersi verificati non verranno mostrati.

Passi

1. Se nella colonna **Ultimo errore** viene visualizzato un messaggio, visualizzarne il testo.

Ad esempio, questo errore indica che il bucket di destinazione per la replica tra griglie era in uno stato non valido, probabilmente perché il controllo delle versioni era sospeso o era abilitato S3 Object Lock.

Grid federation connections			
Clear error		Search...	
		Displaying one result	
Connection name	Buckets with cross-grid replication	Last error	
Grid 1-Grid 2	my-cgr-bucket	2022-12-07 16:02:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)	

2. Eseguire tutte le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso sul bucket di destinazione per la replica tra griglie, riattivare il controllo delle versioni per quel bucket.
3. Selezionare la connessione dalla tabella.
4. Seleziona **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Aspetta 5-6 minuti e poi ingerisci un nuovo oggetto nel secchio. Verificare che il messaggio di errore non venga più visualizzato.



Per garantire che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo il timestamp nel messaggio prima di acquisire un nuovo oggetto.

7. Per determinare se la replica di alcuni oggetti non è riuscita a causa dell'errore del bucket, vedere ["Identificare e riprovare le operazioni di replicazione non riuscite"](#).

Gestisci gruppi e utenti

Utilizzare la federazione delle identità

L'utilizzo della federazione delle identità velocizza 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 Tenant Manager se si desidera che i gruppi e gli utenti dei 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 tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#).
- Stai utilizzando Active Directory, Azure AD, OpenLDAP o Oracle Directory Server come provider di identità.



Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare l'assistenza tecnica.

- Se si prevede di utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere [Linee guida per la configurazione del server OpenLDAP](#).
- Se si prevede di utilizzare Transport Layer Security (TLS) per le comunicazioni con il server LDAP, il provider di identità deve utilizzare TLS 1.2 o 1.3. Vedere ["Cifrature supportate per le connessioni TLS in uscita"](#).

Informazioni su questo compito

La possibilità di configurare un servizio di federazione delle identità per il tenant dipende da come è stato configurato l'account del tenant. Il tenant potrebbe condividere il servizio di federazione delle identità configurato per Grid Manager. Se visualizzi questo messaggio quando accedi alla pagina Federazione delle identità, non puoi configurare un'origine di identità federata separata per questo tenant.



This tenant account uses the LDAP server that is configured for the Grid Manager.
Contact the grid administrator for information or to change this setting.

Inserisci la configurazione

Quando si configura la federazione delle identità, si forniscono i valori necessari a StorageGRID per connettersi a un servizio LDAP.

Passi

1. Selezionare **GESTIONE ACCESSI > Federazione identità**.
2. Selezionare **Abilita federazione delle identità**.
3. Nella sezione Tipo di servizio LDAP, seleziona il tipo di servizio LDAP che desideri configurare.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

Azure

OpenLDAP

Other

Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se hai selezionato **Altro**, compila i campi nella sezione Attributi LDAP. procedere al passaggio successivo.
 - **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`. Il valore di ciascun utente per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
 - **Nome univoco del 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 di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
5. Per tutti i tipi di servizio LDAP, immettere le informazioni richieste sul server LDAP e sulla connessione di rete nella sezione Configura server LDAP.
 - **Nome host:** nome di dominio completo (FQDN) o indirizzo IP del server LDAP.
 - **Porta:** la porta utilizzata per connettersi al server LDAP.



La porta predefinita per STARTTLS è 389, mentre la porta predefinita per LDAPS è 636. Tuttavia, puoi utilizzare qualsiasi porta, a patto che il firewall sia configurato correttamente.

- **Nome utente:** percorso completo del nome distinto (DN) dell'utente che si conatterà al server LDAP.

Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome dell'entità utente.

L'utente specificato deve avere l'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

- `sAMAccountName`O `uid`
- `objectGUID, entryUUID , O nsuniqueid`
- `cn`
- `memberOf`O `isMemberOf`
- **Directory attiva:** `objectSid , primaryGroupID , userAccountControl , E userPrincipalName`
- **Azzurro:** `accountEnabled E userPrincipalName`
- **Password:** la password associata al nome utente.



Se in futuro dovessi cambiare la password, dovrai aggiornarla in questa pagina.

- **DN base gruppo:** percorso completo del nome distinto (DN) per un sottoalbero LDAP in cui si desidera cercare i gruppi. Nell'esempio di Active Directory (sotto), 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 **Nome univoco del gruppo** devono essere univoci all'interno del **DN di base del gruppo** a cui appartengono.

- **DN base utente:** percorso completo del nome distinto (DN) di un sottoalbero LDAP in cui si desidera cercare gli utenti.



I valori **Nome univoco utente** devono essere univoci all'interno del **Nome base utente** a cui appartengono.

- **Formato nome utente associato** (facoltativo): il modello di nome utente predefinito che StorageGRID dovrebbe utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il **formato nome utente di associazione** perché può consentire agli utenti di accedere se StorageGRID non è in grado di associarsi all'account di servizio.

Inserisci 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 di nome distinto:** CN=[USERNAME],CN=Users,DC=example,DC=com

Includi [USERNAME] esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), seleziona un'impostazione di sicurezza.

- **Usa STARTTLS:** usa STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma non è supportata per Azure.
- **Usa LDAPS:** l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario 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 impone la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

7. Se hai selezionato STARTTLS o LDAPS, scegli il certificato utilizzato per proteggere la connessione.

- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni.
- **Utilizza certificato CA personalizzato:** utilizza un certificato di sicurezza personalizzato.

Se selezioni questa impostazione, copia e incolla il certificato di sicurezza personalizzato nella casella di testo Certificato CA.

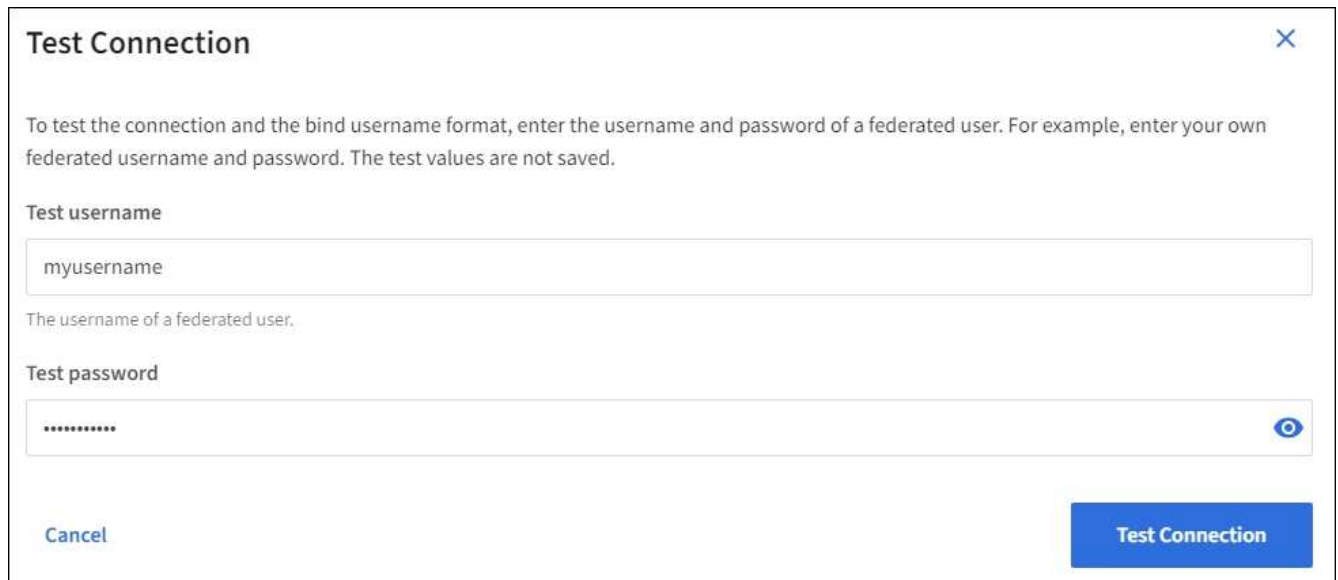
Testare la connessione e salvare la configurazione

Dopo aver immesso tutti i valori, è necessario testare la connessione prima di poter salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente associato, se ne è stato fornito uno.

Passi

1. Selezionare **Test connessione**.
2. Se non hai fornito un formato di nome utente di associazione:
 - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di 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, risolvi eventuali problemi e verifica nuovamente la connessione.
3. Se hai fornito un formato di nome utente vincolato, inserisci il nome utente e la password di un utente federato valido.

Ad esempio, inserisci il tuo nome utente e la tua password. Non includere caratteri speciali nel nome utente, come @ o /.



- Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di connessione riuscito". Selezionare **Salva** per salvare la configurazione.
- Se le impostazioni di connessione, il formato del nome utente associato o il nome utente e la password di prova non sono validi, viene visualizzato un messaggio di errore. Risolvi eventuali problemi e verifica nuovamente la connessione.

Forza la sincronizzazione con la fonte dell'identità

Il sistema StorageGRID sincronizza periodicamente i gruppi federati e gli utenti dalla fonte di identità. È possibile forzare l'avvio della sincronizzazione se si desidera abilitare o limitare le autorizzazioni utente il più rapidamente possibile.

Passi

1. Vai alla pagina Federazione delle identità.

2. Seleziona **Sincronizza server** nella parte superiore della pagina.

Il processo di sincronizzazione potrebbe richiedere del tempo, a seconda dell'ambiente.



L'avviso **Errore di sincronizzazione della federazione delle identità** viene attivato se si verifica un problema durante la sincronizzazione di gruppi e utenti federati dall'origine dell'identità.

Disabilitare la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione delle identità per gruppi e utenti. Quando la federazione delle identità è disabilitata, non c'è comunicazione tra StorageGRID e l'origine dell'identità. Tuttavia, tutte le impostazioni configurate vengono mantenute, consentendoti di riattivare facilmente la federazione delle identità in futuro.

Informazioni su questo compito

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno effettuare l'accesso.
- Gli utenti federati attualmente connessi manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno effettuare l'accesso dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non verrà eseguita e non verranno generati avvisi per gli account che non sono stati sincronizzati.
- La casella di controllo **Abilita federazione delle identità** è disabilitata se l'accesso Single Sign-On (SSO) è impostato su **Abilitato** o **Modalità Sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere "[Disabilitare l'accesso singolo](#)".

Passi

1. Vai alla pagina Federazione delle identità.
2. Deseleziona la casella di controllo **Abilita federazione delle 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 origini identità diverse da ActiveDirectory o Azure, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare tutte le chiavi S3 dell'utente o rimuovere l'utente da tutti i gruppi.

Sovrapposizioni di membri e raffinazione

Le sovrapposizioni memberof e refint dovrebbero essere abilitate. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo in <http://www.openldap.org/doc/admin24/index.html> ["Documentazione OpenLDAP: Guida dell'amministratore 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, assicurati che i campi menzionati nella guida per Nome utente siano indicizzati per prestazioni ottimali.

Consultare le informazioni sul mantenimento dell'appartenenza al gruppo inverso in <http://www.openldap.org/doc/admin24/index.html> ["Documentazione OpenLDAP: Guida dell'amministratore versione 2.4"^] .

Gestire 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 tramite un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#) .
- Se si prevede di importare un gruppo federato, è necessario ["federazione di identità configurata"](#) e il gruppo federato esiste già nell'origine identità configurata.
- Se il tuo account tenant ha l'autorizzazione **Usa connessione federazione griglia**, hai esaminato il flusso di lavoro e le considerazioni per ["clonazione di gruppi di tenant e utenti"](#) e hai effettuato l'accesso alla griglia di origine del tenant.

Accedi alla procedura guidata Crea gruppo

Come primo passo, accedi alla procedura guidata Crea gruppo.

Passi

1. Selezionare **GESTIONE ACCESSI > Gruppi**.
2. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, verifica che venga visualizzato un banner blu, che indica che i nuovi gruppi creati su questa griglia verranno clonati nello stesso tenant sull'altra griglia nella connessione. Se questo banner non viene visualizzato, è possibile che tu abbia effettuato l'accesso alla griglia di destinazione del tenant.

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

0 groups

Create group

Actions ▾

i This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New local tenant groups will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.

3. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federato.

Passi

1. Selezionare la scheda **Gruppo locale** per creare un gruppo locale oppure selezionare la scheda **Gruppo federato** per importare un gruppo dall'origine identità configurata in precedenza.

Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), gli utenti appartenenti a gruppi locali non potranno accedere a Tenant Manager, sebbene possano utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni del gruppo.

2. Inserisci il nome del gruppo.

- **Gruppo locale:** immettere sia un nome visualizzato che un nome univoco. Potrai 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 sulla griglia di destinazione.

- **Gruppo federato:** 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**.

Gestisci i permessi del gruppo

Le autorizzazioni di gruppo controllano quali attività gli utenti possono eseguire in Tenant Manager e nell'API Tenant Management.

Passi

1. Per **Modalità di accesso**, seleziona una delle seguenti opzioni:
 - **Lettura-scrittura** (predefinito): gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.

- **Sola lettura:** gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Tenant Manager o Tenant Management API. Gli utenti locali con privilegi di sola lettura possono modificare le proprie password.



Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su Sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Seleziona una o più autorizzazioni per questo gruppo.

Vedere "[Autorizzazioni di gestione degli inquilini](#)".

3. Selezionare **Continua**.

Imposta i criteri di gruppo S3

I criteri di gruppo determinano quali autorizzazioni di accesso S3 avranno gli utenti.

Passi

1. Seleziona il criterio che vuoi utilizzare per questo gruppo.

Criteri di gruppo	Descrizione
Nessun accesso S3	Predefinito. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non venga concesso tramite un criterio bucket. Se si seleziona questa opzione, per impostazione predefinita solo l'utente root avrà accesso alle risorse S3.
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 oggetti e leggere dati, metadati e tag degli oggetti. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Non puoi 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 con accesso completo. Non puoi modificare questa stringa.
Mitigazione 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 definitivamente gli oggetti dai bucket in cui è abilitato il controllo delle versioni degli oggetti. Gli utenti Tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono ignorare questo criterio di gruppo. Limitare l'autorizzazione Gestisci tutti i bucket agli utenti attendibili e utilizzare l'autenticazione a più fattori (MFA) laddove disponibile.
Costume	Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

2. Se hai selezionato **Personalizzato**, inserisci i criteri di gruppo. Ogni criterio di gruppo ha un limite di dimensione di 5.120 byte. È necessario immettere una stringa valida in formato JSON.

Per informazioni dettagliate sui criteri di gruppo, inclusa la sintassi del linguaggio e gli esempi, vedere ["Criteri di gruppo di esempio"](#).

3. Se stai creando un gruppo locale, seleziona **Continua**. Se stai creando un gruppo federato, seleziona **Crea gruppo e Fine**.

Aggiungi utenti (solo gruppi locali)

È possibile salvare il gruppo senza aggiungere utenti oppure aggiungere facoltativamente eventuali utenti locali già esistenti.



Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, tutti gli utenti selezionati quando si crea un gruppo locale sulla griglia di origine non verranno inclusi quando il gruppo viene clonato sulla griglia di destinazione. Per questo motivo, non selezionare gli utenti quando crei il gruppo. In alternativa, seleziona il gruppo quando crei gli utenti.

Passi

1. Facoltativamente, seleziona uno o più utenti locali per questo gruppo.
2. Seleziona **Crea gruppo e Fine**.

Il gruppo che hai creato appare nell'elenco dei gruppi.

Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ti trovi sulla griglia di origine del tenant, il nuovo gruppo viene clonato nella griglia di destinazione del tenant.

Successo appare come **Stato di clonazione** nella sezione Panoramica 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 di amministratore Swift, necessaria per gestire i contenitori e gli oggetti per un account tenant Swift.



Il supporto per le applicazioni client Swift è stato deprecato e verrà rimosso in una versione futura.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#).
- Se si prevede di importare un gruppo federato, è necessario ["federazione di identità configurata"](#) e il gruppo federato esiste già nell'origine identità configurata.

Accedi alla procedura guidata Crea gruppo

Passi

Come primo passo, accedi alla procedura guidata Crea gruppo.

1. Selezionare **GESTIONE ACCESSI > Gruppi**.
2. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federato.

Passi

1. Selezionare la scheda **Gruppo locale** per creare un gruppo locale oppure selezionare la scheda **Gruppo federato** per importare un gruppo dall'origine identità configurata in precedenza.

Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), gli utenti appartenenti a gruppi locali non potranno accedere a Tenant Manager, sebbene possano utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni del gruppo.

2. Inserisci il nome del gruppo.
 - **Gruppo locale:** immettere sia un nome visualizzato che un nome univoco. Potrai modificare il nome visualizzato in un secondo momento.
 - **Gruppo federato:** 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**.

Gestisci i permessi del gruppo

Le autorizzazioni di gruppo controllano quali attività gli utenti possono eseguire in Tenant Manager e nell'API Tenant Management.

Passi

1. Per **Modalità di accesso**, seleziona una delle seguenti opzioni:
 - **Lettura-scrittura** (predefinito): gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
 - **Sola lettura:** gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Tenant Manager o Tenant Management API. Gli utenti locali con privilegi di sola lettura possono modificare le proprie password.



Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su Sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Selezionare la casella di controllo **Accesso root** se gli utenti del gruppo devono accedere a Tenant Manager o all'API Tenant Management.
3. Selezionare **Continua**.

Imposta i criteri di gruppo Swift

Gli utenti Swift necessitano dell'autorizzazione di amministratore per autenticarsi nella Swift REST API per creare contenitori e acquisire oggetti.

1. Selezionare la casella di controllo **Amministratore Swift** se gli utenti del gruppo devono utilizzare l'API REST Swift per gestire contenitori e oggetti.

2. Se stai creando un gruppo locale, seleziona **Continua**. Se stai creando un gruppo federato, seleziona **Crea gruppo e Fine**.

Aggiungi utenti (solo gruppi locali)

È possibile salvare il gruppo senza aggiungere utenti oppure aggiungere facoltativamente eventuali utenti locali già esistenti.

Passi

1. Facoltativamente, seleziona uno o più utenti locali per questo gruppo.

Se non hai ancora creato utenti locali, puoi aggiungere questo gruppo all'utente nella pagina Utenti. Vedere "[Gestisci gli utenti locali](#)".

2. Seleziona **Crea gruppo e Fine**.

Il gruppo che hai creato appare nell'elenco dei gruppi.

Autorizzazioni di gestione degli inquilini

Prima di creare un gruppo di tenant, valuta quali autorizzazioni vuoi assegnare a quel gruppo. Le autorizzazioni di gestione degli inquilini determinano quali attività gli utenti possono eseguire utilizzando Tenant Manager o Tenant Management API. 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 Tenant Management, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono effettuare l'accesso possono eseguire le seguenti attività:

- Visualizza la dashboard
- Cambiare la propria password (per gli utenti locali)

Per tutte le autorizzazioni, l'impostazione Modalità di accesso del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni oppure se possono solo visualizzare le impostazioni e le funzionalità correlate.



Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su Sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

È possibile assegnare le seguenti autorizzazioni a un gruppo. Si noti che i tenant S3 e i tenant Swift hanno autorizzazioni di gruppo diverse.

Permesso	Descrizione	Dettagli
Accesso root	Fornisce accesso completo al Tenant Manager e all'API Tenant Management.	Gli utenti Swift devono disporre dell'autorizzazione di accesso Root per accedere all'account tenant.

Permesso	Descrizione	Dettagli
Amministratore	Solo per inquilini Swift. Fornisce l'accesso completo ai contenitori e agli oggetti Swift per questo account tenant	Gli utenti Swift devono disporre dell'autorizzazione di amministratore Swift per eseguire qualsiasi operazione con la Swift REST API.
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 ARCHIVIAZIONE (S3) > Le mie chiavi di accesso S3 .
Visualizza tutti i bucket	Tenant S3: consente agli utenti di visualizzare tutti i bucket e le relative configurazioni. Tenant Swift: consente agli utenti Swift di visualizzare tutti i container e le configurazioni dei 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 è sostituita dall'autorizzazione Gestisci tutti i bucket. Non influisce sui criteri di gruppo o sui bucket S3 utilizzati dai client S3 o dalla console S3. È possibile assegnare questa autorizzazione solo ai gruppi Swift dall'API di gestione tenant. Non è possibile assegnare questa autorizzazione ai gruppi Swift tramite Tenant Manager.
Gestisci tutti i bucket	Tenant S3: consente agli utenti di utilizzare Tenant Manager e l'API Tenant Management per creare ed eliminare bucket S3 e gestire le impostazioni per tutti i bucket S3 nell'account tenant, indipendentemente dal bucket S3 o dai criteri di gruppo. Tenant Swift: consente agli utenti Swift di controllare la coerenza dei contenitori 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 sui bucket S3 utilizzati dai client S3 o dalla console S3. È possibile assegnare questa autorizzazione solo ai gruppi Swift dall'API di gestione tenant. Non è possibile assegnare questa autorizzazione ai gruppi Swift tramite Tenant Manager.
Gestisci gli endpoint	Consente agli utenti di utilizzare Tenant Manager o l'API Tenant Management per creare o modificare gli endpoint dei servizi della piattaforma, utilizzati come destinazione per i servizi della piattaforma StorageGRID .	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu Endpoint dei servizi della piattaforma .

Permesso	Descrizione	Dettagli
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.	

Gestisci gruppi

Gestisci i tuoi gruppi di tenant in base alle tue esigenze per visualizzare, modificare o duplicare un gruppo e altro ancora.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#) .

Visualizza o modifica il gruppo

È possibile visualizzare e modificare le informazioni di base e i dettagli per ciascun gruppo.

Passi

1. Selezionare **GESTIONE ACCESSI > Gruppi**.
2. Esaminare 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 sulla griglia di origine del tenant:

- Un messaggio banner indica che se modifichi o rimuovi un gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
- Se necessario, un messaggio banner indica se i gruppi non sono stati clonati nel tenant sulla griglia di destinazione. Puoi [riprovare un clone di gruppo](#) che ha fallito.

3. Se vuoi cambiare il nome del gruppo:
 - a. Selezionare la casella di controllo per il gruppo.
 - b. Seleziona **Azioni > Modifica nome gruppo**.
 - c. Inserisci il nuovo nome.
 - d. Seleziona **Salva modifiche**.
4. Se desideri visualizzare maggiori dettagli o apportare modifiche aggiuntive, procedi in uno dei seguenti modi:
 - Selezionare il nome del gruppo.
 - Seleziona la casella di controllo per il gruppo e seleziona **Azioni > Visualizza dettagli gruppo**.
5. Esaminare la sezione Panoramica, che mostra le seguenti informazioni per ciascun gruppo:
 - Nome da visualizzare
 - Nome univoco
 - Tipo

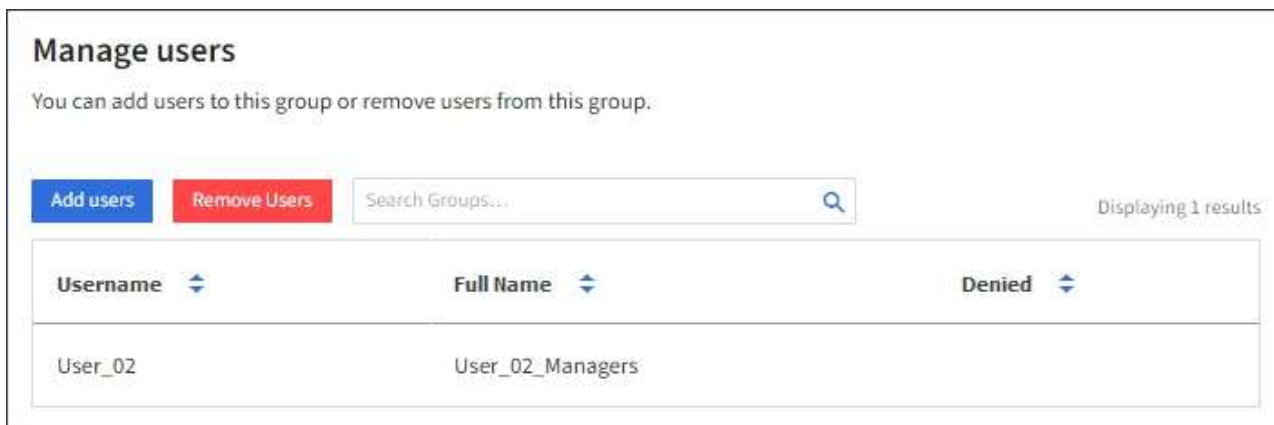
- Modalità di accesso
- Permessi
- Politica S3
- Numero di utenti in questo gruppo
- Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando il gruppo sulla griglia di origine del tenant:
 - Stato della clonazione, **Riuscito** o **Fallito**
 - Un banner blu che indica che se modifichi o elimini questo gruppo, le tue modifiche non verranno sincronizzate con l'altra griglia.

6. Modificare le impostazioni del gruppo secondo necessità. Vedere "[Creare gruppi per un tenant S3](#)" E "[Creare gruppi per un tenant Swift](#)" per i dettagli su cosa inserire.

- Nella sezione Panoramica, modifica il nome visualizzato selezionando il nome o l'icona di modifica .
- Nella scheda **Autorizzazioni gruppo**, aggiorna le autorizzazioni e seleziona **Salva modifiche**.
- Nella scheda **Criteri di gruppo**, apportare le modifiche desiderate e selezionare **Salva modifiche**.
 - Se si sta modificando un gruppo S3, è possibile selezionare facoltativamente un criterio di gruppo S3 diverso oppure immettere la stringa JSON per un criterio personalizzato, a seconda delle necessità.
 - Se stai modificando un gruppo Swift, seleziona o deseleziona facoltativamente la casella di controllo **Amministratore Swift**.

7. Per aggiungere uno o più utenti locali esistenti al gruppo:

- Selezionare la scheda Utenti.



Manage users

You can add users to this group or remove users from this group.

Displaying 1 results

Username	Full Name	Denied
User_02	User_02_Managers	

- Seleziona **Aggiungi utenti**.
- Seleziona gli utenti esistenti che desideri aggiungere e seleziona **Aggiungi utenti**.

In alto a destra appare un messaggio di conferma.

8. Per rimuovere gli utenti locali dal gruppo:

- Selezionare la scheda Utenti.
- Seleziona **Rimuovi utenti**.
- Seleziona gli utenti che vuoi rimuovere e seleziona **Rimuovi utenti**.

In alto a destra appare un messaggio di conferma.

9. Conferma di aver selezionato **Salva modifiche** per ogni sezione modificata.

Gruppo duplicato

È possibile duplicare un gruppo esistente per creare nuovi gruppi più rapidamente.



Se l'account del 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.

Passi

1. Selezionare **GESTIONE ACCESSI > Gruppi**.
2. Seleziona la casella di controllo relativa al gruppo che desideri duplicare.
3. Selezionare **Azioni > Duplica gruppo**.
4. Vedere ["Creare gruppi per un tenant S3"](#) O ["Creare gruppi per un tenant Swift"](#) per i dettagli su cosa inserire.
5. Seleziona **Crea gruppo**.

Riprova a clonare il gruppo

Per riprovare una clonazione non riuscita:

1. Selezionare ciascun gruppo che indica (*Clonazione non riuscita*) sotto il nome del gruppo.
2. Selezionare **Azioni > Clona gruppi**.
3. Visualizza lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun gruppo che stai clonando.

Per ulteriori informazioni, vedere ["Clona gruppi tenant e utenti"](#).

Elimina uno o più gruppi

È possibile eliminare uno o più gruppi. Gli utenti che appartengono solo a un gruppo eliminato non potranno più accedere a 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 sincronizzate queste informazioni, è necessario eliminare lo stesso gruppo da entrambe le griglie.

Passi

1. Selezionare **GESTIONE ACCESSI > Gruppi**.
2. Seleziona la casella di controllo per ogni gruppo che desideri eliminare.
3. Selezionare **Azioni > Elimina gruppo** o **Azioni > Elimina gruppi**.

Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Elimina gruppo** o **Elimina gruppi**.

Gestisci gli utenti locali

È possibile creare utenti locali e assegnarli a gruppi locali per determinare a quali funzionalità possono accedere. Il 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 per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), gli utenti locali non potranno accedere a Tenant Manager o all'API Tenant Management, sebbene possano 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 tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#).
- Se il tuo account tenant ha l'autorizzazione **Usa connessione federazione griglia**, hai esaminato il flusso di lavoro e le considerazioni per ["clonazione di gruppi di tenant e utenti"](#) 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 ad alcun gruppo non hanno autorizzazioni di gestione né criteri di gruppo S3 applicati. A questi utenti potrebbe essere concesso l'accesso al bucket S3 tramite un criterio bucket.

Gli utenti Swift che non appartengono ad alcun gruppo non hanno autorizzazioni di gestione né accesso al contenitore Swift.

Accedi alla procedura guidata Crea utente

Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.

Se l'account del tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, un banner blu indica che questa è la griglia di origine del tenant. Tutti gli utenti locali creati su questa griglia verranno clonati nell'altra griglia nella connessione.

Users

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

1 user

Create user

Actions ▾

i This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New local tenant users will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.

2. Seleziona **Crea utente**.

Inserisci le credenziali

Passi

1. Per il passaggio **Inserisci credenziali utente**, compila i seguenti campi.

Campo	Descrizione
Nome e cognome	Il nome completo di questo utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
Nome utente	Il nome che questo 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 sulla griglia di destinazione.
Password e Conferma password	La password che l'utente utilizzerà inizialmente per effettuare l'accesso.
Nega 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, seleziona Sì per sospendere temporaneamente la possibilità di un utente di accedere.

2. Selezionare **Continua**.

Assegna ai gruppi

Passi

1. Assegnare l'utente a uno o più gruppi locali per determinare quali attività può 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 ad alcun gruppo non avranno autorizzazioni di gestione. I permessi sono cumulativi. Gli utenti avranno tutte le autorizzazioni per tutti i gruppi a cui appartengono. Vedere ["Autorizzazioni di gestione degli inquilini"](#) .

2. Seleziona **Crea utente**.

Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ti trovi sulla griglia di origine del tenant, il nuovo utente locale viene clonato nella griglia di destinazione del tenant. **Successo** appare come **Stato di clonazione** nella sezione Panoramica della pagina dei dettagli dell'utente.

3. Selezionare **Fine** per tornare alla pagina Utenti.

Visualizza o modifica l'utente locale

Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Esaminare 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 visualizza l'utente sulla griglia di origine del tenant:

- Un messaggio banner indica che se modifichi o rimuovi un utente, le modifiche non verranno sincronizzate con l'altra griglia.
- Se necessario, un messaggio banner indica se gli utenti non sono stati clonati nel tenant sulla griglia di destinazione. È possibile [riprova un clone utente che non è riuscito](#) Potrebbe

3. Se vuoi cambiare il nome completo dell'utente:
 - a. Selezionare la casella di controllo per l'utente.
 - b. Seleziona **Azioni > Modifica nome completo**.
 - c. Inserisci il nuovo nome.
 - d. Seleziona **Salva modifiche**.
4. Se desideri visualizzare maggiori dettagli o apportare modifiche aggiuntive, procedi in uno dei seguenti modi:
 - Seleziona il nome utente.
 - Selezionare la casella di controllo per l'utente e selezionare **Azioni > Visualizza dettagli utente**.
5. Esaminare la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:
 - Nome e cognome
 - 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 si visualizza l'utente sulla griglia di origine del tenant:

- Stato della clonazione, **Riuscito** o **Fallito**
- Un banner blu che indica che se modifichi questo utente, le tue modifiche non verranno sincronizzate con l'altra griglia.

6. Modificare le impostazioni utente secondo necessità. Vedere [Crea utente locale](#) per i dettagli su cosa inserire.

a. Nella sezione **Panoramica**, modifica il nome completo selezionando il nome o l'icona di modifica  .

Non è possibile modificare il nome utente.

b. Nella scheda **Password**, modifica la password dell'utente e seleziona **Salva modifiche**.

c. Nella scheda **Accesso**, seleziona **No** per consentire all'utente di accedere oppure seleziona **Sì** per impedirgli di accedere. Quindi, seleziona **Salva modifiche**.

d. Nella scheda **Chiavi di accesso**, seleziona **Crea chiave** e segui le istruzioni per "[creazione delle chiavi di accesso S3 di un altro utente](#)".

e. Nella scheda **Gruppi**, seleziona **Modifica gruppi** per aggiungere l'utente ai gruppi o rimuoverlo dai gruppi. Quindi, seleziona **Salva modifiche**.

7. Conferma di aver selezionato **Salva modifiche** per ogni sezione modificata.

Utente locale duplicato

È possibile duplicare un utente locale per creare più rapidamente un nuovo utente.



Se l'account del 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.

Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Seleziona la casella di controllo relativa all'utente che desideri duplicare.
3. Selezionare **Azioni > Duplica utente**.
4. Vedere [Crea utente locale](#) per i dettagli su cosa inserire.
5. Seleziona **Crea utente**.

Riprova la clonazione dell'utente

Per riprovare una clonazione non riuscita:

1. Selezionare ciascun utente che indica (*Clonazione non riuscita*) sotto il nome utente.
2. Seleziona **Azioni > Clona utenti**.
3. Visualizza lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun utente che stai clonando.

Per ulteriori informazioni, vedere "[Clona gruppi tenant e utenti](#)".

Elimina uno o più utenti locali

È possibile eliminare definitivamente 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 sincronizzate queste informazioni, è necessario eliminare lo stesso utente da entrambe le griglie.



Per eliminare gli utenti federati è necessario utilizzare l'origine dell'identità federata.

Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Seleziona la casella di controllo per ogni utente che desideri eliminare.
3. Selezionare **Azioni > Elimina utente** oppure **Azioni > Elimina utenti**.

Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Elimina utente** o **Elimina utenti**.

Gestisci le chiavi di accesso S3

Gestisci le chiavi di accesso S3

Ogni utente di un account tenant S3 deve disporre di una chiave di accesso per archiviare e recuperare oggetti nel sistema StorageGRID . Una chiave di accesso è composta da un ID 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 **Accesso root** possono gestire le chiavi di accesso per l'account root S3 e per tutti gli altri utenti. Le chiavi di accesso root forniscono l'accesso completo a tutti i bucket e oggetti per il tenant, a meno che non siano disabilitate esplicitamente da un criterio di bucket.

StorageGRID supporta l'autenticazione Signature Version 2 e Signature Version 4. L'accesso tra account non è consentito, a meno che non sia esplicitamente abilitato da un criterio bucket.

Crea le tue chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile creare le proprie chiavi di accesso S3. Per accedere ai tuoi bucket e oggetti devi disporre di una chiave di accesso.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti che ha il ["Gestisci le tue credenziali S3 o l'autorizzazione di accesso Root"](#) .

Informazioni su questo compito

Puoi creare una o più chiavi di accesso S3 che ti consentono di creare e gestire i bucket per il tuo account tenant. Dopo aver creato una nuova chiave di accesso, aggiorna l'applicazione con il tuo nuovo ID chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi del necessario ed elimina quelle che non utilizzi. Se hai una sola chiave e questa sta per scadere, creane una nuova prima che scada quella vecchia, quindi eliminala.

Ogni chiave può avere una scadenza specifica o nessuna scadenza. Per quanto riguarda la scadenza, seguire queste linee guida:

- Imposta una scadenza per le tue chiavi per limitare l'accesso a un determinato periodo di tempo. Impostare un tempo di scadenza breve può aiutare a ridurre il rischio nel caso in cui l'ID della chiave di accesso e la chiave di accesso segreta vengano accidentalmente esposti. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio per la sicurezza nel tuo ambiente è basso e non hai bisogno di creare periodicamente nuove chiavi, non devi impostare una data di scadenza per le tue chiavi. Se in seguito decidi di creare nuove chiavi, elimina manualmente quelle vecchie.



È possibile accedere ai bucket e agli oggetti S3 appartenenti al tuo account utilizzando l'ID chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovi dal tuo account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Le mie chiavi di accesso**.

Viene visualizzata la pagina Le mie chiavi di accesso, in cui sono elencate tutte le chiavi di accesso esistenti.

2. Seleziona **Crea chiave**.

3. Eseguire una delle seguenti operazioni:

- Seleziona **Non impostare una data di scadenza** per creare una chiave che non scadrà. (Predefinito)
- Seleziona **Imposta una data di scadenza** e imposta la data e l'ora di scadenza.



La data di scadenza può essere al massimo di cinque anni dalla data corrente. L'orario di scadenza può essere di almeno un minuto rispetto all'orario corrente.

4. Seleziona **Crea chiave di accesso**.

Viene visualizzata la finestra di dialogo 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 un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.



Non chiudere questa finestra di dialogo finché non hai copiato o scaricato queste informazioni. Non è possibile copiare o scaricare le chiavi dopo aver chiuso la finestra di dialogo.

6. Selezionare **Fine**.

La nuova chiave è elencata nella pagina Le mie chiavi di accesso.

7. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, puoi facoltativamente 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. Vedere "[Clona le chiavi di accesso S3 utilizzando l'API](#)".

Visualizza le tue chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone di "[autorizzazione appropriata](#)", puoi visualizzare un elenco delle tue chiavi di accesso S3. È possibile ordinare l'elenco in base alla data di scadenza, in modo da poter determinare quali chiavi scadranno presto. Se necessario, puoi "[creare nuove chiavi](#)" O "[cancellare i tasti](#)" che non utilizzi più.



È possibile accedere ai bucket e agli oggetti S3 appartenenti al tuo account utilizzando l'ID chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovi dal tuo account quelle non utilizzate e non condividerle mai con altri utenti.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)".
- Appartieni a un gruppo di utenti che ha la possibilità di gestire le proprie credenziali S3 "[permesso](#)".

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Le mie chiavi di accesso**.
2. Dalla pagina Le mie chiavi di accesso, ordina tutte le chiavi di accesso esistenti in base a **Ora di scadenza** o **ID chiave di accesso**.
3. Se necessario, crea nuove chiavi o elimina quelle che non utilizzi più.

Se crei nuove chiavi prima che quelle esistenti scadano, puoi iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti nell'account.

Le chiavi scadute vengono rimosse automaticamente.

Elimina le tue 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. Dopo aver eliminato una chiave di accesso, non sarà più possibile utilizzarla per accedere agli oggetti e ai bucket nell'account tenant.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)".
- Tu hai il "[Gestisci le tue autorizzazioni per le credenziali S3](#)".



È possibile accedere ai bucket e agli oggetti S3 appartenenti al tuo account utilizzando l'ID chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovi dal tuo account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Le mie chiavi di accesso**.
2. Nella pagina Le mie chiavi di accesso, seleziona la casella di controllo per ogni chiave di accesso che desideri rimuovere.
3. Selezionare **Elimina tasto**.
4. Nella finestra di dialogo di conferma, seleziona **Elimina chiave**.

Nell'angolo in alto a destra della pagina appare un messaggio di conferma.

Crea le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile creare chiavi di accesso S3 per altri utenti, ad esempio applicazioni che necessitano di accedere a bucket e oggetti.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#).

Informazioni su questo compito

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, aggiorna 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 necessarie all'utente ed elimina quelle che non vengono utilizzate. Se hai una sola chiave e questa sta per scadere, creane una nuova prima che scada quella vecchia, quindi eliminala.

Ogni chiave può avere una scadenza specifica o nessuna scadenza. Per quanto riguarda la scadenza, seguire queste linee guida:

- Imposta una scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. Impostare un tempo di scadenza breve può aiutare a ridurre il rischio nel caso in cui l'ID della chiave di accesso e la chiave di accesso segreta vengano accidentalmente esposti. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio per la sicurezza nel tuo ambiente è basso e non hai bisogno di creare periodicamente nuove chiavi, non devi impostare una data di scadenza per le chiavi. Se in seguito decidi di creare nuove chiavi, elimina manualmente quelle vecchie.



È possibile accedere ai bucket e agli oggetti S3 appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per quell'utente in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovere dall'account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.

2. Seleziona l'utente di cui desideri gestire le chiavi di accesso S3.

Viene visualizzata la pagina dei dettagli dell'utente.

3. Selezionare **Chiavi di accesso**, quindi selezionare **Crea chiave**.

4. Eseguire una delle seguenti operazioni:

- Seleziona **Non impostare una data di scadenza** per creare una chiave che non scade. (Predefinito)
- Seleziona **Imposta una data di scadenza** e imposta la data e l'ora di scadenza.



La data di scadenza può essere al massimo di cinque anni dalla data corrente. L'orario di scadenza può essere di almeno un minuto rispetto all'orario corrente.

5. Seleziona **Crea chiave di accesso**.

Viene visualizzata la finestra di dialogo Scarica chiave di accesso, in cui sono elencati 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 un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.



Non chiudere questa finestra di dialogo finché non hai copiato o scaricato queste informazioni. Non è possibile copiare o scaricare le chiavi dopo aver chiuso la finestra di dialogo.

7. Selezionare **Fine**.

La nuova chiave è elencata nella scheda Chiavi di accesso della pagina dei dettagli dell'utente.

8. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, puoi facoltativamente 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. Vedere ["Clona le chiavi di accesso S3 utilizzando l'API"](#).

Visualizza 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 alla data di scadenza, in modo da poter determinare quali chiavi scadranno presto. Se necessario, è possibile creare nuove chiavi ed eliminare quelle che non sono più in uso.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).



È possibile accedere ai bucket e agli oggetti S3 appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per quell'utente in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruotare regolarmente le chiavi di accesso, rimuovere dall'account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Dalla pagina Utenti, seleziona l'utente di cui desideri visualizzare le chiavi di accesso S3.
3. Dalla pagina Dettagli utente, seleziona **Chiavi di accesso**.
4. Ordina le chiavi in base a **Data di scadenza** o **ID chiave di accesso**.
5. Se necessario, crea nuove chiavi ed elimina manualmente quelle che non sono più in uso.

Se si creano nuove chiavi prima che quelle esistenti scadano, l'utente può iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti nell'account.

Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

- ["Crea le chiavi di accesso S3 di un altro utente"](#)
- ["Elimina le chiavi di accesso S3 di un altro utente"](#)

Elimina 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. Dopo aver eliminato una chiave di accesso, non sarà più possibile utilizzarla per accedere agli oggetti e ai bucket nell'account tenant.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).



È possibile accedere ai bucket e agli oggetti S3 appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per quell'utente in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruotare regolarmente le chiavi di accesso, rimuovere dall'account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Dalla pagina Utenti, seleziona l'utente di cui desideri gestire le chiavi di accesso S3.
3. Dalla pagina Dettagli utente, seleziona **Chiavi di accesso**, quindi seleziona la casella di controllo per ogni chiave di accesso che desideri eliminare.
4. Selezionare **Azioni > Elimina chiave selezionata**.
5. Nella finestra di dialogo di conferma, seleziona **Elimina chiave**.

Nell'angolo in alto a destra della pagina appare un messaggio di conferma.

Gestisci i bucket S3

Crea un bucket S3

È possibile utilizzare Tenant Manager per creare bucket S3 per i dati degli oggetti.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha accesso Root o Gestisci tutti i bucket ["permesso"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.



Le autorizzazioni per impostare o modificare le proprietà di blocco degli oggetti S3 di bucket o oggetti possono essere concesse da ["criterio bucket o criterio di gruppo"](#).

- Se si prevede di abilitare S3 Object Lock per un bucket, un amministratore della griglia ha abilitato l'impostazione globale S3 Object Lock per il sistema StorageGRID e sono stati esaminati i requisiti per i bucket e gli oggetti S3 Object Lock.
- Se ogni tenant avrà 5.000 bucket, ogni nodo di archiviazione nella griglia avrà un minimo di 64 GB di RAM.



Ogni griglia può avere un massimo di 100.000 bucket.

Accedi alla procedura guidata

Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
2. Seleziona **Crea bucket**.

Inserisci i dettagli

Passi

1. Inserisci i dettagli per il bucket.

Campo	Descrizione
Nome del bucket	Un nome per il bucket che rispetti queste regole: • Deve essere univoco 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 contenere solo lettere minuscole, numeri e trattini. • Non devono contenere punti nelle richieste in stile ospitato virtuale. I punti causeranno problemi con la verifica dei certificati jolly del server. Per maggiori informazioni, vedere il "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione dei bucket". Nota: non è possibile modificare il nome del bucket dopo averlo creato.
Regione	La regione del bucket. L'amministratore StorageGRID gestisce le regioni disponibili. La regione di un bucket può influire sulla politica di protezione dei dati applicata agli oggetti. Per impostazione predefinita, tutti i bucket vengono creati in <code>us-east-1</code> regione. Nota: non è possibile modificare la regione dopo aver creato il bucket.

2. Selezionare **Continua**.

Gestisci le impostazioni

Passi

1. Facoltativamente, abilitare il controllo delle versioni degli oggetti per il bucket.

Abilita il controllo delle versioni degli oggetti se vuoi archiviare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto, se necessario. È necessario abilitare il controllo delle versioni degli oggetti se il bucket verrà utilizzato per la replica tra griglie.

2. Se l'impostazione globale S3 Object Lock è abilitata, abilitare facoltativamente S3 Object Lock per il bucket per archiviare gli oggetti utilizzando un modello write-once-read-many (WORM).

Abilitare S3 Object Lock per un bucket solo se è necessario conservare 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 impedire che gli oggetti vengano eliminati o sovrascritti per un periodo di tempo fisso o indefinitamente.



Dopo aver abilitato l'impostazione Blocco oggetto S3 per un bucket, non è più possibile disattivarla. Chiunque disponga delle autorizzazioni corrette può aggiungere a questo bucket oggetti che non possono essere modificati. Potresti non essere in grado di eliminare questi oggetti o il bucket stesso.

Se si abilita S3 Object Lock per un bucket, il controllo delle versioni del bucket viene abilitato

automaticamente.

3. Se hai selezionato **Abilita blocco oggetto S3**, abilita facoltativamente **Conservazione predefinita** per questo bucket.



L'amministratore della rete deve darti l'autorizzazione a "[utilizzare le funzionalità specifiche di S3 Object Lock](#)".

Quando è abilitata la **Conservazione predefinita**, i nuovi oggetti aggiunti al bucket saranno automaticamente protetti dall'eliminazione o dalla sovrascrittura. L'impostazione **Conservazione predefinita** non si applica agli oggetti che hanno un proprio periodo di conservazione.

- a. Se è abilitata la **Conservazione predefinita**, specificare una **Modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Governance	• Utenti con il <code>s3:BypassGovernanceRetention</code> il permesso può utilizzare il <code>x-amz-bypass-governance-retention: true</code> intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.
Conformità	• L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione. • La data di conservazione dell'oggetto può essere aumentata, ma non diminuita. • La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data. Nota: l'amministratore della rete deve consentirti di utilizzare la modalità di conformità.

- b. Se è abilitata l'opzione **Conservazione predefinita**, specificare il **Periodo di conservazione predefinito** per il bucket.

Il **Periodo di conservazione predefinito** 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 inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della griglia.

Un periodo di conservazione *massimo*, che può essere un valore compreso tra 1 giorno e 100 anni, viene impostato quando l'amministratore della griglia crea il tenant. Quando si imposta un periodo di conservazione *predefinito*, questo non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedi all'amministratore della rete di aumentare o diminuire il periodo massimo di conservazione.

4. Facoltativamente, seleziona **Abilita limite di capacità**.

Il limite di capacità è la capacità massima disponibile per gli oggetti di questo bucket. Questo valore rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione su disco).

Se non viene impostato alcun limite, la capacità di questo bucket è illimitata. Fare riferimento a ["Utilizzo del limite di capacità"](#) per maggiori informazioni.

5. Seleziona **Crea bucket**.

Il bucket viene creato e aggiunto alla tabella nella pagina Bucket.

6. Facoltativamente, seleziona **Vai alla pagina dei dettagli del bucket** per ["visualizza i dettagli del bucket"](#) ed eseguire configurazioni aggiuntive.

Visualizza i dettagli del bucket

Puoi visualizzare i bucket nel tuo account tenant.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Accesso root, autorizzazione Gestisci tutti i bucket o Visualizza tutti i bucket"](#). Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.

Viene visualizzata la pagina Bucket.

2. Esaminare la tabella riepilogativa per ogni bucket.

A seconda delle necessità, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco avanti e indietro.



I valori visualizzati per Conteggio oggetti, Spazio utilizzato e Utilizzo sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo. Se nel bucket è abilitato il controllo delle versioni, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

Nome

Nome univoco del bucket, che non può essere modificato.

Funzionalità abilitate

Elenco delle funzionalità abilitate per il bucket.

Blocco oggetto S3

Se il blocco oggetti S3 è abilitato per il bucket.

Questa colonna viene visualizzata solo se il blocco oggetti S3 è abilitato per la griglia. Questa colonna mostra anche informazioni per eventuali bucket Compliant legacy.

Regione

La regione del bucket, che non può essere modificata. Per impostazione predefinita, questa colonna è nascosta.

Conteggio degli oggetti

Il numero di oggetti in questo bucket. Se nel bucket è abilitato il controllo delle versioni, le versioni degli oggetti non correnti vengono incluse in questo valore.

Quando si aggiungono o si eliminano oggetti, questo valore potrebbe non aggiornarsi immediatamente.

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 per cancellazione o per i metadati degli oggetti.

L'aggiornamento di questo valore può richiedere fino a 10 minuti.

Utilizzo

Percentuale utilizzata del limite di capacità del bucket, se ne è stato impostato uno.

Il valore di utilizzo si basa su stime interne e in alcuni casi potrebbe essere superato. Ad esempio, StorageGRID verifica il limite di capacità (se impostato) quando un tenant inizia a caricare oggetti e rifiuta i nuovi ingest in questo bucket se il tenant ha superato il limite di capacità. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente quando determina se il limite di capacità è stato superato. Se gli oggetti vengono eliminati, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti in questo bucket finché non viene ricalcolato l'utilizzo del limite di capacità. I calcoli possono richiedere 10 minuti o più.

Questo valore indica la dimensione logica, non quella fisica, necessaria per memorizzare gli oggetti e i relativi metadati.

Capacità

Se impostato, il limite di capacità per il bucket.

Data di creazione

Data e ora di creazione del bucket. Per impostazione predefinita, questa colonna è nascosta.

3. Per visualizzare i dettagli di un bucket specifico, seleziona il nome del bucket dalla tabella.
 - a. Visualizza le informazioni riepilogative nella parte superiore della pagina Web per confermare i dettagli del bucket, ad esempio la regione e il numero di oggetti.
 - b. Visualizza la barra di utilizzo del limite di capacità. Se l'utilizzo è pari al 100% o vicino al 100%, valutare l'aumento del limite o l'eliminazione di alcuni oggetti.
 - c. Se necessario, seleziona **Elimina oggetti nel bucket** e **Elimina bucket**.



Prestare molta attenzione alle avvertenze che compaiono quando si seleziona ciascuna di queste opzioni. Per maggiori informazioni, fare riferimento a:

- ["Elimina tutti gli oggetti in un bucket"](#)
- ["Elimina un bucket"](#) (il secchio deve essere vuoto)

- d. Visualizza o modifica le impostazioni per il bucket in ciascuna scheda, secondo necessità.
 - **Console S3**: visualizza gli oggetti per il bucket. Per ulteriori informazioni, fare riferimento a

["Utilizzare la console S3"](#) .

- **Opzioni bucket:** visualizza o modifica le impostazioni delle opzioni. Alcune impostazioni, come S3 Object Lock, non possono essere modificate dopo la creazione del bucket.
 - ["Gestire la coerenza del bucket"](#)
 - ["Aggiornamenti dell'ultimo orario di accesso"](#)
 - ["Limite di capacità"](#)
 - ["Versionamento degli oggetti"](#)
 - ["Blocco oggetto S3"](#)
 - ["Conservazione predefinita del bucket"](#)
 - ["Gestire la replicazione tra griglie"](#)(se consentito all'inquilino)
- **Servizi di piattaforma:**["Gestire i servizi della piattaforma"](#) (se consentito all'inquilino)
- **Accesso bucket:** visualizza o modifica le impostazioni delle opzioni. È necessario disporre di autorizzazioni di accesso specifiche.
 - Configurare ["Condivisione delle risorse tra origini \(CORS\)"](#) in modo che il bucket e gli oggetti al suo interno siano accessibili alle applicazioni web in altri domini.
 - ["Controlla l'accesso degli utenti"](#) per un bucket S3 e gli oggetti in quel bucket.

Applicare un tag di policy ILM a un bucket

Scegli un tag di policy ILM da applicare a un bucket in base ai requisiti di archiviazione degli oggetti.

La policy ILM controlla dove vengono archiviati i dati dell'oggetto e se vengono eliminati dopo un determinato periodo di tempo. L'amministratore della griglia crea criteri ILM e li assegna ai tag dei criteri ILM quando si utilizzano più criteri attivi.



Evitare di riassegnare frequentemente il tag di policy di un bucket. In caso contrario, potrebbero verificarsi problemi di prestazioni.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti che ha il ["Accesso root, autorizzazione Gestisci tutti i bucket o Visualizza tutti i bucket"](#) . Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.

Viene visualizzata la pagina Bucket. A seconda delle necessità, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco avanti e indietro.

2. Selezionare il nome del bucket a cui si desidera assegnare un tag di policy ILM.

È anche possibile modificare l'assegnazione del tag della policy ILM per un bucket a cui è già assegnato un tag.



I valori visualizzati per il conteggio degli oggetti e lo spazio utilizzato sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo. Se nei bucket è abilitato il controllo delle versioni, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

3. Nella scheda Opzioni bucket, espandere l'accordione tag policy ILM. Questa fisarmonica viene visualizzata solo se l'amministratore della griglia ha abilitato l'uso di tag di policy personalizzati.
4. Leggere la descrizione di ciascun tag di policy per determinare quale tag applicare al bucket.



La modifica del tag della policy ILM per un bucket attiverà la rivalutazione ILM di tutti gli oggetti nel bucket. Se la nuova policy conserva gli oggetti per un periodo di tempo limitato, gli oggetti più vecchi verranno eliminati.

5. Selezionare il pulsante di opzione per il tag che si desidera assegnare al bucket.
6. Seleziona **Salva modifiche**. Un nuovo tag bucket S3 verrà impostato sul bucket con la chiave NTAP-SG-ILM-BUCKET-TAG e il valore del nome del tag della policy ILM.



Assicurati che le tue applicazioni S3 non sovrascrivano o eliminino accidentalmente il nuovo tag 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.



Imposta e modifica i tag dei criteri ILM utilizzando solo Tenant Manager o Tenant Manager API in cui viene convalidato il tag dei criteri ILM. Non modificare il NTAP-SG-ILM-BUCKET-TAG Tag di policy ILM tramite l'API S3 PutBucketTagging o l'API S3 DeleteBucketTagging.



La modifica del tag di policy assegnato a un bucket ha un impatto temporaneo sulle prestazioni mentre gli oggetti vengono rivalutati utilizzando la nuova policy ILM.

Gestisci i criteri del bucket

È possibile controllare l'accesso utente per un bucket S3 e per gli oggetti in quel bucket.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Permesso di accesso root"](#). Le autorizzazioni Visualizza tutti i bucket e Gestisci tutti i bucket consentono solo la visualizzazione.
- Hai verificato che sia disponibile il numero richiesto di nodi di archiviazione e siti. Se due o più nodi di archiviazione non sono disponibili in nessun sito, oppure se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

Passi

1. Seleziona **Bucket**, quindi seleziona il bucket che desideri gestire.
2. Nella pagina dei dettagli del bucket, seleziona **Accesso al bucket > Criterio bucket**.
3. Eseguire una delle seguenti operazioni:
 - Immettere un criterio di bucket selezionando la casella di controllo **Abilita criterio**. Quindi inserisci una stringa valida in formato JSON.

Ogni criterio di bucket ha un limite di dimensione di 20.480 byte.

- Modificare una policy esistente modificando la stringa.
- Disattivare un criterio deselectando **Abilita criterio**.

Per informazioni dettagliate sulle policy dei bucket, inclusa la sintassi del linguaggio e gli esempi, vedere ["Criteri di esempio per i bucket"](#).

Gestire la coerenza del bucket

I valori di coerenza possono essere utilizzati per specificare la disponibilità delle modifiche alle impostazioni del bucket, nonché per fornire un equilibrio tra la disponibilità degli oggetti all'interno di un bucket e la coerenza di tali oggetti tra diversi nodi di archiviazione e siti. 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 tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

Linee guida sulla coerenza del bucket

La coerenza del bucket viene utilizzata per determinare la coerenza delle applicazioni client che interessano gli oggetti all'interno di quel bucket S3. In generale, dovresti usare la coerenza **Lettura dopo nuova scrittura** per i tuoi bucket.

Modifica la coerenza del bucket

Se la coerenza **Read-after-new-write** non soddisfa i requisiti dell'applicazione client, è possibile modificarla impostando la coerenza del bucket o utilizzando Consistency-Control intestazione. IL Consistency-Control l'intestazione sovrascrive la coerenza del bucket.



Quando si modifica la consistenza di un bucket, solo gli oggetti acquisiti dopo la modifica sono garantiti per soddisfare l'impostazione rivista.

Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
2. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona la fisarmonica **.
4. Selezionare una coerenza per le operazioni eseguite sugli oggetti in questo bucket.
 - **Tutti**: fornisce il massimo livello di coerenza. Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
 - **Strong-global**: garantisce la coerenza di lettura e scrittura per tutte le richieste dei client su tutti i siti.
 - **Strong-site**: garantisce la coerenza di lettura e scrittura per tutte le richieste client all'interno di un sito.

- **Lettura dopo nuova scrittura** (predefinito): fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
- **Disponibile**: fornisce 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 letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool.

5. Seleziona **Salva modifiche**.

Cosa succede quando si modificano le impostazioni del bucket

I bucket hanno più impostazioni che influenzano il comportamento dei bucket stessi e degli oggetti al loro interno.

Le seguenti impostazioni del bucket utilizzano per impostazione predefinita la coerenza **forte**. Se due o più nodi di archiviazione non sono disponibili in nessun sito, oppure se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

- ["Eliminazione del bucket vuoto in background"](#)
- ["Ultimo orario di accesso"](#)
- ["Ciclo di vita del bucket"](#)
- ["Politica del bucket"](#)
- ["Etichettatura del secchio"](#)
- ["Versionamento del bucket"](#)
- ["Blocco oggetto S3"](#)
- ["Crittografia del bucket"](#)



Il valore di coerenza per il controllo delle versioni dei bucket, il blocco degli oggetti S3 e la crittografia dei bucket non può essere impostato su un valore che non sia fortemente coerente.

Le seguenti impostazioni del bucket non utilizzano una coerenza elevata 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"](#)
- [Modifica la coerenza del bucket](#)



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 il ["API REST S3"](#) oppure utilizzando il `reducedConsistency` O force opzioni nel ["API di gestione degli inquilini"](#).

Abilita o disabilita gli aggiornamenti dell'ultimo orario di accesso

Quando gli amministratori della griglia creano le regole di gestione del ciclo di vita delle informazioni (ILM) per un sistema StorageGRID, possono facoltativamente specificare che l'orario dell'ultimo accesso a un oggetto venga utilizzato per determinare se spostare

tale oggetto in una posizione di archiviazione diversa. Se si utilizza un tenant S3, è possibile sfruttare tali regole abilitando gli aggiornamenti dell'ora dell'ultimo 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 orario di accesso** come filtro avanzato o come orario di riferimento. Se il sistema StorageGRID non include tale regola, è possibile ignorare queste istruzioni. Vedere ["Utilizzare l'orario dell'ultimo accesso nelle regole ILM"](#) per i dettagli.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti che ha il ["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#) . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

Informazioni su questo compito

Ultimo orario di accesso è una delle opzioni disponibili per l'istruzione di posizionamento **Ora di riferimento** per una regola ILM. Impostando l'Ora di riferimento per una regola su Ora ultimo accesso, gli amministratori della griglia possono specificare che gli oggetti vengano posizionati in determinate posizioni di archiviazione in base all'ultima volta in cui tali oggetti sono stati recuperati (letti o visualizzati).

Ad esempio, per garantire che gli oggetti visualizzati di recente rimangano in un archivio più veloce, un amministratore di griglia può creare una regola ILM che specifichi quanto segue:

- Gli oggetti recuperati nel mese precedente devono rimanere sui nodi di archiviazione locali.
- Gli oggetti che non sono stati recuperati nel mese precedente devono essere spostati in un luogo esterno.

Per impostazione predefinita, gli aggiornamenti all'orario dell'ultimo accesso sono disabilitati. Se il sistema StorageGRID include una regola ILM che utilizza l'opzione **Ultimo orario di accesso** e si desidera che questa opzione venga applicata agli oggetti in questo bucket, è necessario abilitare gli aggiornamenti all'ultimo orario di accesso per i bucket S3 specificati in tale regola.



L'aggiornamento dell'orario dell'ultimo accesso quando un oggetto viene recuperato può ridurre le prestazioni StorageGRID , soprattutto per gli oggetti di piccole dimensioni.

Si verifica un impatto sulle prestazioni con gli ultimi aggiornamenti dell'ora di accesso perché StorageGRID deve eseguire questi passaggi aggiuntivi ogni volta che vengono recuperati oggetti:

- Aggiorna gli oggetti con nuovi timestamp
- Aggiungere gli oggetti alla coda ILM, in modo che possano essere rivalutati in base alle attuali regole e policy ILM

La tabella riepiloga il comportamento applicato a tutti gli oggetti nel bucket quando l'orario dell'ultimo accesso è disabilitato o abilitato.

Tipo di richiesta	Comportamento se l'ultimo orario di accesso è disabilitato (predefinito)		Comportamento se l'ultimo orario di accesso è abilitato	
	Ultimo orario di accesso aggiornato?	Oggetto aggiunto alla coda di valutazione ILM?	Ultimo orario di accesso aggiornato?	Oggetto aggiunto alla coda di valutazione ILM?

Richiesta di recupero di un oggetto, del suo elenco di controllo di accesso o dei suoi metadati	NO	NO	Sì	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì	Sì	Sì
Richiesta di elencare oggetti o versioni di oggetti	NO	NO	NO	NO
Richiesta di copiare un oggetto da un bucket all'altro	• No, per la copia sorgente • Sì, per la copia di destinazione	• No, per la copia sorgente • Sì, per la copia di destinazione	• Sì, per la copia sorgente • Sì, per la copia di destinazione	• Sì, per la copia sorgente • Sì, per la copia di destinazione
Richiesta di completamento di un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
2. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona la voce accordion **Aggiornamenti ora ultimo accesso**.
4. Abilita o disabilita gli aggiornamenti dell'orario dell'ultimo accesso.
5. Seleziona **Salva modifiche**.

Modificare il controllo delle versioni degli oggetti per un bucket

Se si utilizza un tenant S3, è possibile modificare lo stato di controllo delle versioni per i bucket S3.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- Hai verificato che sia disponibile il numero richiesto di nodi di archiviazione e siti. Se due o più nodi di archiviazione non sono disponibili in nessun sito, oppure se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

Informazioni su questo compito

È possibile abilitare o sospendere il controllo delle versioni degli oggetti per un bucket. Dopo aver abilitato il controllo delle versioni per un bucket, questo non può tornare a uno stato senza controllo delle versioni. Tuttavia, è possibile sospendere il controllo delle versioni per il bucket.

- Disabilitato: il controllo delle versioni non è mai stato abilitato
- Abilitato: il controllo delle versioni è abilitato
- Sospeso: il controllo delle versioni era precedentemente abilitato ed è sospeso

Per ulteriori informazioni, vedere quanto segue:

- ["Versionamento degli oggetti"](#)
- ["Regole e policy ILM per oggetti con versione S3 \(esempio 4\)"](#)
- ["Come vengono eliminati gli oggetti"](#)

Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
2. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona la voce accordion **Versionamento oggetto**.
4. Seleziona uno stato di controllo delle versioni per gli oggetti in questo bucket.

Il controllo delle versioni degli oggetti deve rimanere abilitato per un bucket utilizzato per la replica tra griglie. Se è abilitato il blocco degli oggetti S3 o la conformità legacy, le opzioni di **Versioning degli oggetti** sono disabilite.

Opzione	Descrizione
Abilita il controllo delle versioni	Abilita il controllo delle versioni degli oggetti se vuoi archiviare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto, se necessario. Gli oggetti già presenti nel bucket verranno sottoposti a versioning quando vengono modificati da un utente.
Sospendi il controllo delle versioni	Sospendi il controllo delle versioni degli oggetti se non desideri più che vengano create nuove versioni degli oggetti. È ancora possibile recuperare tutte le versioni esistenti dell'oggetto.

5. Seleziona **Salva modifiche**.

Utilizzare S3 Object Lock per conservare gli oggetti

È possibile utilizzare S3 Object Lock se i bucket e gli oggetti devono essere conformi ai requisiti normativi per la conservazione.



L'amministratore della griglia deve concederti l'autorizzazione per utilizzare funzionalità specifiche di S3 Object Lock.

Che cos'è S3 Object Lock?

La funzionalità StorageGRID S3 Object Lock è una soluzione di protezione degli oggetti equivalente a S3 Object Lock in Amazon Simple Storage Service (Amazon S3).

Quando l'impostazione globale S3 Object Lock è abilitata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se in un bucket è abilitato S3 Object Lock, è necessario il controllo delle versioni del bucket, che viene abilitato automaticamente.

Un bucket senza S3 Object Lock può contenere solo oggetti per i quali non sono specificate impostazioni di conservazione. Nessun oggetto ingerito avrà impostazioni di conservazione.

Un bucket con S3 Object Lock può contenere oggetti con e senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con S3 Object Lock e conservazione predefinita configurata può contenere oggetti caricati con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, perché l'impostazione di conservazione non è stata configurata a livello di oggetto.

Di fatto, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurata la conservazione predefinita. Gli oggetti esistenti senza impostazioni di conservazione degli oggetti rimangono inalterati.

Modalità di conservazione

La funzionalità StorageGRID S3 Object Lock supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità sono equivalenti alle modalità di conservazione di Amazon S3.

- In modalità conformità:
 - L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione.
 - La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.
 - La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.
- In modalità di governance:
 - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare determinate impostazioni di conservazione.
 - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione.
 - Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.

Impostazioni di conservazione per le versioni degli oggetti

Se viene creato un bucket con S3 Object Lock abilitato, gli utenti possono utilizzare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ciascun oggetto aggiunto al bucket:

- **Modalità di conservazione:** conformità o governance.
- **Retain-until-date:** se la retain-until-date di una versione di un oggetto è futura, l'oggetto può essere recuperato, ma non eliminato.

- **Sospensione legale:** l'applicazione di una sospensione legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potrebbe essere necessario applicare un blocco legale a un oggetto correlato a un'indagine o a una controversia legale. Una sospensione legale non ha una data di scadenza, ma rimane in vigore finché non viene rimossa esplicitamente. Le sospensioni legali sono indipendenti dalla data di conservazione fino alla data di scadenza.



Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

Per i dettagli sulle impostazioni dell'oggetto, vedere ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#).

Impostazione di conservazione predefinita per i bucket

Se viene creato un bucket con S3 Object Lock abilitato, gli utenti possono facoltativamente specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita:** conformità o governance.
- **Periodo di conservazione predefinito:** per quanto tempo devono essere conservate le nuove versioni degli oggetti aggiunte a questo bucket, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non dispongono di impostazioni di conservazione proprie. Gli oggetti bucket esistenti non vengono modificati quando si aggiungono o si modificano queste impostazioni predefinite.

Vedere ["Crea un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco degli oggetti S3"](#).

Attività di blocco degli oggetti S3

Gli elenchi seguenti per gli amministratori della griglia e gli utenti tenant contengono le attività di alto livello per l'utilizzo della funzionalità S3 Object Lock.

Amministratore di rete

- Abilita l'impostazione globale di blocco degli oggetti S3 per l'intero sistema StorageGRID.
- Garantire che le politiche di gestione del ciclo di vita delle informazioni (ILM) siano *conformi*; ovvero, che soddisfino i ["requisiti dei bucket con S3 Object Lock abilitato"](#).
- Se necessario, consentire a un tenant di utilizzare Conformità come modalità di conservazione. In caso contrario, è consentita solo la modalità Governance.
- Se necessario, impostare un periodo massimo di conservazione per un tenant.

Utente inquilino

- Esaminare le considerazioni relative a bucket e oggetti con S3 Object Lock.
- Se necessario, contattare l'amministratore della griglia per abilitare l'impostazione globale di blocco degli oggetti S3 e impostare le autorizzazioni.
- Crea bucket con S3 Object Lock abilitato.
- Facoltativamente, configura le impostazioni di conservazione predefinite per un bucket:
 - Modalità di conservazione predefinita: Governance o Conformità, se consentita dall'amministratore della rete.
 - Periodo di conservazione predefinito: deve essere inferiore o uguale al periodo di conservazione

massimo impostato dall'amministratore della griglia.

- Utilizzare l'applicazione client S3 per aggiungere oggetti e, facoltativamente, impostare la conservazione specifica dell'oggetto:
 - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore della rete.
 - Conserva fino alla data: deve essere inferiore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.

Requisiti per i bucket con S3 Object Lock abilitato

- Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID, è possibile utilizzare Tenant Manager, Tenant Management API o S3 REST API per creare bucket con S3 Object Lock abilitato.
- Se si prevede di utilizzare S3 Object Lock, è necessario abilitarlo quando si crea il bucket. Non è possibile abilitare S3 Object Lock per un bucket esistente.
- Quando S3 Object Lock è abilitato per un bucket, StorageGRID abilita automaticamente il controllo delle versioni per quel bucket. Non è possibile disattivare S3 Object Lock o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione predefinita e un periodo di conservazione per ciascun bucket utilizzando Tenant Manager, Tenant Management API o S3 REST API. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di impostazioni di conservazione proprie. È possibile ignorare queste impostazioni predefinite specificando una modalità di conservazione e una data di conservazione per ogni versione dell'oggetto quando viene caricata.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con S3 Object Lock abilitato.
- La replica CloudMirror non è supportata per i bucket con S3 Object Lock abilitato.

Requisiti per gli oggetti nei bucket con S3 Object Lock abilitato

- Per proteggere una versione dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure specificare le impostazioni di conservazione per ciascuna versione dell'oggetto. Le impostazioni di conservazione a livello di oggetto possono essere specificate tramite l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni degli oggetti. Una versione di un oggetto può avere sia un'impostazione di conservazione fino alla data di scadenza che un'impostazione di conservazione legale, una ma non l'altra, oppure nessuna delle due. Specificando un'impostazione di conservazione fino a data o di conservazione legale per un oggetto, si 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 abilitato

Ogni oggetto salvato in un bucket con S3 Object Lock abilitato attraversa queste fasi:

1. Ingestione di oggetti

Quando una versione di un oggetto viene aggiunta a un bucket in cui è abilitato il blocco degli oggetti S3, le impostazioni di conservazione vengono applicate come segue:

- Se per l'oggetto sono specificate impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.
- Se non vengono specificate impostazioni di conservazione per l'oggetto, vengono applicate le

impostazioni predefinite del bucket, se presenti.

- Se non vengono 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 sia tutti 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 di copie degli oggetti e le posizioni di archiviazione sono determinati dalle regole conformi nelle policy ILM attive. La possibilità di eliminare un oggetto protetto prima che venga raggiunta la data di conservazione dipende dalla sua modalità di conservazione.

- Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

Posso continuare a gestire i bucket Compliant legacy?

La funzionalità S3 Object Lock sostituisce la funzionalità Compliance disponibile nelle versioni precedenti StorageGRID. Se hai creato bucket conformi utilizzando una versione precedente di StorageGRID, puoi continuare a gestire le impostazioni di questi bucket; tuttavia, non puoi più creare nuovi bucket conformi. Per le istruzioni,

vedere https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"] .

Aggiorna la conservazione predefinita del blocco degli oggetti S3

Se hai abilitato S3 Object Lock quando hai creato il bucket, puoi modificare il bucket per cambiare le impostazioni di conservazione predefinite. È possibile abilitare (o disabilitare) la conservazione predefinita e impostare una modalità di conservazione predefinita e un periodo di conservazione.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti che ha il ["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#) . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- S3 Object Lock è abilitato a livello globale per il sistema StorageGRID e hai abilitato S3 Object Lock quando hai creato il bucket. Vedere ["Utilizzare S3 Object Lock per conservare gli oggetti"](#) .

Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
2. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona la voce accordion **Blocco oggetto S3**.
4. Facoltativamente, abilita o disabilita la **Conservazione predefinita** per questo bucket.

Le modifiche a questa impostazione non si applicano agli oggetti già presenti nel bucket o a quelli che potrebbero avere periodi di conservazione propri.

5. Se è abilitata la **Conservazione predefinita**, specificare una **Modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Governance	• Utenti con il <code>s3:BypassGovernanceRetention</code> il permesso può utilizzare il <code>x-amz-bypass-governance-retention: true</code> intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.
Conformità	• L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione. • La data di conservazione dell'oggetto può essere aumentata, ma non diminuita. • La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data. Nota: l'amministratore della rete deve consentirti di utilizzare la modalità di conformità.

6. Se è abilitata l'opzione **Conservazione predefinita**, specificare il **Periodo di conservazione predefinito** per il bucket.

Il **Periodo di conservazione predefinito** 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 inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della griglia.

Un periodo di conservazione *massimo*, che può essere un valore compreso tra 1 giorno e 100 anni, viene impostato quando l'amministratore della griglia crea il tenant. Quando si imposta un periodo di conservazione *predefinito*, questo non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedi all'amministratore della rete di aumentare o diminuire il periodo massimo di conservazione.

7. Seleziona **Salva modifiche**.

Configurare la condivisione delle risorse tra origini (CORS)

È possibile configurare la condivisione delle risorse tra origini (CORS) per un bucket S3 se si desidera che il bucket e gli oggetti in esso contenuti siano accessibili alle applicazioni Web in altri domini.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Per le richieste di configurazione GET CORS, apparteni a un gruppo di utenti che ha ["Autorizzazione Gestisci tutti i bucket o Visualizza tutti i bucket"](#). Queste autorizzazioni sovrascrivono le impostazioni delle

autorizzazioni nei criteri di gruppo o di bucket.

- Per le richieste di configurazione PUT CORS, appartieni a un gruppo di utenti che ha ["Gestisci tutti i permessi dei bucket"](#). Questa autorizzazione sostituisce le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- IL ["Permesso di accesso root"](#) fornisce l'accesso a tutte le richieste di configurazione CORS.

Informazioni su questo compito

La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni web client in un dominio di accedere alle risorse in un dominio diverso. Ad esempio, supponiamo di utilizzare un bucket S3 denominato `Images` per memorizzare la grafica. Configurando CORS per il `Images` bucket, puoi consentire che le immagini in quel bucket vengano visualizzate sul sito web `http://www.example.com`.

Abilita CORS per un bucket

Passi

1. Utilizzare un editor di testo per creare il file XML richiesto. Questo esempio mostra l'XML utilizzato per abilitare CORS per un bucket S3. Nello specifico:
 - Consente a qualsiasi dominio di inviare richieste GET al bucket
 - Permette solo il `http://www.example.com` dominio per inviare richieste GET, POST e DELETE
 - Sono consentite tutte le intestazioni di richiesta

```
<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 di Amazon Web Services \(AWS\): Guida per l'utente di Amazon Simple Storage Service"](#).

2. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
3. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

4. Dalla scheda **Accesso bucket**, seleziona l'accordione **Condivisione risorse tra origini (CORS)**.

5. Selezionare la casella di controllo **Abilita CORS**.
6. Incollare il file XML di configurazione CORS nella casella di testo.
7. Seleziona **Salva modifiche**.

Modificare l'impostazione CORS

Passi

1. Aggiornare l'XML di configurazione CORS nella casella di testo oppure selezionare **Cancella** per ricominciare.
2. Seleziona **Salva modifiche**.

Disabilita l'impostazione CORS

Passi

1. Deseleziona la casella di controllo **Abilita CORS**.
2. Seleziona **Salva modifiche**.

Elimina gli oggetti nel bucket

È possibile utilizzare Tenant Manager per eliminare gli oggetti in uno o più bucket.

Considerazioni e requisiti

Prima di eseguire questi passaggi, tenere presente quanto segue:

- Quando si eliminano gli oggetti in un bucket, StorageGRID rimuove definitivamente tutti gli oggetti e tutte le versioni degli oggetti in ciascun bucket selezionato da tutti i nodi e siti nel sistema StorageGRID . StorageGRID rimuove anche tutti i metadati degli oggetti correlati. Non sarà possibile recuperare queste informazioni.
- L'eliminazione di tutti gli oggetti in un bucket potrebbe richiedere minuti, giorni o addirittura settimane, a seconda del numero di oggetti, delle copie degli oggetti e delle operazioni simultanee.
- Se un secchio ha "**Blocco oggetto S3 abilitato**", potrebbe rimanere nello stato **Eliminazione oggetti: sola lettura** per *anni*.



Un bucket che utilizza S3 Object Lock rimarrà nello stato **Eliminazione oggetti: sola lettura** finché non verrà raggiunta la data di conservazione per tutti gli oggetti e non verranno rimossi eventuali blocchi legali.

- Durante l'eliminazione degli oggetti, lo stato del bucket è **Eliminazione oggetti: sola lettura**. In questo stato non è possibile aggiungere nuovi oggetti al bucket.
- Una volta eliminati tutti gli oggetti, il bucket rimane in stato di sola lettura. Puoi fare una delle seguenti cose:
 - Riporta il bucket in modalità scrittura e riutilizzalo per nuovi oggetti
 - Elimina il bucket
 - Mantieni il bucket in modalità di sola lettura per riservarne il nome per un uso futuro
- Se in un bucket è abilitato il controllo delle versioni degli oggetti, 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 abilitato il controllo delle versioni degli oggetti, l'operazione di eliminazione degli oggetti non rimuoverà i marcatori di eliminazione creati in StorageGRID 11.7 o versioni precedenti. Visualizza le informazioni sull'eliminazione degli oggetti in un bucket in "[Come vengono eliminati gli oggetti con versione S3](#)".
- Se usi "[replicazione cross-grid](#)", notare quanto segue:
 - Utilizzando questa opzione non si elimina alcun oggetto dal bucket sull'altra griglia.
 - Se selezioni questa opzione per il bucket di origine, verrà attivato l'avviso **Errore di replica tra griglie** se aggiungi oggetti al bucket di destinazione sull'altra griglia. Se non puoi garantire che nessuno aggiungerà oggetti al contenitore sull'altra griglia, "[disabilitare la replicazione tra griglie](#)" per quel bucket prima di eliminare tutti gli oggetti bucket.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)".
- Appartieni a un gruppo di utenti che ha il "[Permesso di accesso root](#)". Questa autorizzazione sostituisce le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (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 Azioni

- a. Seleziona la casella di controllo per ogni bucket da cui desideri eliminare gli oggetti.
- b. Seleziona **Azioni > Elimina oggetti nel bucket**.

Pagina dei dettagli

- a. Seleziona il nome di un bucket per visualizzarne i dettagli.
- b. Seleziona **Elimina oggetti nel bucket**.

3. Quando viene visualizzata la finestra di dialogo di conferma, rivedere i dettagli, immettere **Sì** e selezionare **OK**.
4. Attendi che l'operazione di eliminazione abbia inizio.

Dopo qualche minuto:

- 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)** appare dopo il nome del bucket nella pagina dei dettagli del bucket.
- **(Eliminazione oggetti: sola lettura)** appare accanto al nome del bucket nella pagina Bucket.

Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

View bucket contents in Experimental S3 Console

Delete bucket

 **All bucket objects are being deleted**

StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

Stop deleting objects

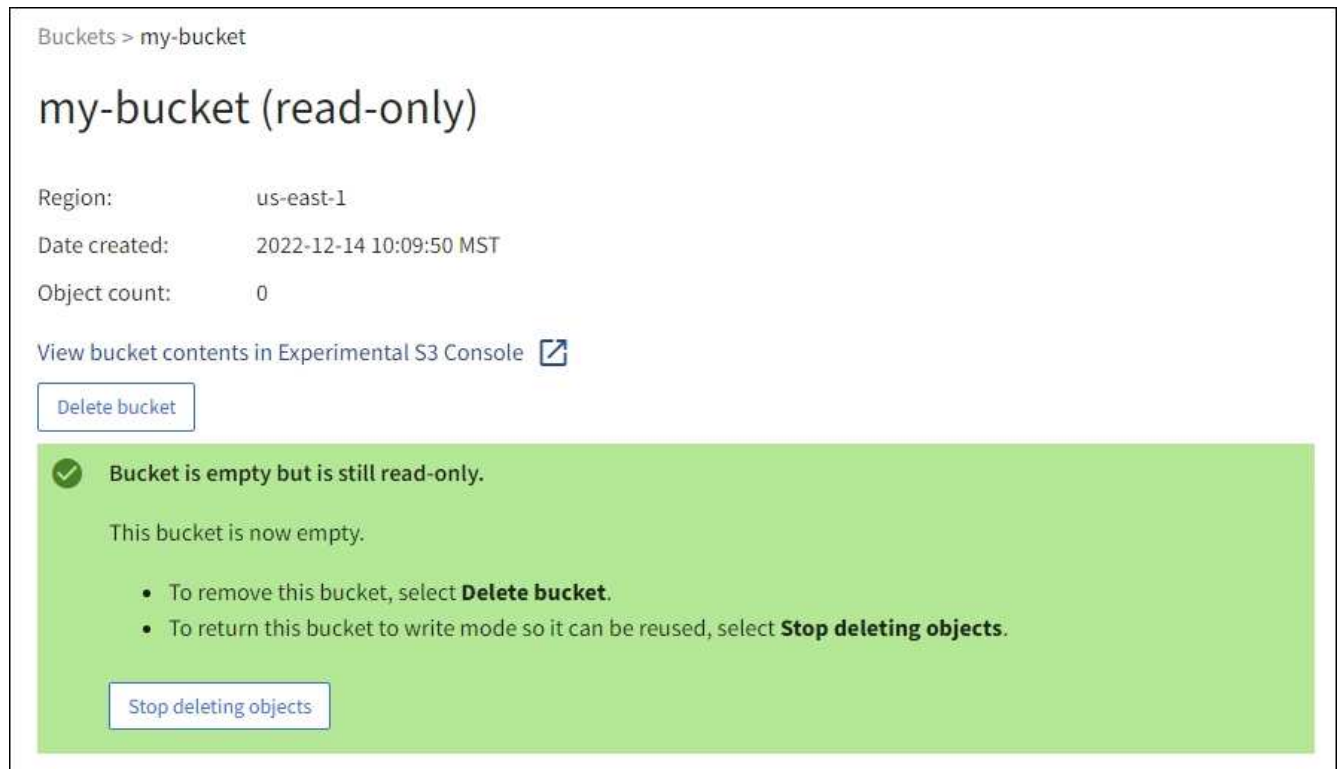
Success
Starting to delete objects from one bucket.

5. Se necessario, durante l'esecuzione dell'operazione, selezionare **Interrompi eliminazione oggetti** per interrompere il processo. Quindi, facoltativamente, seleziona **Elimina oggetti nel bucket** per riprendere il processo.

Quando selezioni **Interrompi eliminazione oggetti**, il bucket torna in modalità scrittura; tuttavia, non puoi accedere o ripristinare gli oggetti che sono stati eliminati.

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. Eseguire una delle seguenti operazioni:

- Esci dalla pagina per mantenere il bucket in modalità di sola lettura. Ad esempio, potresti mantenere un bucket vuoto in modalità di sola lettura per riservare il nome del bucket per un utilizzo futuro.
- Elimina il bucket. È possibile selezionare **Elimina bucket** per eliminare un singolo bucket oppure tornare alla pagina Bucket e selezionare **Azioni > Elimina bucket** per rimuovere più di un bucket.



Se non riesci a eliminare un bucket con versione dopo aver eliminato tutti gli oggetti, i marcatori di eliminazione potrebbero rimanere. Per eliminare il bucket, è necessario rimuovere tutti i marcatori di eliminazione rimanenti.

- Riporta il bucket in modalità scrittura e, facoltativamente, riutilizzalo per nuovi oggetti. È possibile selezionare **Interrompi eliminazione oggetti** per un singolo bucket oppure tornare alla pagina Bucket e selezionare **Azione > Interrompi eliminazione oggetti** per più di un 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 tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- I bucket che vuoi eliminare sono vuoti. Se i bucket che vuoi eliminare *non* sono vuoti, ["elimina gli oggetti dal bucket"](#).

Informazioni su questo compito

Queste istruzioni descrivono come eliminare un bucket S3 utilizzando Tenant Manager. È anche possibile eliminare i bucket S3 utilizzando ["API di gestione degli inquilini"](#) o il ["API REST S3"](#).

Non è possibile eliminare un bucket S3 se contiene oggetti, versioni di oggetti non correnti o marcatori di eliminazione. Per informazioni su come vengono eliminati gli oggetti con versione S3, vedere ["Come vengono eliminati gli oggetti"](#).

Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (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 Azioni

- a. Seleziona la casella di controllo per ogni bucket che desideri eliminare.
- b. Selezionare **Azioni > Elimina bucket**.

Pagina dei dettagli

- a. Seleziona il nome di un bucket per visualizzarne i dettagli.
- b. Seleziona **Elimina bucket**.

3. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Sì**.

StorageGRID conferma che ogni bucket è vuoto e quindi lo elimina. Questa operazione potrebbe richiedere alcuni minuti.

Se un bucket non è vuoto, viene visualizzato un messaggio di errore. Devi ["elimina tutti gli oggetti e tutti i marcatori di eliminazione nel bucket"](#) prima di poter eliminare il bucket.

Utilizzare la console S3

È possibile utilizzare S3 Console per visualizzare e gestire gli oggetti in un bucket S3.

S3 Console ti consente di:

- Carica, scarica, rinomina, copia, sposta ed elimina oggetti
- Visualizza, ripristina, scarica ed elimina le versioni degli oggetti
- Cerca oggetti per prefisso
- Gestisci i tag degli oggetti
- Visualizza i metadati dell'oggetto
- Visualizza, crea, rinomina, copia, sposta ed elimina cartelle



S3 Console 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 fa sì che le operazioni richiedano troppo tempo (ad esempio, minuti o ore), prendere in considerazione quanto segue:

- Riduzione del numero di oggetti selezionati
- Utilizzo di metodi non grafici (API o CLI) per accedere ai dati

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- Se vuoi gestire gli oggetti, devi appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso Root. In alternativa, puoi appartenere a un gruppo di utenti che dispone dell'autorizzazione Utilizza la scheda Console S3 e dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket. Vedere ["Autorizzazioni di gestione degli inquilini"](#) .
- Per l'utente è stato configurato un criterio di gruppo o bucket S3. Vedere ["Utilizzare criteri di accesso a bucket e gruppi"](#) .
- Conosci l'ID della chiave di accesso dell'utente e la chiave di accesso segreta. Facoltativamente, hai un .csv file contenente queste informazioni. Vedi il ["istruzioni per la creazione delle chiavi di accesso"](#) .

Passi

1. Selezionare **ARCHIVIAZIONE > Bucket > nome bucket**.
2. Selezionare la scheda Console S3.
3. Incolla l'ID della chiave di accesso e la chiave di accesso segreta nei campi. Altrimenti, seleziona **Carica chiavi di accesso** e seleziona il tuo .csv file.
4. Seleziona * Sign in*.
5. Viene visualizzata la tabella degli oggetti bucket. Puoi gestire gli oggetti in base alle tue esigenze.

Informazioni aggiuntive

- **Cerca per prefisso:** la funzione di ricerca per prefisso cerca solo gli oggetti che iniziano con una parola specifica relativa alla cartella corrente. La ricerca non include gli oggetti che contengono la parola altrove. Questa regola si applica anche agli oggetti all'interno delle cartelle. Ad esempio, una ricerca per `folder1/folder2/somefile-` restituirebbe oggetti che si trovano all'interno di `folder1/folder2/` cartella e inizia con la parola `somefile-` .
- **Trascinamento della selezione:** puoi trascinare e rilasciare i file dal file manager del tuo computer a S3 Console. Tuttavia, non è possibile caricare cartelle.
- **Operazioni sulle cartelle:** quando si sposta, si copia o si rinomina una cartella, tutti gli oggetti al suo interno vengono aggiornati uno alla volta, il che potrebbe richiedere del tempo.
- **Eliminazione definitiva quando il controllo delle versioni del bucket è disabilitato:** quando si sovrascrive o si elimina un oggetto in un bucket con il controllo delle versioni disabilitato, l'operazione è definitiva. Vedere ["Modificare il controllo delle versioni degli oggetti per un bucket"](#) .

Gestire i servizi della piattaforma S3

Servizi della piattaforma S3

Panoramica e considerazioni sui servizi della piattaforma

Prima di implementare i servizi della piattaforma, rivedere la panoramica e le considerazioni sull'utilizzo di questi servizi.

Per informazioni su S3, vedere ["Utilizzare l'API REST S3"](#) .

Panoramica dei servizi della piattaforma

I servizi della piattaforma StorageGRID possono aiutarti a implementare una strategia cloud ibrida consentendoti di inviare notifiche di eventi e copie di oggetti S3 e metadati di oggetti a destinazioni esterne.

Poiché la posizione di destinazione per i servizi di piattaforma è in genere esterna alla distribuzione StorageGRID , i servizi di piattaforma offrono la potenza e la flessibilità derivanti dall'utilizzo di risorse di archiviazione esterne, servizi di notifica e servizi di ricerca o analisi per i dati.

Per un singolo bucket S3 è possibile configurare qualsiasi combinazione di servizi di piattaforma. Ad esempio, è possibile configurare entrambi i ["Servizio CloudMirror"](#) E ["notifiche"](#) su un bucket StorageGRID S3 in modo da poter eseguire il mirroring di oggetti specifici su Amazon Simple Storage Service (S3), inviando al contempo una notifica su ciascun oggetto a un'applicazione di monitoraggio di terze parti per aiutarti a tenere traccia delle tue spese AWS.



L'utilizzo dei servizi della piattaforma deve essere abilitato per ciascun account tenant da un amministratore StorageGRID tramite Grid Manager o Grid Management API.

Come sono configurati i servizi della piattaforma

I servizi della piattaforma comunicano con endpoint esterni configurati tramite ["Responsabile degli inquilini"](#) o il ["API di gestione degli inquilini"](#) . Ogni endpoint rappresenta una destinazione esterna, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento Amazon SNS o un cluster Elasticsearch ospitato localmente, su AWS o altrove.

Dopo aver creato un endpoint esterno, puoi abilitare 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 della piattaforma che si desidera configurare. Per esempio:

- Se vuoi 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 archiviati nel bucket, è necessario aggiungere una configurazione delle notifiche.
- 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 CloudMirror	• <code>OttieniReplicazioneBucket</code> • <code>PutBucketReplication</code>	• "Replica CloudMirror" • "Operazioni sui bucket"
Notifiche	• Configurazione di notifica di <code>GetBucket</code> • Configurazione della notifica <code>PutBucket</code>	• "Notifiche" • "Operazioni sui bucket"

Servizio di piattaforma	API REST S3	Fare riferimento a
Integrazione della ricerca	• Configurazione della notifica dei metadati del bucket GET • Configurazione della notifica dei metadati del bucket PUT	• "Integrazione della ricerca" • "Operazioni personalizzate StorageGRID"

Considerazioni sull'utilizzo dei servizi della piattaforma

Considerazione	Dettagli
Monitoraggio dell'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 e si verifica un arretrato di richieste elevato, le richieste client aggiuntive (ad esempio le richieste PUT) a StorageGRID non riusciranno. È necessario riprovare queste richieste non riuscite quando l'endpoint diventa raggiungibile.
Limitazione dell'endpoint di destinazione	Il software StorageGRID potrebbe limitare le richieste S3 in arrivo per un bucket se la velocità con cui vengono inviate le richieste supera la velocità con cui l'endpoint di destinazione può riceverle. La limitazione si verifica solo quando è presente un arretrato di richieste in attesa di essere inviate all'endpoint di destinazione. L'unico effetto visibile è che le richieste S3 in arrivo impiegheranno più tempo per essere eseguite. Se si inizia a rilevare un rallentamento significativo delle prestazioni, è opportuno ridurre la velocità di acquisizione o utilizzare un endpoint con capacità maggiore. Se l'arretrato di richieste continua ad aumentare, le operazioni S3 del client (come le richieste PUT) alla fine falliranno. Le richieste CloudMirror hanno maggiori probabilità di essere influenzate dalle prestazioni dell'endpoint di destinazione, perché in genere comportano un trasferimento di dati maggiore rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.
Garanzie di ordinazione	StorageGRID garantisce l'ordinamento delle operazioni su un oggetto all'interno di un sito. Finché tutte le operazioni su un oggetto avvengono nello stesso sito, lo stato finale dell'oggetto (per la replica) sarà sempre uguale allo stato in StorageGRID. StorageGRID fa del suo meglio per ordinare le richieste quando le operazioni vengono eseguite tra i siti StorageGRID. Ad esempio, se inizialmente si scrive un oggetto sul sito A e poi si sovrascrive lo stesso oggetto sul sito B, non è garantito che l'oggetto finale replicato da CloudMirror nel bucket di destinazione sia l'oggetto più recente.

Considerazione	Dettagli
Eliminazioni di oggetti guidate da ILM	Per adeguarsi al comportamento di eliminazione di AWS CRR e Amazon Simple Notification Service, le richieste di notifica di eventi e CloudMirror non vengono inviate quando un oggetto nel bucket di origine viene eliminato a causa delle regole StorageGRID ILM. Ad esempio, non vengono inviate richieste di notifiche di eventi o CloudMirror se una regola ILM elimina un oggetto dopo 14 giorni. 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, Mutual TLS non è supportato. Di conseguenza, se hai <code>ssl.client.auth</code> impostato su <code>required</code> nella configurazione del broker Kafka, potrebbe causare problemi di configurazione dell'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 di nome utente e password. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 Nota: le impostazioni del 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 di replicazione	StorageGRID non supporta il <code>x-amz-replication-status</code> intestazione.
Dimensione dell'oggetto	La dimensione massima degli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è 5 TiB, che è la stessa della dimensione massima <i>supportata</i> dell'oggetto. Nota: la dimensione massima <i>consigliata</i> per una singola operazione PutObject è 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa invece il caricamento multiparte.
Versionamento del bucket e ID versione	Se il bucket S3 di origine in StorageGRID ha il controllo delle versioni abilitato, è necessario abilitare il controllo delle versioni anche per il bucket di destinazione. Quando si utilizza il controllo delle versioni, tenere presente che l'ordinamento delle versioni degli oggetti nel bucket di destinazione è basato sul miglior sforzo possibile e non è garantito dal servizio CloudMirror, a causa delle limitazioni del protocollo S3. Nota: gli ID versione per il bucket di origine in StorageGRID non sono correlati agli ID versione per il bucket di destinazione.

Considerazione	Dettagli
Tagging per le versioni degli oggetti	A causa delle limitazioni del protocollo S3, il servizio CloudMirror non replica alcuna richiesta PutObjectTagging o DeleteObjectTagging che fornisca un ID versione. Poiché gli ID versione per l'origine e la destinazione non sono correlati, non esiste alcun modo per garantire che un aggiornamento del tag a un ID versione specifico venga replicato. Al contrario, il servizio CloudMirror replica le richieste PutObjectTagging o DeleteObjectTagging che non specificano un ID versione. Queste richieste aggiornano i tag per la chiave più recente (o per l'ultima versione se il bucket è sottoposto a versioning). Vengono replicati anche gli ingest normali con tag (non gli aggiornamenti dei tag).
Caricamenti multiparte e ETag valori	Quando si esegue il mirroring di oggetti caricati tramite un caricamento multiparte, il servizio CloudMirror non conserva le parti. Di conseguenza, il ETag il valore per l'oggetto specchiato sarà diverso da quello ETag valore dell'oggetto originale.
Oggetti crittografati con SSE-C (crittografia lato server con chiavi fornite dal cliente)	Il servizio CloudMirror non supporta oggetti crittografati con SSE-C. Se si tenta di importare un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione fallisce.
Bucket con blocco oggetto S3 abilitato	La replica non è supportata per i bucket di origine o di destinazione con S3 Object Lock abilitato.

Comprendere il servizio di replica CloudMirror

È possibile abilitare la replica CloudMirror per un bucket S3 se si desidera che StorageGRID replichi gli oggetti specificati aggiunti al bucket in uno o più bucket di destinazione esterni.

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



La replica CloudMirror non è supportata se nel bucket di origine è abilitato S3 Object Lock.

CloudMirror e ILM

La replica di CloudMirror funziona indipendentemente dalle policy ILM attive della griglia. Il servizio CloudMirror replica gli oggetti così come vengono archiviati nel bucket di origine e li distribuisce al bucket di destinazione il prima possibile. La consegna degli oggetti replicati viene attivata quando l'acquisizione dell'oggetto riesce.

CloudMirror e replicazione cross-grid

La replica di CloudMirror presenta importanti somiglianze e differenze con la funzionalità di replica tra griglie. Fare riferimento a ["Confronta la replicazione cross-grid e la replicazione CloudMirror"](#).

CloudMirror e bucket S3

La replica CloudMirror è in genere configurata per utilizzare un bucket S3 esterno come destinazione. Tuttavia, è anche possibile configurare la replica in modo che utilizzi un'altra distribuzione StorageGRID o qualsiasi servizio compatibile con S3.

Secchi esistenti

Quando si abilita la replica CloudMirror per un bucket esistente, vengono replicati solo i nuovi oggetti aggiunti a quel bucket. Tutti gli oggetti esistenti nel bucket non vengono replicati. Per forzare la replica di 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 di richiesta PUT a 2 KB. Se un oggetto ha metadati definiti dall'utente maggiori di 2 KB, tale oggetto non verrà replicato.

Più bucket di destinazione

Per replicare gli oggetti in un singolo bucket su più bucket di destinazione, specificare la destinazione per ciascuna regola nel file XML di configurazione della replica. Non è possibile replicare un oggetto in più bucket contemporaneamente.

Bucket con o senza versione

È possibile configurare la replica di CloudMirror su bucket con o senza versione. I bucket di destinazione possono essere dotati o meno di versione. È possibile utilizzare qualsiasi combinazione di bucket con e senza controllo delle versioni. Ad esempio, è possibile specificare un bucket con versione come destinazione per un bucket di origine senza versione o viceversa. È anche possibile replicare tra bucket senza controllo delle versioni.

Eliminazione, cicli di replicazione ed eventi

Comportamento di eliminazione

È lo stesso comportamento di eliminazione del servizio Amazon S3, Cross-Region Replication (CRR). 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 sottoposti a versioning, il marcatore di eliminazione viene replicato. Se il bucket di destinazione non è sottoposto a controllo di versione, l'eliminazione di un oggetto nel bucket di origine non replica il marcatore di eliminazione nel bucket di destinazione né elimina l'oggetto di destinazione.

Protezione dai cicli di replicazione

Quando gli oggetti vengono replicati nel bucket di destinazione, StorageGRID li contrassegna come "repliche". Un bucket StorageGRID di destinazione non replicherà più gli oggetti contrassegnati come repliche, proteggendoti da loop di replica accidentali. Questa marcatura della replica è interna 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`. Questa marcatura impedisce la formazione di uno specchio a cascata. StorageGRID supporta un CloudMirror bidirezionale tra due griglie.

Eventi nel bucket di destinazione

L'unicità e l'ordinamento degli eventi nel bucket di destinazione non sono garantiti. A seguito delle operazioni intraprese per garantire il successo della consegna, potrebbero essere consegnate alla

destinazione più copie identiche di un oggetto sorgente. In rari casi, quando lo stesso oggetto viene aggiornato simultaneamente da due o più siti StorageGRID diversi, l'ordinamento delle operazioni sul bucket di destinazione potrebbe non corrispondere all'ordinamento degli eventi sul bucket di origine.

Comprendere le notifiche per i bucket

È possibile abilitare la notifica degli eventi per un bucket S3 se si desidera che StorageGRID invii notifiche su eventi specifici a un cluster Kafka di destinazione o ad Amazon Simple Notification Service.

Ad esempio, è possibile configurare l'invio di avvisi agli amministratori per ogni oggetto aggiunto a un bucket, dove gli oggetti rappresentano file di registro associati a un evento di sistema critico.

Le notifiche degli eventi vengono create nel bucket di origine come specificato nella configurazione delle notifiche e vengono recapitate 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 la consegna.

L'unicità e l'ordinamento delle notifiche non sono garantiti. A seguito delle operazioni intraprese per garantire il successo della consegna, potrebbero essere recapitate alla destinazione più notifiche relative a un evento. Poiché la consegna è asincrona, non è garantito che l'ordinamento temporale delle notifiche a destinazione corrisponda all'ordinamento degli eventi nel bucket di origine, in particolare per le operazioni che hanno origine da siti StorageGRID diversi. Puoi usare il `sequencer` digitare nel messaggio dell'evento per determinare l'ordine degli eventi per un oggetto specifico, come descritto nella documentazione di Amazon S3.

Le notifiche degli eventi StorageGRID seguono l'API Amazon S3 con alcune limitazioni.

- Sono supportati i seguenti tipi di eventi:
 - s3:OggettoCreato:
 - s3:OggettoCreato:Metti
 - s3:OggettoCreato:Post
 - s3:OggettoCreato:Copia
 - s3:ObjectCreated:CompleteMultipartUpload
 - s3:ObjectRemoved:
 - s3:ObjectRemoved:Elimina
 - s3:ObjectRemoved>DeleteMarkerCreated
 - s3:ObjectRestore:Post
- 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 chiave	Valore StorageGRID
origineevento	sgws : s3
Regione aws	<i>non incluso</i>
x-amz-id-2	<i>non incluso</i>

Nome chiave	Valore StorageGRID
arn	urn:sgws:s3:::bucket_name

Comprendere il servizio di integrazione della ricerca

È possibile abilitare 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 degli oggetti S3 a un endpoint di destinazione ogni volta che un oggetto viene creato o eliminato oppure i suoi metadati o tag vengono aggiornati. È quindi possibile utilizzare strumenti sofisticati di ricerca, analisi dei dati, visualizzazione o apprendimento automatico forniti dal servizio di destinazione per cercare, analizzare e ottenere informazioni dai dati degli oggetti.

Ad esempio, puoi configurare i tuoi bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. Potresti quindi utilizzare Elasticsearch per effettuare ricerche tra i bucket e realizzare analisi sofisticate dei modelli presenti nei metadati degli oggetti.

Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Retain Until Date e Legal Hold) degli oggetti non saranno inclusi nei metadati inviati a Elasticsearch.



Poiché il servizio di integrazione della ricerca determina l'invio dei metadati degli oggetti a una destinazione, il suo XML di configurazione viene denominato "XML di configurazione della notifica *metadata*". Questo XML di configurazione è diverso dal "XML di configurazione delle notifiche" utilizzato per abilitare le notifiche *event*.

Integrazione della ricerca e bucket S3

È possibile abilitare il servizio di integrazione della ricerca per qualsiasi bucket con o senza versione. L'integrazione della ricerca viene configurata associando l'XML di configurazione delle notifiche dei metadati al bucket che specifica su quali oggetti agire e la destinazione dei metadati degli oggetti.

Le notifiche dei metadati vengono generate sotto forma di documento JSON denominato con il nome del bucket, il nome dell'oggetto e l'ID della versione, se presente. 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 utente.



Per i tag e i metadati utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo che interpreti queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per la mappatura dei formati di data. È necessario abilitare i mapping dei campi dinamici sull'indice prima di configurare il servizio di integrazione della ricerca. Dopo aver indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Notifiche di ricerca

Le notifiche dei metadati 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 a seguito dell'esecuzione della politica ILM della griglia.

- I metadati o i tag degli oggetti vengono aggiunti, aggiornati o eliminati. Durante l'aggiornamento viene sempre inviato l'insieme completo di metadati e tag, non solo i valori modificati.

Dopo aver aggiunto l'XML di configurazione delle notifiche dei metadati a un bucket, le notifiche vengono inviate per tutti i nuovi oggetti creati e per tutti gli oggetti modificati aggiornandone i dati, i metadati utente o i tag. Tuttavia, le notifiche non vengono inviate per gli oggetti che erano già presenti nel bucket. Per garantire che i metadati degli oggetti per tutti gli oggetti nel bucket vengano inviati alla destinazione, è necessario effettuare una delle seguenti operazioni:

- Configurare il servizio di integrazione della ricerca subito dopo aver creato il bucket e prima di aggiungere qualsiasi oggetto.
- Esegui un'azione su tutti gli oggetti già presenti nel bucket che attiverà l'invio di un messaggio di notifica dei metadati alla destinazione.

Servizio di integrazione della ricerca ed Elasticsearch

Il servizio di integrazione della ricerca StorageGRID supporta un cluster Elasticsearch come destinazione. Come per gli altri servizi della piattaforma, la destinazione è specificata nell'endpoint il cui URN viene utilizzato nell'XML di configurazione per il servizio. Utilizzare il ["Strumento matrice di interoperabilità NetApp"](#) per determinare le versioni supportate di Elasticsearch.

Gestire gli endpoint dei servizi della piattaforma

Configurare gli endpoint dei servizi della piattaforma

Prima di poter configurare un servizio di piattaforma per un bucket, è necessario configurare almeno un endpoint come destinazione per il servizio di piattaforma.

L'accesso ai servizi della piattaforma è abilitato per ogni tenant da un amministratore StorageGRID . Per creare o utilizzare un endpoint dei servizi di piattaforma, è necessario essere un utente tenant con autorizzazione di gestione degli endpoint o di accesso root, in una griglia la cui rete è stata configurata per consentire ai nodi di archiviazione di accedere alle risorse degli endpoint esterni. Per un singolo tenant è possibile configurare un massimo di 500 endpoint dei servizi della piattaforma. Per ulteriori informazioni, contattare l'amministratore StorageGRID .

Che cos'è un endpoint dei servizi di piattaforma?

Un endpoint dei servizi di piattaforma specifica le informazioni di cui StorageGRID ha bisogno per accedere alla destinazione esterna.

Ad esempio, se si desidera replicare oggetti da un bucket StorageGRID a un bucket Amazon S3, è necessario creare un endpoint dei servizi di piattaforma che includa le informazioni e le credenziali necessarie a StorageGRID per accedere al bucket di destinazione su Amazon.

Ogni tipo di servizio di piattaforma richiede il proprio endpoint, quindi è necessario configurare almeno un endpoint per ogni servizio di piattaforma che si intende utilizzare. Dopo aver definito un endpoint dei servizi della piattaforma, si utilizza l'URN dell'endpoint come destinazione nell'XML di configurazione utilizzato per abilitare il servizio.

È possibile utilizzare lo stesso endpoint come destinazione per più di un bucket di origine. Ad esempio, è possibile configurare più bucket di origine per inviare metadati di oggetti allo stesso endpoint di integrazione della ricerca, in modo da poter eseguire ricerche su più bucket. È anche possibile configurare un bucket di origine in modo che utilizzi più di un endpoint come destinazione, il che consente di eseguire operazioni come 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 CloudMirror

StorageGRID supporta endpoint di replica che rappresentano bucket S3. Questi bucket potrebbero essere ospitati su Amazon Web Services, sullo stesso o su una distribuzione StorageGRID remota, oppure su un altro servizio.

Endpoint per le notifiche

StorageGRID supporta gli endpoint Amazon SNS e Kafka. Gli endpoint Simple Queue Service (SQS) o AWS Lambda non sono supportati.

Per gli endpoint Kafka, Mutual TLS non è supportato. Di conseguenza, se hai `ssl.client.auth` impostato su `required` nella configurazione del broker Kafka, potrebbe causare problemi di configurazione dell'endpoint Kafka.

Endpoint per il servizio di integrazione della ricerca

StorageGRID supporta endpoint di integrazione della ricerca che rappresentano cluster Elasticsearch. Questi cluster Elasticsearch possono trovarsi in un data center locale oppure essere ospitati in un cloud AWS o altrove.

L'endpoint di integrazione della ricerca fa riferimento a un indice e a un tipo Elasticsearch specifici. È necessario creare l'indice in Elasticsearch prima di creare l'endpoint in StorageGRID, altrimenti la creazione dell'endpoint non riuscirà. Non è necessario creare il tipo prima di creare l'endpoint. StorageGRID creerà il tipo, se necessario, quando invia i metadati dell'oggetto all'endpoint.

Informazioni correlate

["Amministra StorageGRID"](#)

Specificare l'URN per l'endpoint dei servizi della piattaforma

Quando si crea un endpoint dei servizi della piattaforma, è necessario specificare un nome di risorsa univoco (URN). L'URN verrà utilizzato per fare riferimento all'endpoint quando si crea un XML di configurazione per il servizio della piattaforma. L'URN per ciascun endpoint deve essere univoco.

StorageGRID convalida gli endpoint dei servizi della piattaforma man mano che li crei. Prima di creare un endpoint dei servizi della piattaforma, verificare che la risorsa specificata nell'endpoint esista e che sia raggiungibile.

Elementi URN

L'URN per un endpoint dei servizi di piattaforma deve iniziare con `arn:aws` O `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 CloudMirror	s3
Notifiche	sns`O `kafka
Integrazione della ricerca	es

Ad esempio, per continuare a specificare l'URN per un endpoint CloudMirror ospitato su StorageGRID, è necessario aggiungere s3 ottenere `urn:sgws:s3`.

L'elemento finale dell'URN identifica la risorsa di destinazione specifica nell'URI di destinazione.

Servizio	Risorsa specifica
Replica CloudMirror	bucket-name
Notifiche	sns-topic-name`O `kafka-topic-name
Integrazione della ricerca	domain-name/index-name/type-name Nota: se il cluster Elasticsearch non è configurato per creare indici automaticamente, è necessario creare l'indice manualmente prima di creare l'endpoint.

URN per servizi ospitati su AWS e GCP

Per le entità AWS e GCP, l'URN completo è un ARN AWS valido. Per esempio:

- Replica 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, `domain-name` deve includere la stringa letterale `domain/`, come mostrato qui.

URN per servizi ospitati localmente

Quando si utilizzano servizi ospitati localmente anziché 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 come facoltativi oppure specificarli in qualsiasi modo che aiuti a identificare la risorsa e a rendere univoco l'URN. Per esempio:

- Replica 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 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, `domain-name` l'elemento può essere qualsiasi stringa purché l'URN dell'endpoint sia univoco.

Crea endpoint dei servizi della piattaforma

È necessario creare almeno un endpoint del tipo corretto prima di poter abilitare un servizio di piattaforma.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- I servizi della piattaforma sono stati abilitati per il tuo account tenant da un amministratore StorageGRID .
- Appartieni a un gruppo di utenti che ha il ["Gestisci endpoint o autorizzazione di accesso root"](#) .
- La risorsa a cui fa riferimento l'endpoint dei servizi della piattaforma è stata creata:
 - Replica CloudMirror: bucket S3
 - Notifica evento: Amazon Simple Notification Service (Amazon SNS) o argomento Kafka
 - Notifica di ricerca: indice Elasticsearch, se il cluster di destinazione non è configurato per creare automaticamente indici.
- Hai le informazioni sulla 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 CloudMirror, contattare l'amministratore della griglia per determinare i valori da immettere.

- Nome univoco della risorsa (URN)

["Specificare l'URN per l'endpoint dei servizi della piattaforma"](#)

- Credenziali di autenticazione (se richieste):

Cerca endpoint di integrazione

Per gli endpoint di integrazione della ricerca, puoi utilizzare le seguenti credenziali:

- Chiave di accesso: ID chiave di accesso e chiave di accesso segreta
- HTTP di base: nome utente e password

Endpoint di replicazione CloudMirror

Per gli endpoint di replica CloudMirror, puoi utilizzare le seguenti credenziali:

- Chiave di accesso: ID chiave di accesso e chiave di accesso segreta
- CAP (C2S Access Portal): URL delle credenziali temporanee, certificati server e client, chiavi client e una passphrase facoltativa per la chiave privata del client.

Endpoint Amazon SNS

Per gli endpoint Amazon SNS, puoi utilizzare le seguenti credenziali:

- Chiave di accesso: ID chiave di accesso e chiave di accesso segreta

Punti finali di Kafka

Per gli endpoint Kafka, puoi 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 sicurezza (se si utilizza un certificato CA personalizzato)
- Se le funzionalità di sicurezza di Elasticsearch sono abilitate, si dispone del privilegio di monitoraggio del cluster per i test di connettività e del privilegio di scrittura dell'indice oppure di entrambi i privilegi di indice ed eliminazione dell'indice per gli aggiornamenti dei documenti.

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Endpoint dei servizi di piattaforma**. Viene visualizzata la pagina Endpoint dei servizi della piattaforma.
2. Selezionare **Crea endpoint**.
3. Immettere un nome visualizzato per descrivere brevemente l'endpoint e il suo scopo.

Il tipo di servizio di piattaforma supportato dall'endpoint viene visualizzato accanto al nome dell'endpoint quando è elencato nella pagina Endpoint, quindi non è necessario includere tale informazione 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 gli URI HTTPS e porta 80 per gli URI HTTP (la maggior parte degli endpoint)
- Porta 9092 per HTTPS e URI 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 ad alta disponibilità (HA) StorageGRID e `10443` rappresenta la porta definita nell'endpoint del bilanciatore del carico.



Se possibile, è opportuno connettersi a un gruppo HA di nodi di bilanciamento del carico per evitare un singolo punto di errore.

Allo stesso modo, 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. Inserisci il nome del bucket nel campo **URN**.

5. Immettere il nome univoco della risorsa (URN) per l'endpoint.



Non è possibile modificare l'URN di un endpoint dopo averlo creato.

6. Selezionare **Continua**.

7. Selezionare un valore per **Tipo di autenticazione**.

Cerca endpoint di integrazione

Inserisci o carica le credenziali per un endpoint di integrazione della ricerca.

Le credenziali fornite devono disporre di autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali in stile 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 replicazione CloudMirror

Inserisci o carica le credenziali per un endpoint di replica CloudMirror.

Le credenziali fornite devono disporre di autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali in stile 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 delle credenziali temporanee • 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 crittografata) • Passphrase della chiave privata del client (facoltativa)

Endpoint Amazon SNS

Inserisci o carica le credenziali per un endpoint Amazon SNS.

Le credenziali fornite devono disporre di autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali in stile AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta

Punti finali di Kafka

Inserisci o carica le credenziali per un endpoint Kafka.

Le credenziali fornite devono disporre di autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
SASL/PLAIN	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 tramite un protocollo challenge-response e l'hashing SHA-256 per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-512	Utilizza un nome utente e una password tramite un protocollo challenge-response e l'hashing SHA-512 per autenticare le connessioni alla destinazione.	• Nome utente • Password

Selezionare **Usa autenticazione tramite delega** se il nome utente e la password derivano da un token di delega ottenuto da un cluster Kafka.

8. Selezionare **Continua**.

9. Selezionare un pulsante di opzione per **Verifica server** per scegliere come verificare la connessione TLS all'endpoint.

Tipo di verifica del certificato	Descrizione
Utilizza un certificato CA personalizzato	Utilizzare un certificato di sicurezza personalizzato. Se selezioni questa impostazione, copia e incolla il certificato di sicurezza personalizzato nella casella di testo Certificato CA .
Utilizzare il certificato CA del sistema operativo	Per proteggere le connessioni, utilizzare il certificato Grid CA predefinito installato sul sistema operativo.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non è verificato. Questa opzione non è sicura.

10. Selezionare **Test e crea endpoint**.

- Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di operazione riuscita. 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, seleziona **Test e crea endpoint**.



La creazione dell'endpoint non riesce se i servizi della piattaforma non sono abilitati per l'account tenant. Contatta l'amministratore StorageGRID .

Dopo aver configurato un endpoint, è possibile utilizzare il suo URN per configurare un servizio di piattaforma.

Informazioni correlate

- ["Specificare l'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"](#)

Prova la connessione per l'endpoint dei servizi della piattaforma

Se la connessione a un servizio della piattaforma è cambiata, è possibile testare la connessione per l'endpoint per convalidare che la risorsa di destinazione esista e che possa essere raggiunta utilizzando le credenziali specificate.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti che ha il ["Gestisci endpoint o autorizzazione di accesso root"](#) .

Informazioni su questo compito

StorageGRID non convalida che le credenziali abbiano le autorizzazioni corrette.

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Endpoint dei servizi di piattaforma**.

Viene visualizzata la pagina Endpoint dei servizi di piattaforma, che mostra l'elenco degli endpoint dei servizi di piattaforma già configurati.

2. Selezionare l'endpoint di cui si desidera testare la connessione.

Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Test connessione**.

- Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di operazione riuscita. 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 **Configurazione** e aggiornare le informazioni. Quindi, seleziona **Testa e salva modifiche**.

Modifica endpoint dei servizi della piattaforma

È possibile modificare la configurazione di un endpoint dei servizi della piattaforma per cambiarne 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 dei servizi della piattaforma.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Gestisci endpoint o autorizzazione di accesso root"](#).

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Endpoint dei servizi di piattaforma**.

Viene visualizzata la pagina Endpoint dei servizi di piattaforma, che mostra l'elenco degli endpoint dei servizi di piattaforma già configurati.

2. Seleziona l'endpoint che vuoi 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 averlo creato.

- a. Per modificare il nome visualizzato per l'endpoint, seleziona l'icona di modifica .
- b. Se necessario, modificare l'URI.
- c. Se necessario, modificare il tipo di autenticazione.
 - Per l'autenticazione con chiave di accesso, modificare la chiave secondo necessità selezionando **Modifica chiave S3** e incollando un nuovo ID chiave di accesso e una chiave di accesso segreta. Se devi annullare le modifiche, seleziona **Annulla modifica chiave S3**.

- Per l'autenticazione CAP (C2S Access Portal), modificare l'URL delle credenziali temporanee o la passphrase della chiave privata del client facoltativa e caricare nuovi file di certificato e chiave secondo necessità.



La chiave privata del client deve essere in formato crittografato OpenSSL o in formato chiave privata non crittografata.

d. Se necessario, modificare il metodo di verifica del server.

5. Seleziona **Testa e salva le modifiche**.

- Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di operazione riuscita. 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 salva modifiche**.

Elimina l'endpoint dei servizi della piattaforma

È possibile eliminare un endpoint se non si desidera più utilizzare il servizio della piattaforma associato.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Gestisci endpoint o autorizzazione di accesso root"](#).

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Endpoint dei servizi di piattaforma**.

Viene visualizzata la pagina Endpoint dei servizi di piattaforma, che mostra l'elenco degli endpoint dei servizi di piattaforma già configurati.

2. Seleziona la casella di controllo per ogni endpoint che desideri eliminare.



Se si elimina un endpoint dei servizi di piattaforma in uso, il servizio di piattaforma associato verrà disabilitato per tutti i bucket che utilizzano l'endpoint. Tutte le richieste non ancora completate verranno eliminate. Tutte le nuove richieste continueranno a essere generate finché non modifichi la configurazione del bucket in modo che non faccia più riferimento all'URN eliminato. StorageGRID segnalerà queste richieste come errori irrecoverabili.

3. Selezionare **Azioni > Elimina endpoint**.

Appare un messaggio di conferma.

4. Selezionare **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 nella dashboard. Nella pagina Endpoint dei servizi della piattaforma, la colonna Ultimo errore indica da quanto tempo si è verificato l'errore. Se le autorizzazioni associate alle credenziali di un endpoint sono errate, non viene visualizzato alcun errore.

Determina se si è verificato un errore

Se negli ultimi 7 giorni si sono verificati errori degli endpoint dei servizi della piattaforma, la dashboard di Tenant Manager visualizza un messaggio di avviso. Per maggiori dettagli sull'errore, puoi andare alla pagina Endpoint dei servizi della piattaforma.

 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.

Lo stesso errore che appare nella dashboard appare anche nella parte superiore della pagina Endpoint dei servizi della piattaforma. Per visualizzare un messaggio di errore più dettagliato:

Passi

1. Dall'elenco degli endpoint, seleziona quello che presenta l'errore.
2. Nella pagina dei dettagli dell'endpoint, seleziona **Connessione**. Questa scheda visualizza solo l'errore più recente per un endpoint e indica da quanto tempo si è verificato l'errore. Errori che includono l'icona X rossa  si sono verificati negli ultimi 7 giorni.

Controlla se l'errore è ancora attuale

Alcuni errori potrebbero continuare a essere visualizzati nella colonna **Ultimo errore** anche dopo essere stati risolti. Per verificare se un errore è attuale o per forzare la rimozione di un errore risolto dalla tabella:

Passi

1. Selezionare l'endpoint.

Viene visualizzata la pagina dei dettagli dell'endpoint.

2. Selezionare **Connessione > Test connessione**.

Selezionando **Test connessione**, StorageGRID convalida che l'endpoint dei servizi della piattaforma esiste e che può essere raggiunto con le credenziali correnti. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Risolvi gli errori dell'endpoint

È possibile utilizzare il messaggio **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, può verificarsi un errore CloudMirroring se StorageGRID non è in grado di accedere al bucket S3 di destinazione perché non dispone delle autorizzazioni di accesso corrette o la chiave di accesso è scaduta. 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 **Test e salva modifiche** StorageGRID convalida l'endpoint aggiornato e conferma che può essere raggiunto con le credenziali correnti. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Passi

1. Selezionare l'endpoint.
2. Nella pagina dei dettagli dell'endpoint, seleziona **Configurazione**.
3. Modificare la configurazione dell'endpoint secondo necessità.

4. Selezionare **Connessione > Test connessione**.

Credenziali dell'endpoint con autorizzazioni insufficienti

Quando StorageGRID convalida un endpoint dei servizi della piattaforma, conferma che le credenziali dell'endpoint possono essere utilizzate per contattare la risorsa di destinazione ed esegue un controllo di base delle autorizzazioni. Tuttavia, StorageGRID non convalida tutte le autorizzazioni richieste per determinate operazioni dei servizi della piattaforma. Per questo motivo, se si riceve un errore quando si tenta di utilizzare un servizio della piattaforma (ad esempio "403 Forbidden"), verificare le autorizzazioni associate alle credenziali dell'endpoint.

Informazioni correlate

- [Amministra StorageGRID > Risolvi i problemi dei servizi della piattaforma](#)
- ["Crea endpoint dei servizi della piattaforma"](#)
- ["Prova la connessione per l'endpoint dei servizi della piattaforma"](#)
- ["Modifica endpoint dei servizi della piattaforma"](#)

Configurare la replica di CloudMirror

Per abilitare la replica di CloudMirror per un bucket, è necessario creare e applicare un XML di configurazione della replica del bucket valido.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo account tenant da un amministratore StorageGRID .
- Hai già creato un bucket che fungerà da origine di replicazione.
- L'endpoint che intendi utilizzare come destinazione per la replica CloudMirror esiste già e disponi del suo URN.
- Appartieni a un gruppo di utenti che ha il ["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#) . Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket quando si configura il bucket tramite Tenant Manager.

Informazioni su questo compito

La replica di CloudMirror copia gli oggetti da un bucket di origine a un bucket di destinazione specificato in un endpoint.

Per informazioni generali sulla replicazione dei 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"](#) .



La replica di CloudMirror presenta importanti somiglianze e differenze con la funzionalità di replica tra griglie. Per saperne di più, vedere ["Confronta la replicazione cross-grid e la replicazione CloudMirror"](#) .

Quando si configura la replica di CloudMirror, tenere presente i seguenti requisiti e caratteristiche:

- Quando si crea e si applica un XML di configurazione della replica del bucket valido, è necessario utilizzare l'URN di un endpoint del bucket S3 per ogni destinazione.
- La replica non è supportata per i bucket di origine o di destinazione con S3 Object Lock abilitato.
- Se si abilita 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. Per attivare la replica è necessario aggiornare gli oggetti esistenti.

- Se si specifica una classe di archiviazione nel file XML di configurazione della replica, StorageGRID utilizza tale classe quando esegue operazioni sull'endpoint S3 di destinazione. Anche l'endpoint di destinazione deve supportare la classe di archiviazione specificata. Assicuratevi di seguire tutte le raccomandazioni fornite dal fornitore del sistema di destinazione.

Passi

1. Abilita la replica per il tuo bucket di origine:

- Utilizzare un editor di testo per creare il file XML di configurazione della replicazione necessario per abilitare la replicazione, come specificato nell'API di replicazione S3.
- Durante la configurazione dell'XML:
 - Si noti che StorageGRID supporta solo la versione 1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'uso di `Filter` elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per maggiori dettagli, consultare la documentazione di Amazon sulla configurazione della replica.
 - Utilizzare l'URN di un endpoint del bucket S3 come destinazione.
 - Aggiungere facoltativamente il `<StorageClass>` elemento e specificare una delle seguenti opzioni:
 - `STANDARD`: La classe di archiviazione predefinita. Se non si specifica una classe di archiviazione quando si carica un oggetto, `STANDARD` viene utilizzata la classe di archiviazione.
 - `STANDARD_IA`: (Standard - accesso poco frequente.) Utilizzare questa classe di archiviazione per i dati a cui si accede meno frequentemente, ma che richiedono comunque un accesso rapido quando necessario.
 - `REDUCED_REDUNDANCY`: Utilizzare questa classe di archiviazione per dati non critici e riproducibili che possono essere archiviati con una ridondanza inferiore rispetto a `STANDARD` classe di archiviazione.
 - Se si specifica un `Role` nella configurazione XML verrà ignorato. Questo valore non è 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 **ARCHIVIAZIONE (S3) > Bucket**.
3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Servizi di piattaforma > Replica**.
5. Selezionare la casella di controllo **Abilita replica**.
6. Incollare il file XML di configurazione della replica nella casella di testo e selezionare **Salva modifiche**.



I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID tramite Grid Manager o Grid Management API. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore 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 mostrato 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 replicazione avviene rapidamente.

Informazioni correlate

["Crea endpoint dei servizi della piattaforma"](#)

Configurare le notifiche degli eventi

È possibile abilitare le notifiche per un bucket creando un XML di configurazione delle notifiche e utilizzando Tenant Manager per applicare l'XML a un bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo account tenant da un amministratore StorageGRID.
- Hai già creato un bucket che fungerà da fonte di notifiche.
- L'endpoint che intendi utilizzare come destinazione per le notifiche degli eventi esiste già e disponi del relativo URN.
- Appartieni a un gruppo di utenti che ha il ["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#). Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket quando si configura il bucket tramite Tenant Manager.

Informazioni su questo compito

È possibile configurare le notifiche degli eventi associando l'XML di configurazione delle notifiche a un bucket di origine. Il codice XML di configurazione delle notifiche segue le convenzioni S3 per la configurazione delle notifiche dei bucket, con l'argomento di destinazione Kafka o Amazon SNS specificato come URN di un endpoint.

Per informazioni generali sulle notifiche degli eventi e su come configurarle, fare riferimento a ["Documentazione Amazon"](#). Per informazioni su come StorageGRID implementa l'API di configurazione delle notifiche del bucket S3, fare riferimento a ["Istruzioni per l'implementazione di applicazioni client S3"](#).

Quando si configurano le notifiche degli eventi per un bucket, tenere presente i seguenti requisiti e

caratteristiche:

- Quando si crea e si applica un XML di configurazione delle notifiche valido, è necessario utilizzare l'URN di un endpoint delle notifiche degli eventi per ciascuna destinazione.
- Sebbene la notifica degli eventi possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Conserva fino alla data e Conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.
- 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.
- 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 delle notifiche.

Passi

1. Abilita le notifiche per il tuo bucket di origine:

- Utilizzare un editor di testo per creare il file XML di configurazione delle notifiche necessario per abilitare le notifiche degli eventi, come specificato nell'API di notifica S3.
- Durante la configurazione dell'XML, utilizzare l'URN di un endpoint di notifiche 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, seleziona **ARCHIVIAZIONE (S3) > Bucket**.

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Servizi piattaforma > Notifiche eventi**.

5. Seleziona la casella di controllo **Abilita notifiche eventi**.

6. Incolla il file XML di configurazione delle notifiche nella casella di testo e seleziona **Salva modifiche**.



I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID tramite Grid Manager o Grid Management API. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore 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 nell'XML di configurazione.

Nell'esempio, una notifica di evento viene inviata ogni volta che un oggetto viene creato con `images/` prefisso.

- b. Conferma che una notifica è stata recapitata all'argomento Amazon SNS o Kafka di destinazione.

Ad esempio, se l'argomento di destinazione è ospitato su Amazon SNS, puoi configurare il servizio in modo che ti venga inviata un'e-mail quando la notifica viene recapitata.

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "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"](#)

Configurare il servizio di integrazione della ricerca

È possibile abilitare l'integrazione della ricerca per un bucket creando un XML di integrazione della ricerca e utilizzando Tenant Manager per applicare l'XML al bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo account tenant da un amministratore StorageGRID .
- Hai già creato un bucket S3 di cui desideri indicizzare il contenuto.
- L'endpoint che intendi utilizzare come destinazione per il servizio di integrazione della ricerca esiste già e disponi del suo URN.
- Appartieni a un gruppo di utenti che ha il "[Gestisci tutti i bucket o l'autorizzazione di accesso Root](#)". Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket quando si configura il bucket tramite Tenant Manager.

Informazioni su questo compito

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 si abilita il servizio di integrazione della ricerca per un bucket che contiene già oggetti, le notifiche sui metadati non vengono inviate automaticamente per gli oggetti esistenti. Aggiornare questi oggetti esistenti per garantire che i loro metadati vengano aggiunti all'indice di ricerca di destinazione.

Passi

1. Abilita l'integrazione della ricerca per un bucket:

- Utilizzare un editor di testo per creare il file XML di notifica dei metadati necessario per abilitare l'integrazione della ricerca.
- Durante la configurazione dell'XML, utilizzare l'URN di un endpoint di integrazione della ricerca come destinazione.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, potresti inviare metadati per oggetti con il prefisso `images` verso una destinazione e metadati per oggetti con il prefisso `videos` all'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 è consentito.

Se necessario, fare riferimento a [esempi per la configurazione dei metadati XML](#) .


```

<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Elementi nel file XML di configurazione della notifica dei metadati:

Nome	Descrizione	Necessario
MetadatiNotificaCo nfigurazione	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione delle notifiche dei metadati. Contiene uno o più elementi Rule.	Sì
Regola	Tag contenitore 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 per la regola. Incluso nell'elemento Regola.	NO
Stato	Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilite. Incluso nell'elemento Regola.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata. Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Regola.	Sì
Destinazione	Tag contenitore per la destinazione di una regola. Incluso nell'elemento Regola.	Sì

Nome	Descrizione	Necessario
Urna	URN della destinazione a 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 archiviati i metadati, nel formato <code>domain-name/myindex/mytype</code>. Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma: • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404. L'URN è incluso nell'elemento Destinazione.	Sì

2. In Tenant Manager seleziona **ARCHIVIAZIONE (S3) > Bucket**.

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Seleziona **Servizi della piattaforma > Integrazione di ricerca**

5. Seleziona la casella di controllo **Abilita integrazione ricerca**.

6. Incolla la configurazione della notifica dei metadati nella casella di testo e seleziona **Salva modifiche**.



I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID tramite Grid Manager o Management API. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore StorageGRID.

7. Verificare che il servizio di integrazione della ricerca sia configurato correttamente:

- Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per l'attivazione di una notifica di metadati come specificato nel file XML di configurazione.

Nell'esempio mostrato in precedenza, tutti gli oggetti aggiunti al bucket attivano una notifica sui metadati.

- Verificare che un documento JSON contenente i metadati e i tag dell'oggetto sia stato aggiunto all'indice di ricerca specificato nell'endpoint.

Dopo aver finito

Se necessario, puoi disattivare l'integrazione della ricerca per un bucket utilizzando uno dei seguenti metodi:

- Selezionare **ARCHIVIAZIONE (S3) > Bucket** e deselezionare la casella di controllo **Abilita integrazione ricerca**.
- Se si utilizza direttamente l'API S3, utilizzare una richiesta di notifica dei metadati DELETE Bucket. Consultare le istruzioni per l'implementazione delle applicazioni client S3.

Esempio: configurazione della notifica dei metadati che si applica a tutti gli oggetti

In questo esempio, i metadati di 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>
```

Esempio: configurazione della notifica dei metadati con due regole

In questo esempio, metadati degli oggetti per gli oggetti che corrispondono al prefisso `/images` viene inviato a una destinazione, mentre i metadati degli oggetti 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-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Formato di notifica dei metadati

Quando si abilita il servizio di integrazione della ricerca per un bucket, ogni volta che vengono aggiunti, aggiornati o eliminati metadati o tag di un oggetto, viene generato un documento JSON che viene inviato all'endpoint di destinazione.

Questo esempio mostra un esempio del JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. Il `test` il bucket non è sottoposto a `versioning`, quindi `versionId` il tag è vuoto.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Campi inclusi nel documento JSON

Il nome del documento include il nome del bucket, il nome dell'oggetto e l'ID della versione, se presente.

Informazioni su bucket e oggetti

bucket: Nome del bucket

key: Nome chiave dell'oggetto

versionID: Versione dell'oggetto, per gli oggetti nei bucket con versione

region: Regione del bucket, ad esempio us-east-1

Metadati di sistema

size: Dimensione dell'oggetto (in byte) visibile a un client HTTP

md5: Hash dell'oggetto

Metadati utente

metadata: Tutti i metadati utente per l'oggetto, come coppie chiave-valore

key:value

Etichette

tags: Tutti i tag oggetto definiti per l'oggetto, come coppie chiave-valore

key:value

Come visualizzare i risultati in Elasticsearch

Per i tag e i metadati utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo che interpreti queste stringhe come date o

numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per la mappatura dei formati di data. Abilitare i mapping dei campi dinamici sull'indice prima di configurare il servizio di integrazione della ricerca. Dopo aver 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 Simple Storage Service (S3), implementata come un 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 l'archiviazione di oggetti on-premise che utilizza il sistema StorageGRID . Sono necessarie modifiche minime all'uso attuale delle chiamate API REST S3 da parte di un'applicazione client.

Versioni supportate

StorageGRID supporta le seguenti versioni specifiche di S3 e HTTP.

Articolo	Versione
Specifiche API S3	"Documentazione di Amazon Web Services (AWS): Riferimento API di 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 il pipelining HTTP/1.1.

Aggiornamenti al supporto dell'API REST S3

Pubblicazione	Commenti
11,9	• Aggiunto supporto per valori di checksum SHA-256 precalcolati per le seguenti richieste e intestazioni supportate. Puoi utilizzare questa funzionalità per verificare l'integrità degli oggetti caricati: ◦ Caricamento multiparte completo: <code>x-amz-checksum-sha256</code> ◦ CreaCaricamentoMultiparte: <code>x-amz-checksum-algorithm</code> ◦ OttieniOggetto: <code>x-amz-checksum-mode</code> ◦ OggettoTesta: <code>x-amz-checksum-mode</code> ◦ ElencoParti ◦ MettiOggetto: <code>x-amz-checksum-sha256</code> ◦ CaricaParte: <code>x-amz-checksum-sha256</code> • Aggiunta la possibilità per l'amministratore della griglia di controllare le impostazioni di conservazione e conformità a livello di tenant. Queste impostazioni influiscono sulle impostazioni di Blocco oggetti S3. ◦ Modalità di conservazione predefinita del bucket e modalità di conservazione degli oggetti: Governance o Conformità, se consentito dall'amministratore della griglia. ◦ Periodo di conservazione predefinito del bucket e data di conservazione dell'oggetto: deve essere inferiore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia. • Supporto migliorato per <code>aws-chunked</code> codifica e streaming dei contenuti <code>x-amz-content-sha256</code> valori. Limitazioni: ◦ Se presente, <code>chunk-signature</code> è facoltativo e non convalidato ◦ Se presente, <code>x-amz-trailer</code> il contenuto viene ignorato
11,8	Aggiornati i nomi delle operazioni S3 per abbinarli ai nomi utilizzati in "Documentazione di Amazon Web Services (AWS): Riferimento API di Amazon Simple Storage Service" .
11,7	• Aggiunto "Riferimento rapido: richieste API S3 supportate" . • Aggiunto supporto per l'utilizzo della modalità GOVERNANCE con S3 Object Lock. • Aggiunto supporto per StorageGRID specifico <code>x-ntap-sg-cgr-replication-status</code> intestazione di risposta per le richieste GET Object e HEAD Object. Questa intestazione fornisce lo stato di replicazione di un oggetto per la replica tra griglie. • Le richieste SelectObjectContent ora supportano gli oggetti Parquet.

Pubblicazione	Commenti
11,6	• Aggiunto supporto per l'utilizzo di <code>partNumber</code> parametro di richiesta nelle richieste GET Object e HEAD Object. • Aggiunto il supporto per una modalità di conservazione predefinita e un periodo di conservazione predefinito a livello di bucket per S3 Object Lock. • Aggiunto supporto per il <code>s3:object-lock-remaining-retention-days</code> chiave di condizione della policy per impostare l'intervallo di periodi di conservazione consentiti per i tuoi oggetti. • Modificata la dimensione massima <i>consigliata</i> per una singola operazione PUT Object a 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa invece il caricamento multiparte.
11,5	• Aggiunto supporto per la gestione della crittografia dei bucket. • Aggiunto supporto per S3 Object Lock e richieste di conformità legacy deprecated. • Aggiunto supporto per l'utilizzo di DELETE Multiple Objects su bucket con versione. • IL <code>Content-MD5</code> l'intestazione della richiesta è ora supportata correttamente.
11,4	• Aggiunto supporto per il tagging DELETE Bucket, GET Bucket e PUT 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 in termini di prestazioni. • Aggiunto supporto per le notifiche bucket su <code>s3:ObjectRestore:Post</code> tipo di evento. • Sono ora applicati i limiti dimensionali AWS per le parti multiparte. Ogni parte di un caricamento multiparte deve avere una dimensione 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 degli oggetti con chiavi fornite dal cliente (SSE-C). • Aggiunto supporto per le operazioni del ciclo di vita del bucket DELETE, GET e PUT (solo azione di scadenza) e per <code>x-amz-expiration</code> intestazione di risposta. • Aggiornati PUT Object, PUT Object - Copia e Caricamento multiparte per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono durante l'acquisizione. • I cifrari TLS 1.1 non sono più supportati.
11,2	Aggiunto supporto per il ripristino di oggetti POST per l'uso con Cloud Storage Pool. Aggiunto supporto per l'utilizzo della sintassi AWS per ARN, chiavi di condizione della policy e variabili della policy nelle policy di gruppo e bucket. Continueranno a essere supportati i criteri di gruppo e bucket esistenti che utilizzano la sintassi StorageGRID . Nota: gli utilizzi di ARN/URN in altre configurazioni JSON/XML, compresi quelli utilizzati nelle funzionalità StorageGRID personalizzate, non sono cambiati.

Pubblicazione	Commenti
11,1	Aggiunto supporto per la condivisione delle risorse tra origini (CORS), HTTP per le connessioni client S3 ai nodi della griglia e impostazioni di conformità sui bucket.
11,0	Aggiunto supporto per la configurazione dei servizi della piattaforma (replica CloudMirror, notifiche e integrazione della ricerca Elasticsearch) per i bucket. È stato inoltre aggiunto il supporto per i vincoli di posizione del tagging degli oggetti per i bucket e la coerenza disponibile.
10,4	Aggiunto supporto per le modifiche alla scansione ILM relative al controllo delle versioni, aggiornamenti della pagina Nomi di dominio endpoint, condizioni e variabili nelle policy, esempi di policy e autorizzazione PutOverwriteObject.
10,3	Aggiunto supporto per il controllo delle versioni.
10,2	Aggiunto supporto per criteri di accesso a gruppi e bucket e per la copia multiparte (Carica parte - Copia).
10,1	Aggiunto supporto per caricamento multiparte, richieste in stile virtual hosted e autenticazione v4.
10,0	Supporto iniziale dell'API REST S3 da parte del sistema StorageGRID. La versione attualmente supportata del <i>Simple Storage Service API Reference</i> è 2006-03-01.

Riferimento rapido: richieste API S3 supportate

Questa pagina riassume 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 per ciascuna operazione, selezionare il collegamento nell'intestazione.

Parametri di query URI comuni e intestazioni di richiesta

Se non diversamente specificato, sono supportati i seguenti parametri di query URI comuni:

- `versionId`(come richiesto per le operazioni sugli oggetti)

Se non diversamente 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 di implementazione dell'API REST S3"](#)
- ["Riferimento API di Amazon Simple Storage Service: intestazioni di richiesta comuni"](#)

"Annulla caricamento multiparte"

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"](#)

"Caricamento multiparte completo"

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
- x-amz-checksum-sha256

Tag XML del corpo della richiesta

StorageGRID supporta i seguenti tag XML del corpo della richiesta:

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

Documentazione StorageGRID

["Caricamento multiparte completo"](#)

"CopiaOggetto"

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

"CopiaOggetto"

"CreaBucket"

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"](#)

"CreaCaricamentoMultiparte"

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-checksum-algorithm
- 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

["CreaCaricamentoMultiparte"](#)

"EliminaBucket"

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"](#)
- ["Crea 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"](#)

"EliminaOggetto"

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"](#)

"EliminaOggetti"

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"](#)

"OttieniBucketAcl"

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"](#)

"Ottieni crittografia dei bucket"

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"](#)
- ["Crea la configurazione del ciclo di vita S3"](#)

"OttieniPosizioneBucket"

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"](#)

"Configurazione di notifica di GetBucket"

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"](#)

"OttieniPoliticaBucket"

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"](#)

"OttieniReplicazioneBucket"

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"](#)

"OttieniBucketTagging"

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"

"OttieniOggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più questi parametri di query URI aggiuntivi:

- x-amz-checksum-mode
- 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

"OttieniOggetto"

"OttieniOggettoAcl"

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"](#)

"OttieniOggettoLegaleHold"

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 S3 Object Lock"](#)

"Ottieni configurazione blocco oggetto"

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 S3 Object Lock"](#)

"Ottieni conservazione oggetto"

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 S3 Object Lock"](#)

"OttieniTaggingOggetto"

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"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più queste intestazioni aggiuntive:

- x-amz-checksum-mode
- 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"](#)

"ListBuckets"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Caricamenti multiparte di List"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più questi parametri aggiuntivi:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Caricamenti multiparte di List"](#)

"ElencoOggetti"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più questi 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, più questi 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, più questi parametri aggiuntivi:

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"ElencoParti"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più questi parametri aggiuntivi:

- max-parts
- part-number-marker
- uploadId

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Caricamenti multiparte di List"](#)

"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 i seguenti tag XML del corpo della richiesta:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"Configurazione del ciclo di vita di PutBucket"

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 i seguenti 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"](#)
- ["Crea la configurazione del ciclo di vita S3"](#)

"Configurazione della notifica PutBucket"

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 i seguenti 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 i dettagli sui campi del corpo JSON supportati, vedere ["Utilizzare criteri 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 i seguenti parametri del corpo della richiesta:

- VersioningConfiguration
- Status

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"MettiOggetto"

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-checksum-sha256
- 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

["MettiOggetto"](#)

"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 S3 Object Lock"](#)

"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 S3 Object Lock"](#)

"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 S3 Object Lock"](#)

"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"](#)

"Ripristina oggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Per i dettagli sui campi del corpo supportati, vedere ["Ripristina oggetto"](#).

"SelezionaOggettoContenuto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Per maggiori dettagli sui campi del corpo supportati, vedere quanto segue:

- ["Utilizzare S3 Select"](#)
- ["SelezionaOggettoContenuto"](#)

"CaricaParte"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più questi parametri di query URI aggiuntivi:

- partNumber
- uploadId

E queste intestazioni di richiesta aggiuntive:

- x-amz-checksum-sha256
- 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

"CaricaParte"

"CaricaParteCopia"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più questi 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

["CaricaParteCopia"](#)

Testare la configurazione dell'API REST S3

È possibile utilizzare l'interfaccia a riga di comando di Amazon Web Services (AWS CLI) per testare la connessione al sistema e verificare di poter leggere e scrivere oggetti.

Prima di iniziare

- Hai scaricato e installato AWS CLI da ["aws.amazon.com/cli"](https://aws.amazon.com/cli) .
- Facoltativamente, hai ["creato un endpoint del bilanciatore del carico"](#) . In caso contrario, è necessario conoscere 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"](#) .
- Hai ["creato un account tenant S3"](#) .
- Hai effettuato l'accesso al tenant e ["ha creato una chiave di accesso"](#) .

Per i dettagli su questi passaggi, vedere ["Configurare le connessioni client"](#) .

Passi

1. Configura le impostazioni AWS CLI per utilizzare l'account creato nel sistema StorageGRID :
 - a. Entra nella modalità di configurazione: `aws configure`
 - b. Inserisci l'ID della chiave di accesso per l'account che hai creato.
 - c. Inserisci la chiave di accesso segreta per l'account che hai creato.
 - d. Inserisci 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. Crea un bucket.

In questo esempio si presuppone che sia stato configurato un endpoint del bilanciatore 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. Carica 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, ovvero un hash dei dati dell'oggetto.

4. Elenca il contenuto 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. Elimina l'oggetto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-object --bucket testbucket --key s3.pdf
```

6. Elimina 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 dei clienti in conflitto

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins".

La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Valori di coerenza

La coerenza fornisce un equilibrio tra la disponibilità degli oggetti e la coerenza di tali oggetti tra diversi nodi di archiviazione e siti. È possibile modificare la coerenza in base alle esigenze dell'applicazione.

Per impostazione predefinita, StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi GET successivo a un PUT completato con successo sarà in grado di leggere i dati

appena scritti. Le sovrascritture di oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni alla fine risultano coerenti. In genere, la propagazione delle sovrascritture richiede secondi o minuti, ma può richiedere fino a 15 giorni.

Se si desidera eseguire operazioni sugli oggetti con una consistenza diversa, è possibile:

- Specificare una coerenza per **ogni secchio** .
- Specificare una coerenza per **ogni operazione API** .
- Modificare la coerenza predefinita dell'intera griglia eseguendo una delle seguenti attività:
 - In Grid Manager, vai su **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, consultare il registro di controllo situato in `/var/local/log` (cerca **consistencyLevel**).

Valori di coerenza

La coerenza influisce sul modo in cui i metadati utilizzati da StorageGRID per tracciare gli 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:

- **Tutti**: tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
- **Strong-global**: garantisce la coerenza di lettura e scrittura per tutte le richieste dei client su tutti i siti.
- **Strong-site**: garantisce la coerenza di lettura e scrittura per tutte le richieste client all'interno di un sito.
- **Lettura dopo nuova scrittura**: (predefinito) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
- **Disponibile**: fornisce 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 letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool .

Utilizzare la coerenza "Lettura dopo nuova scrittura" e "Disponibile"

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 fallisce, la ripete al valore di coerenza successivo finché non raggiunge una coerenza equivalente al comportamento di strong-global.

Se un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write" ma l'oggetto non esiste, la ricerca dell'oggetto raggiungerà sempre una coerenza equivalente al comportamento per strong-global. Poiché questa coerenza richiede che siano disponibili più copie dei metadati dell'oggetto in ogni sito, è possibile ricevere un numero elevato di errori 500 Internal Server se due o più nodi di archiviazione nello stesso sito non sono disponibili.

A meno che non siano necessarie garanzie di coerenza simili ad Amazon S3, è possibile prevenire questi errori per le operazioni HEAD e GET impostando la coerenza su "Disponibile". Quando un'operazione HEAD o GET utilizza la coerenza "Disponibile", StorageGRID fornisce solo la coerenza finale. Non riprova un'operazione non riuscita aumentando la coerenza, quindi non richiede che siano disponibili più copie dei metadati dell'oggetto.

Specifica 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. In questo esempio la coerenza viene impostata 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.

Specifica la coerenza per il bucket

Per impostare la coerenza per il bucket, puoi utilizzare StorageGRID ["PUT Consistenza del secchio"](#) richiesta. Oppure puoi ["modificare la consistenza di un bucket"](#) dal gestore dell'affitto.

Quando si imposta la consistenza di un bucket, tenere presente quanto segue:

- L'impostazione della coerenza per un bucket determina quale coerenza viene utilizzata per le operazioni S3 eseguite sugli oggetti nel bucket o sulla configurazione del bucket. Non influisce sulle operazioni sul bucket stesso.
- La coerenza di una singola operazione API prevale sulla coerenza del bucket.
- In generale, i bucket dovrebbero utilizzare la coerenza predefinita, "Lettura dopo nuova scrittura". Se le richieste non funzionano correttamente, modificare, se possibile, il comportamento del client dell'applicazione. Oppure, configura il client in modo che specifichi la coerenza per ogni richiesta API. Impostare la coerenza a livello di bucket solo come ultima risorsa.

Come interagiscono la coerenza e le regole ILM per influenzare la protezione dei dati

Sia la scelta della coerenza sia la regola ILM influiscono sul modo in cui gli oggetti vengono protetti. Queste impostazioni possono interagire.

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

Il seguente ["opzioni di ingestione"](#) sono disponibili per le regole ILM:

Doppio impegno

StorageGRID crea immediatamente copie provvisorie dell'oggetto e restituisce l'esito positivo al client. Quando possibile, vengono effettuate le copie specificate nella norma ILM.

Rigoroso

Tutte le copie specificate nella regola ILM devono essere effettuate prima che il successo venga restituito al cliente.

Equilibrato

StorageGRID tenta di effettuare tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono effettuate copie provvisorie e il client riceve un messaggio di conferma dell'operazione riuscita. Quando possibile, vengono effettuate le copie specificate nella norma ILM.

Esempio di come la coerenza e la regola ILM possono interagire

Supponiamo di avere una griglia a due siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM:** creare due copie dell'oggetto, una nel sito locale e una in un sito remoto. Utilizzare un comportamento di acquisizione rigoroso.
- **coerenza:** Strong-global (i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie dell'oggetto e distribuisce i metadati a entrambi i siti prima di restituire l'esito positivo al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione corretta del messaggio. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, copie sia dei dati dell'oggetto sia dei metadati dell'oggetto sono ancora presenti nel sito remoto. L'oggetto è completamente recuperabile.

Se invece si utilizzasse la stessa regola ILM e la coerenza del sito forte, il client potrebbe ricevere un messaggio di successo dopo che i dati dell'oggetto sono stati replicati sul sito remoto, ma prima che i metadati dell'oggetto vengano distribuiti lì. 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 subito dopo l'acquisizione, anche i metadati dell'oggetto vengono persi. L'oggetto non può essere recuperato.

L'interrelazione tra coerenza e regole ILM può essere complessa. Se hai bisogno di assistenza, contatta NetApp .

Versionamento degli oggetti

È possibile impostare lo stato di controllo delle versioni di un bucket se si desidera conservare più versioni di ciascun oggetto. Abilitare il controllo delle versioni per un bucket può contribuire a proteggere gli oggetti dall'eliminazione accidentale e consente di recuperare e ripristinare le versioni precedenti di un oggetto.

Il sistema StorageGRID implementa il controllo delle versioni con supporto per la maggior parte delle funzionalità e con alcune limitazioni. StorageGRID supporta fino a 10.000 versioni di ciascun oggetto.

Il controllo delle versioni degli oggetti può essere combinato con la gestione del ciclo di vita delle informazioni (ILM) StorageGRID o con la configurazione del ciclo di vita del bucket S3. È necessario abilitare esplicitamente il controllo delle versioni per ogni bucket. Quando il controllo delle versioni è abilitato per un bucket, a ogni oggetto aggiunto al bucket viene assegnato un ID versione, generato dal sistema StorageGRID .

L'eliminazione tramite MFA (autenticazione a più fattori) non è supportata.



Il controllo delle versioni può essere abilitato solo sui bucket creati con StorageGRID versione 10.3 o successiva.

ILM e controllo delle versioni

Le policy ILM vengono applicate a ciascuna versione di un oggetto. Un processo di scansione ILM analizza continuamente tutti gli oggetti e li rivaluta in base alla politica ILM corrente. Tutte le modifiche apportate ai criteri ILM vengono applicate a tutti gli oggetti precedentemente acquisiti. Sono incluse le versioni precedentemente acquisite se è abilitato il controllo delle versioni. La scansione ILM applica le nuove modifiche ILM agli oggetti precedentemente acquisiti.

Per gli oggetti S3 nei bucket abilitati per il controllo delle versioni, il supporto del controllo delle versioni consente di creare regole ILM che utilizzano "Ora non corrente" come ora di riferimento (selezionare **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti?" in ["Passaggio 1 della procedura guidata Crea una regola ILM"](#)). Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. Utilizzando un filtro "Tempo non corrente" è possibile creare criteri che riducono l'impatto sull'archiviazione delle versioni precedenti degli oggetti.



Quando si carica una nuova versione di un oggetto utilizzando un'operazione di caricamento multiparte, il tempo non corrente per la versione originale dell'oggetto riflette il momento in cui è stato creato il caricamento multiparte per la nuova versione, non il momento in cui è stato completato il caricamento multiparte. In casi limitati, l'orario non aggiornato della versione originale potrebbe essere precedente di ore o giorni rispetto all'orario della versione corrente.

Informazioni correlate

- ["Come vengono eliminati gli oggetti con versione S3"](#)
- ["Regole e policy ILM per oggetti con versione S3 \(esempio 4\)"](#) .

Utilizzare l'API REST S3 per configurare S3 Object Lock

Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID , è possibile creare bucket con S3 Object Lock abilitato. È possibile specificare la conservazione predefinita per ogni bucket o le impostazioni di conservazione per ogni versione dell'oggetto.

Come abilitare S3 Object Lock per un bucket

Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID , è possibile abilitare facoltativamente S3 Object Lock quando si crea ogni bucket.

S3 Object Lock è un'impostazione permanente che può essere abilitata solo quando si crea un bucket. Non è possibile aggiungere o disabilitare S3 Object Lock dopo aver creato un bucket.

Per abilitare S3 Object Lock per un bucket, utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando Tenant Manager. Vedere ["Crea bucket S3"](#) .
- Crea 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 delle versioni dei bucket, che viene abilitato automaticamente al momento della creazione del bucket. Non è possibile sospendere il controllo delle versioni per il bucket. Vedere ["Versionamento degli oggetti"](#) .

Impostazioni di conservazione predefinite per un bucket

Quando S3 Object Lock è abilitato per un bucket, è possibile abilitare facoltativamente 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 CONFORMITÀ:
 - L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione.
 - La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.
 - La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.
- In modalità GOVERNANCE:
 - Utenti con il `s3:BypassGovernanceRetention` il permesso può utilizzare il `x-amz-bypass-governance-retention: true` intestazione della richiesta per ignorare le impostazioni di conservazione.
 - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione.
 - Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.

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:

- Gestisci le impostazioni del bucket da Tenant Manager. Vedere ["Crea un bucket S3" E "Aggiorna la conservazione predefinita del blocco degli oggetti S3"](#) .
- Inviare una richiesta `PutObjectLockConfiguration` al 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 in cui è abilitato S3 Object Lock. È anche possibile rimuovere le impostazioni di conservazione predefinite configurate in precedenza.

Quando nuove versioni di 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 la data di conservazione fino a se `x-amz-object-lock-retain-until-date` non è specificato.

Se il periodo di conservazione predefinito viene modificato dopo l'acquisizione di una versione dell'oggetto, la data di conservazione fino alla versione dell'oggetto rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito.

Devi avere il `s3:PutBucketObjectLockConfiguration` autorizzazione, oppure essere l'account root, per completare questa operazione.

IL Content-MD5 l'intestazione della richiesta deve essere specificata nella richiesta PUT.

Richiedi esempio

Questo esempio abilita S3 Object Lock per un bucket e imposta la modalità di conservazione predefinita su CONFORMITÀ 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 abilitato per un bucket e per visualizzare la modalità di conservazione predefinita e il periodo di conservazione, utilizzare uno di questi metodi:

- Visualizza il bucket in Tenant Manager. Vedere ["Visualizza i bucket S3"](#).
- Inviare una richiesta GetObjectLockConfiguration.

Ottieni configurazione blocco oggetto

La richiesta GetObjectLockConfiguration consente di determinare se S3 Object Lock è abilitato per un bucket e, in tal caso, di verificare se sono configurati una modalità di conservazione predefinita e un periodo di conservazione per il bucket.

Quando nuove versioni di oggetti vengono acquisite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` non è specificato. Il periodo di conservazione predefinito viene utilizzato per calcolare la data di conservazione fino a se `x-amz-object-lock-retain-until-date` non è specificato.

Devi avere il `s3:GetBucketObjectLockConfiguration` autorizzazione, oppure essere l'account root, per completare questa operazione.

Richiedi esempio

```
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 impostazioni di conservazione S3 Object Lock.

Le impostazioni di conservazione a livello di oggetto vengono specificate tramite l'API REST S3. Le impostazioni di conservazione per un oggetto sostituiscono tutte le impostazioni di conservazione predefinite per il bucket.

Per ogni oggetto è possibile specificare le seguenti impostazioni:

- **Modalità di conservazione:** CONFORMITÀ o GOVERNANCE.
- **Retain-until-date:** data che specifica per quanto tempo la versione dell'oggetto deve essere conservata da

StorageGRID.

- In modalità CONFORMITÀ, se la data di conservazione è futura, l'oggetto può essere recuperato, ma non può essere modificato o eliminato. La data di conservazione può essere aumentata, ma questa data non può essere diminuita o rimossa.
- In modalità GOVERNANCE, gli utenti con autorizzazione speciale possono ignorare l'impostazione di conservazione fino alla data indicata. Possono eliminare una versione di un oggetto prima che scada il periodo di conservazione. Possono anche aumentare, diminuire o addirittura rimuovere la data di conservazione.
- **Sospensione legale:** l'applicazione di una sospensione legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potrebbe essere necessario applicare un blocco legale a un oggetto correlato a un'indagine o a una controversia legale. Una sospensione legale non ha una data di scadenza, ma rimane in vigore finché non viene rimossa esplicitamente.

L'impostazione di conservazione legale per un oggetto è indipendente dalla modalità di conservazione e dalla data di conservazione fino alla data di scadenza. Se una versione di un oggetto è sottoposta a blocco legale, nessuno può eliminarla.

Per specificare le impostazioni di blocco degli oggetti S3 quando si aggiunge una versione dell'oggetto a un bucket, emettere un **"MettiOggetto"**, **"CopiaOggetto"**, O **"CreaCaricamentoMultiparte"** richiesta.

Puoi usare quanto segue:

- `x-amz-object-lock-mode`, che può essere COMPLIANCE o GOVERNANCE (con distinzione tra maiuscole e minuscole).



Se specifichi `x-amz-object-lock-mode`, devi anche specificare `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
 - Il valore `retain-until-date` deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentite frazioni di secondo, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Altri formati ISO 8601 non sono consentiti.
 - La data di conservazione deve essere futura.
- `x-amz-object-lock-legal-hold`

Se la conservazione legale è ATTIVA (sensibile alle maiuscole e alle minuscole), l'oggetto viene sottoposto a conservazione legale. Se la conservazione legale è disattivata, non verrà applicata alcuna conservazione legale. 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-*` Se è presente l'intestazione della richiesta, viene restituito un errore 400 Bad Request (InvalidRequest).
- La richiesta `PutObject` supporta l'uso di `x-amz-storage-class: REDUCED_REDUNDANCY` per adattarsi al comportamento di AWS. Tuttavia, quando un oggetto viene inserito in un bucket con S3 Object Lock abilitato, StorageGRID eseguirà sempre un inserimento 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`, `x-amz-object-lock-legal-hold`, se configurato e se il mittente della richiesta ha il corretto `s3:Get*` permessi.

Puoi usare il `s3:object-lock-remaining-retention-days` chiave di condizione della policy per limitare i periodi di conservazione minimi e massimi consentiti per i tuoi oggetti.

Come aggiornare le impostazioni di conservazione per un oggetto

Se è necessario aggiornare le impostazioni di conservazione o di blocco legale per una versione esistente di un oggetto, è possibile eseguire le seguenti operazioni sulle sottorisorse dell'oggetto:

- `PutObjectLegalHold`

Se il nuovo valore di conservazione legale è impostato su ON, l'oggetto viene sottoposto a conservazione legale. Se il valore di sospensione legale è OFF, la sospensione legale viene revocata.

- `PutObjectRetention`
 - Il valore della modalità può essere COMPLIANCE o GOVERNANCE (con distinzione tra maiuscole e minuscole).
 - Il valore `retain-until-date` deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentite frazioni di secondo, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Altri formati ISO 8601 non sono consentiti.
 - Se una versione di un oggetto ha una data di conservazione (`retain-until-date`) esistente, è possibile solo aumentarla. Il nuovo valore deve essere nel futuro.

Come utilizzare la modalità GOVERNANCE

Gli utenti che hanno il `s3:BypassGovernanceRetention` l'autorizzazione può ignorare le impostazioni di conservazione attive di un oggetto che utilizza la modalità GOVERNANCE. Tutte le operazioni DELETE o `PutObjectRetention` devono includere `x-amz-bypass-governance-retention:true` intestazione della richiesta. Questi utenti possono eseguire le seguenti operazioni aggiuntive:

- Eseguire le operazioni `DeleteObject` o `DeleteObjects` per eliminare una versione dell'oggetto prima che scada il periodo di conservazione.

Gli oggetti sottoposti a conservazione legale non possono essere eliminati. La conservazione legale deve essere DISATTIVATA.

- Eseguire operazioni `PutObjectRetention` che modificano la modalità di una versione dell'oggetto da GOVERNANCE a COMPLIANCE prima che sia trascorso il periodo di conservazione dell'oggetto.

Non è mai consentito cambiare la modalità da COMPLIANCE a GOVERNANCE.

- Eseguire operazioni `PutObjectRetention` per aumentare, diminuire o rimuovere il periodo di conservazione di una versione dell'oggetto.

Informazioni correlate

- ["Gestisci gli oggetti con S3 Object Lock"](#)
- ["Utilizzare S3 Object Lock per conservare gli oggetti"](#)
- ["Guida per l'utente di Amazon Simple Storage Service: blocco degli oggetti"](#)

Crea la configurazione del ciclo di vita S3

È possibile creare una configurazione del ciclo di vita S3 per controllare quando oggetti specifici vengono eliminati dal sistema StorageGRID .

Il semplice esempio in questa sezione illustra come una configurazione del ciclo di vita S3 può controllare quando determinati oggetti vengono eliminati (scadono) da specifici bucket S3. L'esempio in questa sezione è solo a scopo illustrativo. Per i dettagli completi sulla creazione di configurazioni del ciclo di vita S3, vedere ["Guida per l'utente di Amazon Simple Storage Service: gestione del ciclo di vita degli oggetti"](#) . Si noti che StorageGRID supporta solo azioni di scadenza; non supporta azioni di transizione.

Qual è la configurazione del ciclo di vita?

Una configurazione del ciclo di vita è un insieme di regole applicate agli oggetti in bucket S3 specifici. Ogni regola specifica quali oggetti sono interessati e quando tali oggetti 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: elimina un oggetto quando viene raggiunta una data specificata o quando viene raggiunto un numero di giorni specificato, a partire dal momento in cui l'oggetto è stato acquisito.
- NoncurrentVersionExpiration: elimina un oggetto quando viene raggiunto un numero di giorni specificato, a partire dal momento in cui l'oggetto è diventato non corrente.
- Filtro (Prefisso, Tag)
- Stato
- ID

Ogni oggetto segue le impostazioni di conservazione del ciclo di vita di un bucket S3 o di una policy 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 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 del bucket e non vengono specificate esplicitamente azioni di scadenza, le impostazioni di conservazione del criterio ILM non vengono utilizzate e si implica che le versioni dell'oggetto vengano conservate per sempre. Vedere ["Esempio di priorità per il ciclo di vita del bucket S3 e la policy ILM"](#) .

Di conseguenza, un oggetto potrebbe essere rimosso dalla griglia anche se le istruzioni di posizionamento in una regola ILM sono ancora valide per l'oggetto. Oppure, un oggetto potrebbe essere mantenuto sulla griglia anche dopo che tutte le istruzioni di posizionamento ILM per l'oggetto sono scadute. Per maggiori dettagli, vedere ["Come funziona l'ILM durante la vita di un oggetto"](#) .



La configurazione del ciclo di vita del bucket può essere utilizzata con bucket in cui è abilitato S3 Object Lock, ma la configurazione del ciclo di vita del bucket non è supportata per i bucket Compliant legacy.

StorageGRID supporta l'utilizzo delle seguenti operazioni bucket per gestire le configurazioni del ciclo di vita:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- Configurazione del ciclo di vita di PutBucket

Crea la configurazione del ciclo di vita

Come primo passaggio nella creazione di una configurazione del ciclo di vita, si crea un file JSON che include 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 che corrispondono al filtro scadranno a mezzanotte del 22 agosto 2020.
2. La regola 2 si applica solo agli oggetti che corrispondono al prefisso `category2` /. IL `Expiration` Il parametro specifica che gli oggetti che corrispondono al filtro scadranno 100 giorni dopo essere stati acquisiti.



Le regole che specificano un numero di giorni sono relative al momento in cui l'oggetto è stato ingerito. 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` Il parametro specifica che tutte le versioni non correnti degli oggetti corrispondenti scadranno 50 giorni dopo essere diventate non correnti.


```

{
  "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, puoi 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 convalidare che una configurazione del ciclo di vita sia stata applicata correttamente al bucket, inviare una richiesta `GetBucketLifecycleConfiguration`. Per esempio:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Una risposta positiva elenca la configurazione del ciclo di vita appena applicata.

Convalida 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 scade l'oggetto e quale regola di scadenza è stata rispettata.



Poiché il ciclo di vita del bucket sostituisce ILM, `expiry-date` viene mostrata la data effettiva in cui l'oggetto verrà eliminato. Per maggiori dettagli, vedere ["Come viene determinata la ritenzione dell'oggetto"](#).

Ad esempio, questa richiesta `PutObject` è stata emessa il 22 giugno 2020 e inserisce un oggetto nel `testbucket` `secchio`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La risposta di successo 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 soddisfa la 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 al controllo delle versioni, `x-amz-expiration` l'intestazione di risposta si applica solo alle versioni correnti degli oggetti.

Raccomandazioni per l'implementazione dell'API REST S3

Quando si implementa l'API REST S3 per l'uso con StorageGRID, è necessario seguire queste raccomandazioni.

Raccomandazioni per HEAD su oggetti inesistenti

Se la tua applicazione controlla regolarmente se un oggetto esiste in un percorso in cui non ti aspetti che l'oggetto esista effettivamente, dovresti usare "Disponibile"["coerenza"](#). Ad esempio, dovresti usare la coerenza "Disponibile" se la tua applicazione esegue l'HEAD di una posizione prima di eseguirvi un PUT.

In caso contrario, se l'operazione HEAD non trova l'oggetto, è possibile che venga visualizzato un numero elevato di errori 500 Internal Server se due o più nodi di archiviazione nello stesso sito non sono disponibili o un sito remoto non è raggiungibile.

È possibile impostare la coerenza "Disponibile" per ogni bucket utilizzando ["PUT Consistenza del secchio"](#) richiesta oppure è possibile specificare la coerenza nell'intestazione della richiesta per una singola operazione

API.

Raccomandazioni per le chiavi degli oggetti

Seguire questi consigli per i nomi delle chiavi degli oggetti, in base al momento in cui il bucket è stato creato per la prima volta.

Bucket creati in StorageGRID 11.4 o versioni precedenti

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi degli oggetti. Ciò è in contrasto con la precedente raccomandazione di AWS per i prefissi delle chiavi. Utilizzare invece prefissi non casuali e non univoci, come ad esempio `image`.
- Se si segue la precedente raccomandazione di AWS di utilizzare caratteri casuali e univoci nei prefissi delle chiavi, aggiungere un nome di directory come prefisso alle chiavi degli oggetti. Cioè, usa 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 migliori pratiche in termini di prestazioni. Nella maggior parte dei casi, è possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi degli oggetti.



Un'eccezione è il carico di lavoro S3 che rimuove continuamente tutti gli oggetti dopo un breve periodo di tempo. Per ridurre al minimo l'impatto sulle prestazioni in questo caso d'uso, modificare una parte iniziale del nome della chiave ogni diverse migliaia di oggetti con qualcosa come la data. Ad esempio, supponiamo che un client S3 scriva in genere 2.000 oggetti al secondo e che la policy ILM o del ciclo di vita del bucket rimuova tutti gli oggetti dopo tre giorni. Per ridurre al minimo l'impatto sulle prestazioni, potresti denominare le chiavi utilizzando uno schema come questo: `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Consigli per le "letture di intervallo"

Se il "[opzione globale per comprimere gli oggetti memorizzati](#)" è abilitato, le applicazioni client S3 dovrebbero evitare di eseguire operazioni `GetObject` che specificano un intervallo di byte da restituire. Queste operazioni di "lettura di intervallo" sono inefficienti perché StorageGRID deve effettivamente decomprimere gli oggetti per accedere ai byte richiesti. Le operazioni `GetObject` che richiedono un intervallo ridotto di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, non è efficiente 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 potrebbero scadere.



Se è necessario comprimere oggetti e l'applicazione client deve utilizzare letture di intervallo, aumentare il timeout di lettura per l'applicazione.

Supporto per l'API REST di Amazon S3

Dettagli di implementazione dell'API REST S3

Il sistema StorageGRID implementa l'API Simple Storage Service (versione API 2006-03-01) con supporto per la maggior parte delle operazioni e con alcune limitazioni. Quando si integrano applicazioni client S3 REST API, è necessario comprendere i dettagli di implementazione.

Il sistema StorageGRID supporta sia le richieste in stile host virtuale sia quelle in stile percorso.

Gestione delle date

L'implementazione StorageGRID dell'API REST S3 supporta solo formati di data HTTP validi.

Il sistema StorageGRID supporta solo formati di data HTTP validi per tutte le intestazioni che accettano valori di data. La parte oraria della data può essere specificata nel formato Greenwich Mean Time (GMT) o nel formato Universal Coordinated Time (UTC) senza differenza di fuso orario (è necessario specificare +0000). Se includi il `x-amz-date` nell'intestazione della richiesta, sovrascrive qualsiasi valore specificato nell'intestazione della richiesta Data. Quando si utilizza AWS Signature versione 4, `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 ["Riferimento API di Amazon Simple Storage Service: intestazioni di richiesta comuni"](#), con una eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	Supporto completo per AWS Signature versione 2 Supporto per AWS Signature versione 4, con le seguenti eccezioni: Quando si fornisce il valore effettivo del checksum del payload in <code>x-amz-content-sha256</code>, il valore viene accettato senza convalida, come se il valore <code>UNSIGNED-PAYLOAD</code> era stato fornito per l'intestazione. Quando fornisci un <code>x-amz-content-sha256</code> valore dell'intestazione che implica <code>aws-chunked streaming</code> (ad esempio, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), le firme dei blocchi non vengono verificate rispetto ai dati dei blocchi.
token di sicurezza x-amz	Non implementato. Resi <code>XNotImplemented</code> .

Intestazioni di risposta comuni

Il sistema StorageGRID supporta tutte le intestazioni di risposta comuni definite da *Simple Storage Service API Reference*, con un'eccezione.

Intestazione di risposta	Implementazione
<code>x-amz-id-2</code>	Non utilizzato

Autenticare le richieste

Il sistema StorageGRID supporta sia l'accesso autenticato che quello anonimo agli oggetti tramite l'API S3.

L'API S3 supporta la versione 2 e la versione 4 della firma 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 utilizzando parametri di query.

Utilizzare l'intestazione di autorizzazione HTTP

L'HTTP Authorization L'intestazione viene utilizzata da tutte le operazioni API S3, ad eccezione delle richieste anonime, ove consentito dalla policy del bucket. IL Authorization L'intestazione contiene tutte le informazioni di firma necessarie 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 e può essere utilizzata per concedere l'accesso temporaneo a risorse specifiche. Gli utenti con l'URL prefirmato non hanno bisogno di conoscere la chiave di accesso segreta per accedere alla risorsa, il che consente di fornire a terze parti un accesso limitato a una risorsa.

Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

Operazione	Implementazione
ListBuckets (precedentemente denominato Servizio GET)	Implementato con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
Utilizzo dello spazio di archiviazione GET	StorageGRID" Utilizzo dello spazio di archiviazione GET " La richiesta indica la quantità totale di spazio di archiviazione utilizzato da un account e per ogni bucket associato all'account. Questa è un'operazione sul servizio con un percorso di / e un parametro di query personalizzato(?x-ntap-sg-usage) aggiunto.
OPZIONI /	Le applicazioni client possono emettere OPTIONS / richieste alla porta S3 su un nodo di archiviazione, senza fornire credenziali di autenticazione S3, per determinare se il nodo di archiviazione è disponibile. È possibile utilizzare questa richiesta per il monitoraggio o per consentire ai bilanciatori di carico esterni di identificare quando un nodo di archiviazione è inattivo.

Operazioni sui bucket

Il sistema StorageGRID supporta un massimo di 5.000 bucket per ogni account tenant S3.

Ogni griglia può avere un massimo di 100.000 bucket.

Per supportare 5.000 bucket, ogni nodo di archiviazione nella griglia deve disporre di almeno 64 GB di RAM.

Le restrizioni sui nomi dei bucket seguono le restrizioni della regione AWS US Standard, ma è opportuno limitarle ulteriormente alle convenzioni di denominazione DNS per supportare le richieste in stile hosting virtuale S3.

Per maggiori informazioni vedere quanto segue:

- ["Guida per l'utente di Amazon Simple Storage Service: quote, 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 all'orario dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket. Vedere ["GET Ora dell'ultimo accesso al bucket"](#).

La tabella seguente descrive come StorageGRID implementa le operazioni del bucket S3 REST API. Per eseguire una qualsiasi di queste operazioni, è necessario fornire le credenziali di accesso necessarie per l'account.

Operazione	Implementazione
CreaBucket	Crea un nuovo bucket. Creando il bucket, ne diventi il proprietario. • I nomi dei bucket devono rispettare le seguenti regole: ◦ Deve essere univoco 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 contenere solo lettere minuscole, numeri e trattini. ◦ Non deve avere l'aspetto di un indirizzo IP formattato come testo. ◦ Non utilizzare punti nelle richieste in stile ospitato virtuale. I punti causeranno problemi con la verifica dei certificati jolly del server. • Per impostazione predefinita, i bucket vengono creati in <code>us-east-1</code> regione; tuttavia, è possibile utilizzare il <code>LocationConstraint</code> elemento di richiesta nel corpo della richiesta per specificare una regione diversa. Quando si utilizza il <code>LocationConstraint</code> elemento, è necessario specificare il nome esatto di una regione definita tramite Grid Manager o Grid Management API. Se non conosci il nome della regione da utilizzare, contatta l'amministratore di sistema. Nota: si verificherà un errore se la richiesta <code>CreateBucket</code> utilizza una regione non definita in StorageGRID. • Puoi includere il <code>x-amz-bucket-object-lock-enabled</code> intestazione della richiesta per creare un bucket con S3 Object Lock abilitato. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock". Quando si crea il bucket, è necessario abilitare S3 Object Lock. Non è possibile aggiungere o disabilitare S3 Object Lock dopo aver creato un bucket. S3 Object Lock richiede il controllo delle versioni dei bucket, che viene abilitato automaticamente quando si crea il bucket.
EliminaBucket	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 tutti i nuovi oggetti aggiunti al bucket non vengono crittografati.
DeleteBucketLifecycle	Elimina la configurazione del ciclo di vita dal bucket. Vedere "Crea la configurazione del ciclo di vita S3" .
DeleteBucketPolicy	Elimina la policy associata al bucket.

Operazione	Implementazione
DeleteBucketReplication	Elimina la configurazione di replica associata al bucket.
DeleteBucketTagging	Utilizza il <code>tagging</code> sottorisorsa per rimuovere tutti i tag da un bucket. Attenzione: se per questo bucket è impostato un tag di policy ILM non predefinito, si verificherà un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket a cui è assegnato un valore. Non inviare una richiesta <code>DeleteBucketTagging</code> se è presente un <code>NTAP-SG-ILM-BUCKET-TAG</code> etichetta del secchio. Invece, emetti una richiesta <code>PutBucketTagging</code> con solo <code>NTAP-SG-ILM-BUCKET-TAG</code> tag e il valore assegnato per rimuovere tutti gli altri tag dal bucket. Non modificare o rimuovere il <code>NTAP-SG-ILM-BUCKET-TAG</code> etichetta del secchio.
OttieniBucketAcl	Restituisce una risposta positiva e l'ID, il <code>DisplayName</code> e l'autorizzazione del proprietario del bucket, a indicare che il proprietario ha accesso completo al bucket.
GetBucketCors	Restituisce il <code>cors</code> configurazione per il bucket.
Ottieni crittografia del bucket	Restituisce la configurazione di crittografia predefinita per il bucket.
GetBucketLifecycleConfiguration (in precedenza denominato ciclo di vita del bucket GET)	Restituisce la configurazione del ciclo di vita per il bucket. Vedere "Crea la configurazione del ciclo di vita S3" .
OttieniPosizioneBucket	Restituisce la regione impostata utilizzando <code>LocationConstraint</code> elemento nella richiesta <code>CreateBucket</code> . Se la regione del bucket è <code>us-east-1</code> , viene restituita una stringa vuota per la regione.
Configurazione di notifica di GetBucket (in precedenza denominata notifica GET Bucket)	Restituisce la configurazione delle notifiche allegata al bucket.
OttieniPoliticaBucket	Restituisce la policy associata al bucket.
OttieniReplicazioneBucket	Restituisce la configurazione di replica associata al bucket.

Operazione	Implementazione
OttieniBucketTagging	Utilizza il <code>tagging</code> sottorisorsa per restituire tutti i tag per un bucket. Attenzione: se per questo bucket è impostato un tag di policy ILM non predefinito, si verificherà un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket a cui è assegnato un valore. Non modificare o rimuovere questo tag.
GetBucketVersioning	Questa implementazione utilizza il <code>versioning</code> sottorisorsa per restituire lo stato di controllo delle versioni di un bucket. • <i>blank</i>: il controllo delle versioni non è mai stato abilitato (il bucket è "Senza controllo delle versioni") • Abilitato: il controllo delle versioni è abilitato • Sospeso: il controllo delle versioni era precedentemente abilitato ed è sospeso
Ottieni configurazione blocco oggetto	Restituisce la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito, se configurati. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" .
HeadBucket	Determina se esiste un bucket e se si dispone dell'autorizzazione per accedervi. Questa operazione restituisce: • <code>x-ntap-sg-bucket-id</code>: L'UUID del bucket nel formato UUID. • <code>x-ntap-sg-trace-id</code>: ID traccia univoco della richiesta associata.
ListObjects e ListObjectsV2 (precedentemente denominato GET Bucket)	Restituisce alcuni o tutti (fino a 1.000) gli oggetti in un bucket. La classe di archiviazione per gli oggetti può avere uno dei due valori, anche se l'oggetto è stato ingerito con <code>REDUCED_REDUNDANCY</code> opzione classe di archiviazione: • <code>STANDARD</code>, che indica che l'oggetto è archiviato in un pool di archiviazione costituito da nodi di archiviazione. • <code>GLACIER</code>, 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 che hanno lo stesso prefisso, la risposta potrebbe includere alcune <code>CommonPrefixes</code> che non contengono chiavi.
ListObjectVersions (precedentemente denominate versioni GET Bucket Object)	Con accesso <code>READ</code> su un bucket, utilizzando questa operazione con <code>versions</code> 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 richieste multiorigine. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni web client in un dominio di accedere alle risorse in un dominio diverso. Ad esempio, supponiamo di utilizzare un bucket S3 denominato <code>images</code> per memorizzare la grafica. Impostando la configurazione CORS per <code>images</code> bucket, puoi consentire che le immagini in quel bucket vengano visualizzate sul sito web <code>http://www.example.com</code>.
PutBucketEncryption	Imposta lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è abilitata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati. StorageGRID supporta la crittografia lato server con chiavi gestite StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare <code>SSEAlgorithm</code> parametro a <code>AES256</code> e non usare il <code>KMSMasterKeyID</code> parametro. La configurazione di crittografia predefinita del bucket viene ignorata se la richiesta di caricamento dell'oggetto specifica già la crittografia (ovvero, se la richiesta include <code>x-amz-server-side-encryption-*</code> intestazione della richiesta).
Configurazione del ciclo di vita di PutBucket (in precedenza denominato ciclo di vita del 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, <code>ExpiredObjectDeleteMarker</code>) • <code>NoncurrentVersionExpiration</code> (<code>NewerNoncurrentVersions</code>, <code>NoncurrentDays</code>) • Filtro (Prefisso, Tag) • Stato • ID StorageGRID non supporta queste azioni: • <code>AnnulInCompletoCaricamento</code> multiparte • Transizione Vedere "Crea la configurazione del ciclo di vita S3" . Per comprendere come l'azione di scadenza nel ciclo di vita di un bucket interagisce con le istruzioni di posizionamento ILM, vedere "Come funziona l'ILM durante la vita di un oggetto" . Nota: la configurazione del ciclo di vita del bucket può essere utilizzata con bucket in cui è abilitato S3 Object Lock, ma la configurazione del ciclo di vita del bucket non è supportata per i bucket Compliant legacy.

Operazione	Implementazione
Configurazione della notifica PutBucket (in precedenza denominata notifica PUT Bucket)	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 come destinazioni gli argomenti Amazon Simple Notification Service (Amazon SNS) o Kafka. Gli endpoint Simple Queue Service (SQS) 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 Tenant Manager o Tenant Management API. Affinché la configurazione della notifica abbia esito positivo, è necessario che l'endpoint esista. Se l'endpoint non esiste, un 400 Bad Request l'errore viene restituito con il codice <code>InvalidArgument</code> . - Non è possibile configurare una notifica per i seguenti tipi di eventi. Questi tipi di eventi non sono supportati. <code>s3:ReducedRedundancyLostObject</code> <code>s3:ObjectRestore:Completed</code> - Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, con la differenza che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente: fonteevento <code>sgws:s3</code> awsRegion non incluso x-amz-id-2 non incluso arn <code>urn:sgws:s3:::bucket_name</code>
PutBucketPolicy	Imposta la policy associata al bucket. Vedere "Utilizzare criteri di accesso a bucket e gruppi" .

Operazione	Implementazione
PutBucketReplication	Configura "Replica StorageGRID CloudMirror" per il bucket utilizzando l'XML di configurazione della replica fornito nel corpo della richiesta. Per la replica CloudMirror, è necessario conoscere i seguenti dettagli di implementazione: • StorageGRID supporta solo la versione 1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'uso di <code>Filter</code> elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per i dettagli, vedere "Guida per l'utente di Amazon Simple Storage Service: configurazione della replica". • La replica dei bucket può essere configurata su bucket con o senza versione. • È possibile specificare un bucket di destinazione diverso in ogni regola del file XML di configurazione della replica. Un bucket di origine può replicarsi su più di un bucket di destinazione. • I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID come specificato in Tenant Manager o nell'API Tenant Management. Vedere "Configurare la replica di CloudMirror". Affinché la configurazione della replica abbia esito positivo, è necessario che l'endpoint esista. Se l'endpoint non esiste, la richiesta fallisce come 400 Bad Request Il messaggio di errore afferma: Unable to save the replication policy. The specified endpoint URN does not exist: <i>URN</i>. • Non è necessario specificare un <code>Role</code> nell'XML di configurazione. Questo valore non viene utilizzato da StorageGRID e verrà ignorato se inviato. • Se si omette la classe di archiviazione dall'XML di configurazione, StorageGRID utilizza <code>STANDARD</code> classe di archiviazione predefinita. • Se si elimina un oggetto dal bucket di origine o si elimina il bucket di origine stesso, il comportamento della replica tra regioni è il seguente: ◦ Se elimini l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non verrà replicato e non riceverai alcuna notifica. ◦ Se si elimina l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento di eliminazione standard di Amazon S3 per la V1 della replica tra regioni.

Operazione	Implementazione
PutBucketTagging	Utilizza il <code>tagging</code> sottorisorsa per aggiungere o aggiornare un set di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni: • Sia StorageGRID che Amazon S3 supportano fino a 50 tag per ogni bucket. • I tag associati a un bucket devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode. • I valori dei tag possono avere una lunghezza massima di 256 caratteri Unicode. • Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole. Attenzione: se per questo bucket è impostato un tag di policy ILM non predefinito, si verificherà un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket a cui è assegnato un valore. Assicuratevi che il <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket è incluso con il valore assegnato in tutte le richieste <code>PutBucketTagging</code>. Non modificare o rimuovere questo tag. Nota: questa operazione sovrascriverà tutti i tag correnti già presenti nel bucket. Se vengono omessi tag esistenti dal set, tali tag verranno rimossi dal bucket.
PutBucketVersioning	Utilizza il <code>versioning</code> sottorisorsa per impostare lo stato di controllo delle versioni di un bucket esistente. È possibile impostare lo stato di controllo delle versioni con uno dei seguenti valori: • Abilitato: abilita il controllo delle versioni per gli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID versione univoco. • Sospeso: disattiva il controllo delle versioni per gli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID versione <code>null</code>.
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 fino alle versioni esistenti degli oggetti rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" per informazioni dettagliate.

Operazioni sugli oggetti

Operazioni sugli oggetti

Questa sezione descrive come il sistema StorageGRID implementa le operazioni S3 REST API per gli oggetti.

Le seguenti condizioni si applicano a tutte le operazioni sugli oggetti:

- StorageGRID ["valori di coerenza"](#) sono supportati da tutte le operazioni sugli oggetti, ad eccezione delle

seguenti:

- OttieniOggettoAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - SelezionaOggettoContenuto
- Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.
 - Tutti gli oggetti in un bucket StorageGRID sono di proprietà del proprietario del bucket, compresi gli oggetti creati da un utente anonimo o da un altro account.
 - Gli oggetti dati acquisiti nel sistema StorageGRID tramite Swift non sono accessibili tramite S3.

La tabella seguente descrive come StorageGRID implementa le operazioni degli oggetti S3 REST API.

Operazione	Implementazione
EliminaOggetto	Autenticazione a più fattori (MFA) e intestazione di risposta <code>x-amz-mfa</code> non sono supportati. Durante l'elaborazione di una richiesta <code>DeleteObject</code>, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni archiviate. In caso di esito 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 quindi segnala l'esito positivo al client. Controllo delle versioni Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare <code>versionId</code> sottorisorsa. L'utilizzo di questa sottorisorsa elimina definitivamente la versione. Se il <code>versionId</code> corrisponde a un marcatore di eliminazione, l'intestazione della risposta <code>x-amz-delete-marker</code> viene restituito impostato su <code>true</code>. • Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket con controllo delle versioni abilitato, si traduce nella generazione di un marcatore di eliminazione. IL <code>versionId</code> per il marcatore di eliminazione viene restituito utilizzando il <code>x-amz-version-id</code> intestazione di risposta e <code>x-amz-delete-marker</code> l'intestazione di risposta viene restituita impostata su <code>true</code>. • Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket con controllo delle versioni sospeso, si traduce nell'eliminazione permanente di una versione 'null' già esistente o di un marcatore di eliminazione 'null' e nella generazione di un nuovo marcatore di eliminazione 'null'. IL <code>x-amz-delete-marker</code> l'intestazione di risposta viene restituita impostata su <code>true</code>. Nota: in alcuni casi, potrebbero esistere più marcatori di eliminazione per un oggetto. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" per scoprire come eliminare le versioni degli oggetti in modalità GOVERNANCE.
EliminaOggetti (in precedenza denominato DELETE Multiple Objects)	Autenticazione a più fattori (MFA) e intestazione di risposta <code>x-amz-mfa</code> non sono supportati. È possibile eliminare più oggetti nello stesso messaggio di richiesta. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" per scoprire come eliminare le versioni degli oggetti in modalità GOVERNANCE.

Operazione	Implementazione
DeleteObjectTagging	Utilizza il <code>tagging</code> sottorisorsa per rimuovere tutti i tag da un oggetto. Controllo delle versioni Se il <code>versionId</code> Se il parametro di 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 <code>x-amz-delete-marker</code> intestazione di risposta impostata su <code>true</code>.
OttieniOggetto	"OttieniOggetto"
OttieniOggettoAcl	Se vengono fornite le credenziali di accesso necessarie per l'account, l'operazione restituisce una risposta positiva e l'ID, il <code>DisplayName</code> e l'autorizzazione del proprietario dell'oggetto, a indicare che il proprietario ha accesso completo all'oggetto.
OttieniOggettoLegaleHold	"Utilizzare l'API REST S3 per configurare S3 Object Lock"
Ottieni conservazione oggetto	"Utilizzare l'API REST S3 per configurare S3 Object Lock"
OttieniTaggingOggetto	Utilizza il <code>tagging</code> sottorisorsa per restituire tutti i tag per un oggetto. Controllo delle versioni Se il <code>versionId</code> Se il parametro query non è specificato nella richiesta, l'operazione restituisce 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 <code>x-amz-delete-marker</code> intestazione di risposta impostata su <code>true</code>.
HeadObject	"HeadObject"
Ripristina oggetto	"Ripristina oggetto"
MettiOggetto	"MettiOggetto"
CopiaOggetto (in precedenza denominato PUT Object - Copy)	"CopiaOggetto"
PutObjectLegalHold	"Utilizzare l'API REST S3 per configurare S3 Object Lock"
PutObjectRetention	"Utilizzare l'API REST S3 per configurare S3 Object Lock"

Operazione	Implementazione
PutObjectTagging	Utilizza il <code>tagging</code> sottorisorsa per aggiungere un set di tag a un oggetto esistente. Limiti dei tag degli oggetti Puoi aggiungere tag ai nuovi oggetti quando li carichi oppure puoi aggiungerli agli oggetti esistenti. Sia StorageGRID che Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode e i valori tag possono avere una lunghezza massima di 256 caratteri Unicode. Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole. Aggiornamenti dei tag e comportamento di acquisizione Quando si utilizza PutObjectTagging per aggiornare i tag di un oggetto, StorageGRID non reingestisce l'oggetto. Ciò significa che l'opzione per il comportamento di acquisizione specificata nella regola ILM corrispondente non viene utilizzata. Tutte le modifiche al posizionamento degli oggetti 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 Rigorosa per il comportamento di acquisizione, non viene intrapresa alcuna azione se non è possibile effettuare i posizionamenti degli oggetti richiesti (ad esempio perché una posizione appena richiesta non è disponibile). L'oggetto aggiornato mantiene la sua posizione attuale finché non sarà possibile il posizionamento richiesto. Risolvere i conflitti Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione. Controllo delle versioni Se il <code>versionId</code> Se il parametro <code>query</code> 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 <code>x-amz-delete-marker</code> intestazione di risposta impostata su <code>true</code>.
SelezionaOggettoContenuto	"SelezionaOggettoContenuto"

Utilizzare S3 Select

StorageGRID supporta le seguenti clausole Amazon S3 Select, tipi di dati e operatori per "Comando `SelectObjectContent`".



Tutti gli elementi non elencati non sono supportati.

Per la sintassi, vedere ["SelezionaOggettoContenuto"](#) . Per ulteriori informazioni su S3 Select, vedere ["Documentazione AWS per S3 Select"](#) .

Solo gli account tenant che hanno abilitato S3 Select possono inviare query SelectObjectContent. Vedi il ["considerazioni e requisiti per l'utilizzo di S3 Select"](#) .

Clausole

- SELEZIONA elenco
- clausola FROM
- clausola WHERE
- Clausola LIMIT

Tipi di dati

- bool
- intero
- corda
- galleggiante
- decimale, numerico
- marca temporale

Operatori

Operatori logici

- E
- NON
- O

Operatori di confronto

- <
- >
- <=
- >=
- =
- =
- <>
- !=
- FRA
- IN

Operatori di corrispondenza di pattern

- COME
- _
- %

Operatori unitari

- È NULLO
- NON È NULLO

Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

Funzioni aggregate

- MEDIA()
- CONTARE(*)
- MAX()
- MIN()
- SOMMA()

Funzioni condizionali

- CASO
- COALESCERE
- NULLIF

Funzioni di conversione

- CAST (per i tipi di dati supportati)

Funzioni di data

- DATA_AGGIUNGI
- DATE_DIFF
- ESTRARRE
- A_STRINGA
- TO_TIMESTAMP

- UTCNOW

Funzioni stringa

- LUNGHEZZA_CARATTERE, LUNGHEZZA_CARATTERE
- INFERIORE
- SOTTOSTRINGA
- ORDINARE
- SUPERIORE

Utilizzare la crittografia lato server

La crittografia lato server consente di proteggere i dati degli oggetti quando sono inattivi. StorageGRID crittografa i dati durante la scrittura dell'oggetto e li decrittografa quando si accede all'oggetto.

Se si desidera utilizzare la crittografia lato server, è possibile scegliere una delle due opzioni reciprocamente esclusive, in base al modo in cui vengono gestite le chiavi di crittografia:

- **SSE (crittografia lato server con chiavi gestite StorageGRID):** quando si invia una richiesta S3 per archiviare 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 decrittografare l'oggetto.
- **SSE-C (crittografia lato server con chiavi fornite dal cliente):** quando si invia una richiesta S3 per archiviare un oggetto, si fornisce la propria chiave di crittografia. Quando recuperi un oggetto, fornisci la stessa chiave di crittografia come parte della tua 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 decrittografia 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 anche l'oggetto corrispondente.



Se un oggetto è 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 sugli oggetti:

- "MettiOggetto"
- "CopiaOggetto"
- "CreaCaricamentoMultiparte"

Utilizzare SSE-C

Per crittografare un oggetto con una chiave univoca gestita da te, puoi utilizzare 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 decrittografare l'oggetto. Il valore della chiave deve essere a 256 bit, codificato in base64.
x-amz-server-side-encryption-customer-key-MD5	Specificare il digest MD5 della chiave di crittografia secondo RFC 1321, utilizzato per garantire che la chiave di crittografia sia stata trasmessa senza errori. Il valore per il digest MD5 deve essere codificato in base64 a 128 bit.

Le intestazioni delle richieste SSE-C sono supportate dalle seguenti operazioni sugli oggetti:

- "OttieniOggetto"
- "HeadObject"
- "MettiOggetto"
- "CopiaOggetto"
- "CreaCaricamentoMultiparte"
- "CaricaParte"
- "CaricaParteCopia"

Considerazioni sull'utilizzo della crittografia lato server con chiavi fornite dal cliente (SSE-C)

Prima di utilizzare SSE-C, tenere presente quanto segue:

- Devi usare https.



StorageGRID rifiuta qualsiasi richiesta effettuata tramite http quando si utilizza SSE-C. Per motivi di sicurezza, è opportuno considerare compromessa qualsiasi chiave inviata accidentalmente tramite http. Scartare la chiave e ruotarla come appropriato.

- L'ETag nella risposta non è l'MD5 dei dati dell'oggetto.
- È necessario gestire la mappatura delle chiavi di crittografia sugli oggetti. StorageGRID non memorizza le chiavi di crittografia. Sei responsabile del monitoraggio della chiave di crittografia fornita per ciascun oggetto.
- Se il bucket è abilitato al controllo delle versioni, ogni versione dell'oggetto dovrebbe avere la propria chiave di crittografia. Sei responsabile del monitoraggio della chiave di crittografia utilizzata per ogni versione dell'oggetto.
- Poiché le chiavi di crittografia vengono gestite sul lato client, è necessario gestire anche eventuali misure di sicurezza 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 anche l'oggetto corrispondente.

- Se per il bucket è configurata la replica tra griglie o la replica CloudMirror, non è possibile acquisire oggetti SSE-C. L'operazione di acquisizione non andrà a buon fine.

Informazioni correlate

["Guida per l'utente di Amazon S3: utilizzo della crittografia lato server con chiavi fornite dal cliente \(SSE-C\)"](#)

CopiaOggetto

È possibile utilizzare la richiesta S3 CopyObject per creare una copia di un oggetto già archiviato in S3. Un'operazione CopyObject equivale all'esecuzione di GetObject seguito da PutObject.

Risolvere i conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *consigliata* per una singola operazione PutObject è 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa ["caricamento multiparte"](#). Invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).



Se hai eseguito l'aggiornamento da StorageGRID 11.6 o da una versione precedente, verrà attivato l'avviso S3 PUT Object size too large (Dimensioni oggetto troppo grandi) se tenti di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11.7 o 11.8, in questo caso l'avviso non verrà attivato. Tuttavia, per allinearsi allo standard AWS S3, le future versioni di StorageGRID non supporteranno caricamenti di oggetti di dimensioni superiori a 5 GiB.

Caratteri UTF-8 nei metadati utente

Se una richiesta include valori UTF-8 (non sottoposti a escape) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento StorageGRID non è definito.

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 sottoposti a escape vengono trattati come caratteri ASCII:

- Le richieste hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 con escape.
- StorageGRID non restituisce il `x-amz-missing-meta` intestazione 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.

Puoi 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.

Puoi specificare REPLACE per sovrascrivere i tag esistenti durante la copia dell'oggetto o per aggiornare i tag.

- Intestazioni delle richieste di blocco degli 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, vengono utilizzate le impostazioni di conservazione predefinite del bucket per calcolare la modalità di versione dell'oggetto e la data di conservazione fino alla data di scadenza. Vedere ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#) .

- Intestazioni delle richieste 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-checksum-algorithm

Quando si copia un oggetto, se l'oggetto di origine ha un checksum, StorageGRID non copia quel valore di checksum nel nuovo oggetto. Questo comportamento si applica indipendentemente dal fatto che tu provi o meno a utilizzare `x-amz-checksum-algorithm` nella richiesta dell'oggetto.

- x-amz-website-redirect-location

Opzioni di classe di archiviazione

IL `x-amz-storage-class` l'intestazione della richiesta è supportata e influisce sul numero di copie dell'oggetto che StorageGRID crea se la regola ILM corrispondente utilizza il commit doppio o bilanciato "opzione di ingestione".

- STANDARD

(Predefinito) Specifica un'operazione di acquisizione a doppio commit quando la regola ILM utilizza l'opzione Doppio commit o quando l'opzione Bilanciato ricorre alla creazione di copie provvisorie.

- REDUCED_REDUNDANCY

Specifica un'operazione di acquisizione con commit singolo quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ricorre alla creazione di copie provvisorie.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, REDUCED_REDUNDANCY l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme legacy, REDUCED_REDUNDANCY l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Utilizzo di x-amz-copy-source in CopyObject

Se il bucket di origine e la chiave, specificati in `x-amz-copy-source` intestazione, sono diversi dal bucket di destinazione e dalla chiave, una copia dei dati dell'oggetto sorgente viene scritta nella destinazione.

Se la sorgente 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 reingenerisce l'oggetto. Ciò ha due importanti conseguenze:

- Non è possibile utilizzare CopyObject per crittografare un oggetto esistente sul posto o per modificare la crittografia di un oggetto esistente sul posto. Se fornisci il `x-amz-server-side-encryption`

intestazione o il `x-amz-server-side-encryption-customer-algorithm` intestazione, StorageGRID rifiuta la richiesta e restituisce `XNotImplemented`.

- L'opzione per il comportamento di acquisizione specificata nella regola ILM corrispondente non viene utilizzata. Tutte le modifiche al posizionamento degli oggetti 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 Rigorosa per il comportamento di acquisizione, non viene intrapresa alcuna azione se non è possibile effettuare i posizionamenti degli oggetti richiesti (ad esempio perché una posizione appena richiesta non è disponibile). L'oggetto aggiornato mantiene la sua posizione attuale finché non sarà possibile il posizionamento richiesto.

Intestazioni di richiesta per la crittografia lato server

Se tu "[utilizzare la crittografia lato server](#)", le intestazioni di richiesta fornite dipendono dal fatto che l'oggetto di origine sia crittografato e dal fatto che si intenda crittografare l'oggetto di destinazione.

- Se l'oggetto sorgente è 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`: Specifica la chiave di crittografia fornita al momento della creazione dell'oggetto sorgente.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 fornito quando hai creato l'oggetto sorgente.
- Se desideri crittografare l'oggetto di destinazione (la copia) con una chiave univoca che fornisci e gestisci, includi 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 anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni per "[utilizzando la 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` il valore dell'oggetto non può essere aggiornato. Invece, fai una copia con un nuovo `server-side-encryption` valore utilizzando `x-amz-metadata-directive: REPLACE`.

Controllo delle versioni

Se il bucket di origine è sottoposto a versioning, 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 sottoposto a versioning, la versione generata viene restituita nel `x-amz-version-id` intestazione di risposta. Se il controllo delle versioni è sospeso per il bucket di destinazione, allora `x-amz-version-id` restituisce un valore "null".

OttieniOggetto

È possibile utilizzare la richiesta S3 `GetObject` per recuperare un oggetto da un bucket S3.

GetObject e oggetti multipart

Puoi usare il `partNumber` parametro di richiesta per recuperare una parte specifica di un oggetto multipart o segmentato. IL `x-amz-mp-parts-count` l'elemento di risposta indica quante parti ha l'oggetto.

Puoi impostare `partNumber` a 1 sia per gli oggetti segmentati/multiparte che per gli oggetti non segmentati/non multiparte; tuttavia, il `x-amz-mp-parts-count` l'elemento response viene restituito solo per oggetti segmentati o multiparte.

Caratteri UTF-8 nei metadati utente

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape nei metadati definiti dall'utente. Le richieste GET per un oggetto con caratteri UTF-8 sfuggiti 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 supportata

È supportata la seguente intestazione di richiesta:

- `x-amz-checksum-mode`: Specificare `ENABLED`

IL Range l'intestazione non è supportata con `x-amz-checksum-mode` per `GetObject`. Quando includi Range nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore di checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented` :

- `x-amz-website-redirect-location`

Controllo delle versioni

Se un `versionId` Se la sottorisorsa non è 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 di risposta impostata su `true`.

Intestazioni di richiesta 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 da te fornita.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256 .
- `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specifica 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 anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in ["Utilizzare la crittografia lato server"](#) .

Comportamento di GetObject per gli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in un ["Pool di archiviazione cloud"](#) , il comportamento di una richiesta GetObject dipende dallo stato dell'oggetto. Vedere ["HeadObject"](#) per maggiori dettagli.



Se un oggetto è archiviato in un Cloud Storage Pool e una o più copie dell'oggetto esistono anche sulla griglia, le richieste GetObject tenteranno di recuperare i dati dalla griglia prima di recuperarli dal Cloud Storage Pool.

Stato dell'oggetto	Comportamento di GetObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM, oppure oggetto archiviato in un pool di archiviazione tradizionale o mediante codifica di cancellazione	200 OK Viene recuperata una copia dell'oggetto.
Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	200 OK Viene recuperata una copia dell'oggetto.
Oggetto passato a uno stato non recuperabile	403 Forbidden , InvalidObjectState Utilizzare un "Ripristina oggetto" richiesta di ripristinare l'oggetto a uno stato recuperabile.
Oggetto in fase di ripristino da uno stato non recuperabile	403 Forbidden , InvalidObjectState Attendi 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 archiviazione cloud

Se hai caricato un oggetto multiparte o se StorageGRID ha suddiviso un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel Cloud Storage Pool campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta `GetObject` potrebbe restituire in modo errato `200 OK` 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.

In questi casi:

- La richiesta `GetObject` potrebbe restituire alcuni dati ma interrompersi a metà del trasferimento.
- Una successiva richiesta `GetObject` potrebbe restituire `403 Forbidden`.

GetObject e replicazione tra griglie

Se stai usando "federazione di rete" E "replicazione cross-grid" è abilitato per un bucket, il client S3 può verificare lo stato di replicazione di un oggetto emettendo una richiesta `GetObject`. La risposta include StorageGRID-specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	• COMPLETO: La replica è riuscita. • IN ATTESA: 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 il `x-amz-replication-status` intestazione.

HeadObject

È possibile utilizzare la richiesta S3 `HeadObject` per recuperare i metadati da un oggetto senza restituire l'oggetto stesso. Se l'oggetto è archiviato in un Cloud Storage Pool, è possibile utilizzare `HeadObject` per determinare lo stato di transizione dell'oggetto.

HeadObject e oggetti multiparte

Puoi usare il `partNumber` parametro di richiesta per recuperare i metadati per una parte specifica di un oggetto multiparte o segmentato. IL `x-amz-mp-parts-count` l'elemento di risposta indica quante parti ha l'oggetto.

Puoi impostare `partNumber` a 1 sia per gli oggetti segmentati/multiparte che per gli oggetti non segmentati/non multiparte; tuttavia, il `x-amz-mp-parts-count` l'elemento response viene restituito solo per oggetti segmentati o multiparte.

Caratteri UTF-8 nei metadati utente

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape nei metadati definiti dall'utente. Le

richieste HEAD per un oggetto con caratteri UTF-8 sfuggiti 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 supportata

È supportata la seguente intestazione di richiesta:

- `x-amz-checksum-mode`

Il `partNumber` parametro e `Range` l'intestazione non è supportata con `x-amz-checksum-mode` per `HeadObject`. Quando li includi nella richiesta con `x-amz-checksum-mode` abilitato, `StorageGRID` non restituisce un valore di checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented` :

- `x-amz-website-redirect-location`

Controllo delle versioni

Se un `versionId` Se la sottorisorsa non è 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 di risposta impostata su `true`.

Intestazioni di richiesta 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 da te fornita.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256 .
- `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specifica 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 anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in ["Utilizzare la crittografia lato server"](#) .

Risposte `HeadObject` per gli oggetti `Cloud Storage Pool`

Se l'oggetto è memorizzato in un ["Pool di archiviazione cloud"](#) , vengono restituite le seguenti intestazioni di risposta:

- `x-amz-storage-class`: GLACIER
- `x-amz-restore`

Le intestazioni di risposta forniscono informazioni sullo stato di un oggetto mentre viene spostato in un `Cloud Storage Pool`, facoltativamente portato a uno stato non recuperabile e ripristinato.

Stato dell'oggetto	Risposta a HeadObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM, oppure oggetto archiviato in un pool di archiviazione tradizionale o mediante codifica di cancellazione	200 OK(Non viene restituita alcuna intestazione di risposta speciale.)
Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" Finché l'oggetto non viene portato in uno stato non recuperabile, il valore per expiry-date è ambientato in un lontano futuro. Il momento esatto della transizione non è controllato dal sistema StorageGRID .
L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche sulla griglia	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" Il valore per expiry-date è ambientato in un lontano futuro. Nota: se la copia sulla griglia non è disponibile (ad esempio, un nodo di archiviazione è inattivo), è necessario emettere un "Ripristina oggetto" richiedere di ripristinare la copia dal Cloud Storage Pool prima di poter recuperare correttamente l'oggetto.
L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia sulla 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: ongoing-request="true"

Stato dell'oggetto	Risposta a HeadObject
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" IL expiry-date indica quando l'oggetto nel Cloud Storage Pool tornerà a uno stato non recuperabile.

Oggetti multiparte o segmentati in Cloud Storage Pool

Se hai caricato un oggetto multiparte o se StorageGRID ha suddiviso un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel Cloud Storage Pool campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta HeadObject potrebbe restituire in modo errato `x-amz-restore: ongoing-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 replicazione cross-grid

Se stai usando "federazione di rete" E "replicazione cross-grid" è abilitato per un bucket, il client S3 può verificare lo stato di replicazione di un oggetto inviando una richiesta HeadObject. La risposta include StorageGRID-specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	• COMPLETO: La replica è riuscita. • IN ATTESA: 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 il `x-amz-replication-status` intestazione.

MettiOggetto

È possibile utilizzare la richiesta S3 PutObject per aggiungere un oggetto a un bucket.

Risolvere i conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *consigliata* per una singola operazione PutObject è 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa "[caricamento multiparte](#)". Invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).



Se hai eseguito l'aggiornamento da StorageGRID 11.6 o da una versione precedente, verrà attivato l'avviso S3 PUT Object size too large (Dimensioni oggetto troppo grandi) se tenti di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11.7 o 11.8, in questo caso l'avviso non verrà attivato. Tuttavia, per allinearsi allo standard AWS S3, le future versioni di StorageGRID non supporteranno caricamenti di oggetti di dimensioni superiori a 5 GiB.

Dimensione dei metadati 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 utente a 24 KiB. La dimensione dei metadati definiti dall'utente viene misurata sommando il numero di byte nella codifica UTF-8 di ciascuna chiave e valore.

Caratteri UTF-8 nei metadati utente

Se una richiesta include valori UTF-8 (non sottoposti a escape) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento StorageGRID non è definito.

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 sottoposti a escape 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 con escape.
- StorageGRID non restituisce il `x-amz-missing-meta` intestazione se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

Limiti dei tag degli oggetti

Puoi aggiungere tag ai nuovi oggetti quando li carichi oppure puoi aggiungerli agli oggetti esistenti. Sia StorageGRID che Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode e i valori tag possono avere una lunghezza massima di 256 caratteri Unicode. Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole.

Proprietà dell'oggetto

In StorageGRID, tutti gli oggetti sono di proprietà dell'account proprietario del bucket, compresi 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 specifichi `aws-chunked` per `Content-Encoding` StorageGRID non verifica i seguenti elementi:

- StorageGRID non verifica il `chunk-signature` rispetto ai dati in blocco.
- StorageGRID non verifica il valore fornito per `x-amz-decoded-content-length` contro l'oggetto.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

La codifica di trasferimento in blocchi è supportata se `aws-chunked` viene utilizzata anche la firma del payload.

- `x-amz-checksum-sha256`
- `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 **Ora di creazione definita dall'utente** come ora di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano quando è stato creato l'oggetto. Per esempio:

```
x-amz-meta-creation-time: 1443399726
```

Il valore per `creation-time` viene valutato in secondi a partire dal 1° gennaio 1970.



Una regola ILM non può utilizzare sia un **orario di creazione definito dall'utente** per l'orario di riferimento sia l'opzione di acquisizione bilanciata o rigorosa. Viene restituito un errore quando viene creata la regola ILM.

- `x-amz-tagging`
- Intestazioni di richiesta di blocco degli 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, vengono utilizzate le impostazioni di conservazione predefinite del bucket per calcolare la modalità di versione dell'oggetto e la data di conservazione fino alla data di scadenza. Vedere ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#).

- Intestazioni delle richieste 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:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

IL `x-amz-website-redirect-location` intestazione ritorna `XNotImplemented`.

Opzioni di classe di archiviazione

IL `x-amz-storage-class` è supportata l'intestazione della richiesta. 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 archiviate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto ingerito utilizza l'opzione di ingestione rigorosa, `x-amz-storage-class` l'intestazione non ha alcun effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class`:

- **STANDARD(Predefinito)**
 - **Doppio commit:** se la regola ILM specifica l'opzione Doppio commit per Comportamento di acquisizione, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita a un diverso nodo di archiviazione (doppio commit). Quando l'ILM viene valutato, StorageGRID determina se queste copie provvisorie iniziali soddisfano le istruzioni di posizionamento nella regola. In caso contrario, potrebbe essere necessario creare nuove copie dell'oggetto in posizioni diverse e le copie provvisorie iniziali potrebbero dover essere eliminate.
 - **Bilanciato:** se la regola ILM specifica l'opzione Bilanciato e StorageGRID non riesce a effettuare immediatamente tutte le copie specificate nella regola, StorageGRID effettua due copie provvisorie su nodi di archiviazione diversi.

Se StorageGRID può creare immediatamente tutte le copie degli oggetti specificate nella regola ILM (posizionamento sincrono), `x-amz-storage-class` l'intestazione non ha alcun effetto.

- REDUCED_REDUNDANCY

- **Doppio commit:** se la regola ILM specifica l'opzione Doppio commit per Comportamento di acquisizione, StorageGRID crea una singola copia provvisoria durante l'acquisizione dell'oggetto (singolo commit).
- **Bilanciato:** se la regola ILM specifica l'opzione Bilanciato, StorageGRID esegue una singola copia provvisoria solo se il sistema non riesce a eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID può eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. IL REDUCED_REDUNDANCY L'opzione è più indicata quando la regola ILM che corrisponde all'oggetto crea una singola copia replicata. In questo caso utilizzando REDUCED_REDUNDANCY elimina la creazione e l'eliminazione non necessarie di una copia extra dell'oggetto per ogni operazione di acquisizione.

Utilizzando il REDUCED_REDUNDANCY questa opzione non è consigliata in altre circostanze.

REDUCED_REDUNDANCY aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, si potrebbero perdere dati se la singola copia viene inizialmente archiviata su un nodo di archiviazione che si guasta prima che possa aver luogo la valutazione ILM.



Disporre di una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

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 effettuate quando l'oggetto viene valutato dai criteri ILM attivi e non determina l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID .



Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, REDUCED_REDUNDANCY l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme legacy, REDUCED_REDUNDANCY l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio 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 la 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`

Quando il `x-amz-server-side-encryption` l'intestazione non è inclusa nella richiesta PutObject, la griglia "impostazione di crittografia degli oggetti memorizzati" viene omesso dalla risposta PutObject.

- **SSE-C:** utilizzare tutte e tre queste intestazioni 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:` Specifica 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 anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni per ["utilizzando la crittografia lato server"](#).



Se un oggetto è crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Controllo delle versioni

Se il controllo delle versioni è abilitato per un bucket, univoco `versionId` viene generato automaticamente per la versione dell'oggetto memorizzato. Questo `versionId` viene restituito anche nella risposta utilizzando il `x-amz-version-id` intestazione di risposta.

Se il controllo delle versioni è sospeso, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, questa verrà sovrascritta.

Calcoli della firma per l'intestazione di autorizzazione

Quando si utilizza il `Authorization` intestazione per autenticare le richieste, StorageGRID differisce da AWS nei seguenti modi:

- StorageGRID non richiede `host` intestazioni da includere all'interno `CanonicalHeaders`.
- StorageGRID non richiede `Content-Type` da includere all'interno `CanonicalHeaders`.
- StorageGRID non richiede `x-amz-*` intestazioni da includere all'interno `CanonicalHeaders`.



Come buona pratica generale, includi sempre queste intestazioni all'interno `CanonicalHeaders` per garantire che siano verificati; tuttavia, se si escludono queste intestazioni, StorageGRID non restituisce un errore.

Per i dettagli, fare riferimento a ["Calcoli della firma per l'intestazione di autorizzazione: trasferimento del payload in un singolo blocco \(AWS Signature versione 4\)"](#).

Informazioni correlate

- ["Gestire gli oggetti con ILM"](#)
- ["Riferimento API di Amazon Simple Storage Service: PutObject"](#)

Ripristina oggetto

È possibile utilizzare la richiesta `S3 RestoreObject` per ripristinare un oggetto archiviato in un Cloud Storage Pool.

Tipo di richiesta supportato

StorageGRID supporta solo le richieste `RestoreObject` per ripristinare un oggetto. Non supporta il `SELECT` tipo

di restauro. Seleziona le richieste di ritorno `XNotImplemented`.

Controllo delle versioni

Facoltativamente, specificare `versionId` per ripristinare una versione specifica di un oggetto in un bucket con versione. Se non specifichi `versionId`, viene ripristinata la versione più recente dell'oggetto

Comportamento di `RestoreObject` sugli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in un "[Pool di archiviazione cloud](#)", una richiesta `RestoreObject` ha il seguente comportamento, in base allo stato dell'oggetto. Vedere "[HeadObject](#)" per maggiori dettagli.



Se un oggetto è archiviato in un Cloud Storage Pool e sulla griglia sono presenti anche una o più copie dell'oggetto, non è necessario ripristinare l'oggetto inviando una richiesta `RestoreObject`. In alternativa, è possibile recuperare direttamente la copia locale, utilizzando una richiesta `GetObject`.

Stato dell'oggetto	Comportamento di <code>RestoreObject</code>
Oggetto inserito in <code>StorageGRID</code> ma non ancora valutato da ILM oppure l'oggetto non si trova in un Cloud Storage Pool	<code>403 Forbidden, InvalidObjectState</code>
Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	<code>`200 OK`</code> Non vengono apportate modifiche. Nota: prima che un oggetto sia passato a uno stato non recuperabile, non è possibile modificarne lo stato. <code>expiry-date</code> .
Oggetto passato a uno stato non recuperabile	<code>`202 Accepted`</code> 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 torna a uno stato non recuperabile. Facoltativamente, utilizzare il <code>Tier</code> elemento di richiesta per determinare quanto tempo impiegherà il processo di ripristino per essere completato (<code>Expedited</code> , <code>Standard</code> , <code>On Bulk</code>). Se non specifichi <code>Tier</code> , il <code>Standard</code> viene utilizzato il livello. Importante: se un oggetto è stato trasferito a S3 Glacier Deep Archive o il pool di archiviazione cloud utilizza l'archiviazione BLOB di Azure, non è possibile ripristinarlo utilizzando <code>Expedited</code> livello. Viene restituito il seguente errore <code>403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class</code> .
Oggetto in fase di ripristino da uno stato non recuperabile	<code>409 Conflict, RestoreAlreadyInProgress</code>

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK Nota: se un oggetto è stato ripristinato in uno stato recuperabile, è possibile modificarne lo stato <code>expiry-date</code> rimettendo la richiesta <code>RestoreObject</code> con un nuovo valore per <code>Days</code>. La data di ripristino viene aggiornata in base al momento della richiesta.

SelezionaOggettoContenuto

È possibile utilizzare la richiesta `S3 SelectObjectContent` per filtrare il contenuto di un oggetto S3 in base a una semplice istruzione SQL.

Per maggiori informazioni vedere ["Riferimento API di Amazon Simple Storage Service: SelectObjectContent"](#).

Prima di iniziare

- L'account tenant dispone dell'autorizzazione `S3 Select`.
- Hai `s3:GetObject` autorizzazione per l'oggetto che si desidera interrogare.
- L'oggetto che si desidera interrogare 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 Parquet:
 - S3 Select supporta solo la compressione colonnare tramite GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti Parquet.
 - S3 Select non supporta l'output Parquet. È necessario specificare il formato di output come CSV o JSON.
 - La dimensione massima del gruppo di righe non compresso è 512 MB.
 - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
 - Non è possibile utilizzare i tipi logici INTERVAL, JSON, LIST, TIME o UUID.
- La lunghezza massima dell'espressione SQL è di 256 KB.
- Ogni record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

Esempio di sintassi della richiesta 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 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 ricava il nome dello stato, la popolazione del 2010, la popolazione stimata del 2015 e la percentuale di variazione dai 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 , assomiglia a questo:

```
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, assomiglia a questo:

```
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
```

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, hanno questo aspetto:

```
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 caricamenti multiparte

Questa sezione descrive come StorageGRID supporta le operazioni per i caricamenti multiparte.

Le seguenti condizioni e note si applicano a tutte le operazioni di caricamento multiparte:

- Non dovresti superare i 1.000 caricamenti multipart simultanei in un singolo bucket perché i risultati delle query ListMultipartUploads per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID impone limiti dimensionali AWS per le parti multiparte. I client S3 devono seguire queste linee guida:
 - Ogni parte di un caricamento multipart deve avere una dimensione 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 dovrebbero essere le più grandi possibile. Ad esempio, utilizzare dimensioni di parti pari a 5 GiB per un oggetto da 100 GiB. Poiché ogni parte è considerata un oggetto unico, l'utilizzo di parti di grandi dimensioni riduce il sovraccarico dei metadati StorageGRID.
 - Per oggetti di dimensioni inferiori a 5 GiB, si consiglia di utilizzare il caricamento non multiparte.
- ILM viene valutato per ogni parte di un oggetto multipart mentre viene ingerito e per l'oggetto nel suo complesso quando il caricamento multipart viene completato, se la regola ILM utilizza Bilanciato o Rigoroso **"opzione di ingestione"**. È necessario essere consapevoli di come ciò influisce sul posizionamento di oggetti e parti:
 - Se ILM cambia mentre è in corso un caricamento multipart S3, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento multiparte. Ogni parte non posizionata

correttamente viene messa in coda per la rivalutazione ILM e successivamente spostata nella posizione corretta.

- Quando si valuta l'ILM per una parte, StorageGRID filtra in base alle dimensioni della parte, non in base alle dimensioni dell'oggetto. Ciò significa che parti di un oggetto possono essere archiviate 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 vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene archiviata in DC2 al momento dell'acquisizione. Tuttavia, quando l'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 ingerito tramite caricamento multiparte, **"soglia di segmentazione degli oggetti (1 GiB)"** non viene applicato.
- Se necessario, puoi utilizzare **"crittografia lato server"** con caricamenti in più parti. 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), è necessario specificare le stesse tre intestazioni di richiesta della chiave di crittografia nella richiesta CreateMultipartUpload e in ogni successiva richiesta UploadPart.

Operazione	Implementazione
Annulla caricamento multiparte	Implementato con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
Caricamento multiparte completo	Vedere "Caricamento multiparte completo"
CreaCaricamentoMultiparte (in precedenza denominato Avvia caricamento multiparte)	Vedere "CreaCaricamentoMultiparte"
Caricamenti multiparte di List	Vedere "Caricamenti multiparte di List"
ElencoParti	Implementato con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
CaricaParte	Vedere "CaricaParte"
CaricaParteCopia	Vedere "CaricaParteCopia"

Caricamento multiparte completo

L'operazione CompleteMultipartUpload completa il caricamento multiparte di un oggetto assemblando le parti caricate in precedenza.



StorageGRID supporta valori non consecutivi in ordine crescente per `partNumber` parametro di richiesta con CompleteMultipartUpload. Il parametro può iniziare con qualsiasi valore.

Risolvere i conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

IL `x-amz-storage-class` l'intestazione influisce sul numero di copie dell'oggetto che StorageGRID crea se la regola ILM corrispondente specifica ["Opzione di commit doppio o di gestione bilanciata"](#).

- STANDARD

(Predefinito) Specifica un'operazione di acquisizione a doppio commit quando la regola ILM utilizza l'opzione Doppio commit o quando l'opzione Bilanciato ricorre alla creazione di copie provvisorie.

- REDUCED_REDUNDANCY

Specifica un'operazione di acquisizione con commit singolo quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ricorre alla creazione di copie provvisorie.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, REDUCED_REDUNDANCY l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme legacy, REDUCED_REDUNDANCY l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio commit per garantire che i requisiti di conformità siano soddisfatti.



Se un caricamento multipart non viene completato entro 15 giorni, l'operazione viene contrassegnata come inattiva e tutti i dati associati vengono eliminati 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 multipart.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controllo delle versioni

Questa operazione completa un caricamento in più parti. Se per un bucket è abilitato il controllo delle versioni, la versione dell'oggetto viene creata dopo il completamento del caricamento multipart.

Se il controllo delle versioni è abilitato per un bucket, univoco `versionId` viene generato automaticamente

per la versione dell'oggetto memorizzato. Questo `versionId` viene restituito anche nella risposta utilizzando il `x-amz-version-id` intestazione di risposta.

Se il controllo delle versioni è sospeso, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, questa verrà sovrascritta.



Quando il controllo delle versioni è abilitato per un bucket, il completamento di un caricamento multiparte crea sempre una nuova versione, anche se sono stati completati caricamenti multiparte simultanei sulla stessa chiave oggetto. Quando il controllo delle versioni non è abilitato per un bucket, è possibile avviare un caricamento multiparte e quindi avviare e completare prima un altro caricamento multiparte sulla stessa chiave dell'oggetto. Nei bucket senza controllo delle versioni, ha la precedenza il caricamento multiparte completato per ultimo.

Replicazione, notifica o notifica dei metadati non riuscita

Se il bucket in cui avviene il caricamento multiparte è configurato per un servizio di piattaforma, il caricamento multiparte riesce anche se l'azione di replica o notifica associata fallisce.

Un tenant può attivare la replica non riuscita o la notifica aggiornando i metadati o i tag dell'oggetto. Un inquilino può reinviare i valori esistenti per evitare di apportare modifiche indesiderate.

Fare riferimento a ["Risolvere i problemi dei servizi della piattaforma"](#).

CreaCaricamentoMultiparte

L'operazione `CreateMultipartUpload` (in precedenza denominata `Initiate Multipart Upload`) avvia un caricamento multiparte per un oggetto e restituisce un ID di caricamento.

IL `x-amz-storage-class` è supportata l'intestazione della richiesta. 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 archiviate nel sistema `StorageGRID` (determinato da ILM).

Se la regola ILM corrispondente a un oggetto ingerito utilizza Strict"[opzione di ingestione](#)", IL `x-amz-storage-class` l'intestazione non ha alcun effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class`:

- **STANDARD(Predefinito)**
 - **Doppio commit:** se la regola ILM specifica l'opzione di acquisizione Doppio commit, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita a un diverso nodo di archiviazione (doppio commit). Quando l'ILM viene valutato, `StorageGRID` determina se queste copie provvisorie iniziali soddisfano le istruzioni di posizionamento nella regola. In caso contrario, potrebbe essere necessario creare nuove copie dell'oggetto in posizioni diverse e le copie provvisorie iniziali potrebbero dover essere eliminate.
 - **Bilanciato:** se la regola ILM specifica l'opzione Bilanciato e `StorageGRID` non riesce a effettuare immediatamente tutte le copie specificate nella regola, `StorageGRID` effettua due copie provvisorie su nodi di archiviazione diversi.

Se `StorageGRID` può creare immediatamente tutte le copie degli oggetti specificate nella regola ILM (posizionamento sincrono), `x-amz-storage-class` l'intestazione non ha alcun effetto.

- **REDUCED_REDUNDANCY**

- **Doppio commit:** se la regola ILM specifica l'opzione Doppio commit, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (singolo commit).
- **Bilanciato:** se la regola ILM specifica l'opzione Bilanciato, StorageGRID esegue una singola copia provvisoria solo se il sistema non riesce a eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID può eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. IL `REDUCED_REDUNDANCY` L'opzione è più indicata quando la regola ILM che corrisponde all'oggetto crea una singola copia replicata. In questo caso utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia extra dell'oggetto per ogni operazione di acquisizione.

Utilizzando il `REDUCED_REDUNDANCY` questa opzione non è consigliata in altre circostanze.

`REDUCED_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, si potrebbero perdere dati se la singola copia viene inizialmente archiviata su un nodo di archiviazione che si guasta prima che possa aver luogo la valutazione ILM.



Disporre di una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

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 effettuate quando l'oggetto viene valutato dai criteri ILM attivi e non determina l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Content-Type`
- `x-amz-checksum-algorithm`

Attualmente, solo il valore `SHA256` per `x-amz-checksum-algorithm` è supportato.

- `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 **Ora di creazione definita dall'utente** come ora di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano quando è

stato creato l'oggetto. Per esempio:

```
x-amz-meta-creation-time: 1443399726
```

Il valore per `creation-time` viene valutato in secondi a partire dal 1° gennaio 1970.



Aggiunta `creation-time` poiché i metadati definiti dall'utente non sono consentiti se si aggiunge un oggetto a un bucket in cui è abilitata la conformità legacy. Verrà restituito un errore.

- Intestazioni delle richieste di blocco degli 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, per calcolare la versione dell'oggetto `retain-until-date` vengono utilizzate le impostazioni di conservazione predefinite del bucket.

["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#)

- Intestazioni delle richieste 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 ["MettiOggetto"](#).

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto multipart con la 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 queste intestazioni nella richiesta `CreateMultipartUpload` (e in ogni successiva richiesta `UploadPart`) 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`: Specifica 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 anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni per ["utilizzando la crittografia lato server"](#).

Intestazioni di richiesta non supportate

La seguente intestazione di richiesta non è supportata:

- `x-amz-website-redirect-location`

IL `x-amz-website-redirect-location` intestazione ritorna `XNotImplemented`.

Controllo delle versioni

Il caricamento multiparte consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e sottoposti a controllo di versione, se applicabile) quando viene eseguita l'operazione `CompleteMultipartUpload`.

Caricamenti multiparte di List

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`

Controllo delle versioni

Il caricamento multiparte consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e sottoposti a controllo di versione, se applicabile) quando viene eseguita l'operazione `CompleteMultipartUpload`.

CaricaParte

L'operazione `UploadPart` carica una parte in un caricamento multiparte per un oggetto.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Intestazioni di richiesta per la crittografia lato server

Se hai specificato la crittografia SSE-C per la richiesta `CreateMultipartUpload`, devi 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 anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in ["Utilizzare la crittografia lato server"](#) .

Se hai specificato un checksum SHA-256 durante la richiesta `CreateMultipartUpload`, devi includere anche la seguente intestazione di richiesta in ogni richiesta `UploadPart`:

- `x-amz-checksum-sha256`: Specificare il checksum SHA-256 per questa parte.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controllo delle versioni

Il caricamento multiparte consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e sottoposti a controllo di versione, se applicabile) quando viene eseguita l'operazione `CompleteMultipartUpload`.

CaricaParteCopia

L'operazione `UploadPartCopy` carica una parte di un oggetto copiando i dati da un oggetto esistente come origine dati.

L'operazione `UploadPartCopy` è implementata con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.

Questa richiesta legge e scrive i dati dell'oggetto specificati in `x-amz-copy-source-range` all'interno del 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 hai specificato la crittografia SSE-C per la richiesta `CreateMultipartUpload`, devi 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 sorgente è 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`: Specifica la chiave di crittografia fornita al momento della creazione dell'oggetto sorgente.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 fornito quando hai creato l'oggetto sorgente.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in "[Utilizzare la crittografia lato server](#)".

Controllo delle versioni

Il caricamento multipart consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e sottoposti a controllo di versione, se applicabile) quando viene eseguita l'operazione `CompleteMultipartUpload`.

Risposte di errore

Il sistema StorageGRID supporta tutte le risposte di errore standard S3 REST API applicabili. Inoltre, l'implementazione StorageGRID aggiunge diverse risposte personalizzate.

Codici di errore API S3 supportati

Nome	Stato HTTP
Accesso negato	403 Proibito
BadDigest	400 Richiesta non valida
BucketAlreadyExists	409 Conflitto
BucketNotEmpty	409 Conflitto
Corpo incompleto	400 Richiesta non valida
Errore interno	500 Errore interno del server
ID chiave di accesso non valido	403 Proibito
Argomento non valido	400 Richiesta non valida
NomeBucketNonValido	400 Richiesta non valida
StatoBucketNonValido	409 Conflitto
InvalidDigest	400 Richiesta non valida
Errore algoritmo di crittografia non valido	400 Richiesta non valida
Parte non valida	400 Richiesta non valida
OrdineParteNonValido	400 Richiesta non valida
Intervallo non valido	416 Intervallo richiesto non soddisfacibile
Richiesta non valida	400 Richiesta non valida
Classe di archiviazione non valida	400 Richiesta non valida
Tag non valido	400 Richiesta non valida
URI non valido	400 Richiesta non valida
KeyTooLong	400 Richiesta non valida
XML malformato	400 Richiesta non valida

Nome	Stato HTTP
Metadati troppo grandi	400 Richiesta non valida
Metodo non consentito	405 Metodo non consentito
Lunghezza del contenuto mancante	411 Lunghezza richiesta
Errore mancante nel corpo della richiesta	400 Richiesta non valida
MissingSecurityHeader	400 Richiesta non valida
NoSuchBucket	404 Non trovato
Nessuna chiave	404 Non trovato
NoSuchUpload	404 Non trovato
Non implementato	501 Non implementato
NoSuchBucketPolicy	404 Non trovato
Errore ObjectLockConfigurationNotFound	404 Non trovato
Precondizione fallita	412 Precondizione fallita
RequestTimeTooSkewed	403 Proibito
Servizio non disponibile	503 Servizio non disponibile
Firma non corrisponde	403 Proibito
Troppi secchi	400 Richiesta non valida
UserKeyMustBeSpecified	400 Richiesta non valida

Codici di errore personalizzati StorageGRID

Nome	Descrizione	Stato HTTP
XBucketLifecycleNotAllowed	La configurazione del ciclo di vita del bucket non è consentita in un bucket conforme legacy	400 Richiesta non valida
XBucketPolicyParseException	Impossibile analizzare il JSON del criterio del bucket ricevuto.	400 Richiesta non valida

Nome	Descrizione	Stato HTTP
XComplianceConflict	Operazione negata a causa delle impostazioni di conformità legacy.	403 Proibito
XComplianceReducedRedundancyForbidden	La ridondanza ridotta non è consentita nel bucket Compliant legacy	400 Richiesta non valida
XMaxBucketPolicyLengthExceeded	La tua policy supera la lunghezza massima consentita per il bucket.	400 Richiesta non valida
XMissingInternalRequestHeader	Manca un'intestazione di una richiesta interna.	400 Richiesta non valida
XNoSuchBucketCompliance	Nel bucket specificato non è abilitata la conformità legacy.	404 Non trovato
XNon accettabile	La richiesta contiene una o più intestazioni di accettazione che non è stato possibile soddisfare.	406 Non accettabile
XNonImplementato	La richiesta da te fornita implica una funzionalità non implementata.	501 Non implementato

Operazioni personalizzate StorageGRID

Operazioni personalizzate StorageGRID

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
"OTTIENI la coerenza del bucket"	Restituisce la coerenza applicata a un determinato bucket.
"PUT Consistenza del secchio"	Imposta la coerenza applicata a un determinato bucket.
"GET Ora dell'ultimo accesso al bucket"	Restituisce se gli aggiornamenti dell'ora dell'ultimo accesso sono abilitati o disabilitati per un determinato bucket.
"Ora dell'ultimo accesso al bucket PUT"	Consente di abilitare o disabilitare gli aggiornamenti dell'ora dell'ultimo accesso per un determinato bucket.
"ELIMINA la configurazione della notifica dei metadati del bucket"	Elimina l'XML di configurazione delle notifiche dei metadati associato a un determinato bucket.

Operazione	Descrizione
"Configurazione della notifica dei metadati del bucket GET"	Restituisce il file XML di configurazione delle notifiche dei metadati associato a un determinato bucket.
"Configurazione della notifica dei metadati del bucket PUT"	Configura il servizio di notifica dei metadati per un bucket.
"Utilizzo dello spazio di archiviazione GET"	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 la conformità abilitata.
"Obsoleto: conformità al bucket GET"	Obsoleto ma supportato: restituisce le impostazioni di conformità attualmente in vigore per un bucket Compliant legacy esistente.
"Obsoleto: conformità al bucket PUT"	Obsoleto ma supportato: consente di modificare le impostazioni di conformità per un bucket Compliant legacy esistente.

OTTIENI la coerenza del bucket

La richiesta di coerenza del bucket GET consente di determinare la coerenza applicata a un determinato bucket.

La coerenza predefinita è impostata per garantire la lettura dopo la scrittura per gli oggetti appena creati.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:GetBucketConsistency oppure essere l'account root.

Richiedi esempio

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Risposta

Nella risposta XML, <Consistency> restituirà uno dei seguenti valori:

Coerenza	Descrizione
Tutto	Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
forte-globale	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti.

Coerenza	Descrizione
sito forte	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito.
lettura dopo nuova scrittura	(Predefinito) Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
disponibile	Fornisce 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 letti raramente o per operazioni HEAD o GET su chiavi inesistenti). 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"](#)

PUT Consistenza del secchio

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 la scrittura per gli oggetti appena creati.

Prima di iniziare

Per completare questa operazione è necessario disporre dell'autorizzazione s3:PutBucketConsistency oppure essere l'account root.

Richiesta

IL x-ntap-sg-consistency il parametro deve contenere uno dei seguenti valori:

Coerenza	Descrizione
Tutto	Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
forte-globale	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti.
sito forte	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito.
lettura dopo nuova scrittura	(Predefinito) Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
disponibile	Fornisce 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 letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool .

Nota: in generale, dovresti usare la coerenza "Lettura dopo nuova scrittura". Se le richieste non funzionano correttamente, modificare, se possibile, il comportamento del client dell'applicazione. Oppure, configura il client in modo che specifichi la coerenza per ogni richiesta API. Impostare la coerenza a livello di bucket solo come ultima risorsa.

Richiedi esempio

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informazioni correlate

["Valori di coerenza"](#)

GET Ora dell'ultimo accesso al bucket

La richiesta GET sull'orario dell'ultimo accesso al bucket consente di determinare se gli aggiornamenti dell'orario dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket.

Per completare questa operazione è necessario disporre dell'autorizzazione `s3:GetBucketLastAccessTime` oppure essere l'account root.

Richiedi esempio

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Questo esempio mostra che gli aggiornamenti dell'ora dell'ultimo accesso sono abilitati 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>
```

Ora dell'ultimo accesso al bucket PUT

La richiesta dell'orario dell'ultimo accesso al bucket PUT consente di abilitare o disabilitare gli aggiornamenti dell'orario dell'ultimo accesso per singoli bucket. La disattivazione degli aggiornamenti dell'ora dell'ultimo 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 oppure essere l'account root.



A partire dalla versione 10.3 StorageGRID, gli aggiornamenti all'ora dell'ultimo accesso sono disabilitati per impostazione predefinita per tutti i nuovi bucket. Se si dispone di bucket creati utilizzando una versione precedente di StorageGRID e si desidera applicare il nuovo comportamento predefinito, è necessario disabilitare esplicitamente gli aggiornamenti dell'ora dell'ultimo accesso per ciascuno di tali bucket precedenti. È possibile abilitare o disabilitare gli aggiornamenti all'orario dell'ultimo accesso tramite la richiesta dell'orario dell'ultimo accesso al bucket PUT o dalla pagina dei dettagli di un bucket in Tenant Manager. Vedere ["Abilita o disabilita gli aggiornamenti dell'ultimo orario di accesso"](#).

Se gli aggiornamenti dell'ora dell'ultimo accesso sono disabilitati 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 della gestione del ciclo di vita delle informazioni (ILM).

- 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 all'ora dell'ultimo accesso sono disabilitati 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 per il 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.
- Le richieste CompleteMultipartUpload aggiornano l'orario dell'ultimo accesso. L'oggetto completato viene aggiunto alle code per la valutazione ILM.

Esempi di richiesta

Questo esempio abilita l'orario dell'ultimo accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Questo esempio disabilita l'orario dell'ultimo accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

ELIMINA la configurazione della notifica dei metadati del bucket

La richiesta di configurazione della notifica dei metadati DELETE Bucket consente di disabilitare il servizio di integrazione della ricerca per singoli bucket eliminando l'XML di configurazione.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:DeleteBucketMetadataNotification per un bucket oppure essere l'account root.

Richiedi esempio

Questo esempio mostra come disabilitare il 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
```

Configurazione della notifica dei metadati del bucket GET

La richiesta di configurazione della notifica dei metadati del bucket GET 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` oppure essere l'account root.

Richiedi esempio

Questa richiesta recupera la configurazione della 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 come configurare il bucket per l'integrazione della ricerca. Ciò significa che è possibile determinare quali oggetti sono 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 a cui StorageGRID deve inviare i metadati degli oggetti. Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID.

Nome	Descrizione	Necessario
MetadatiNotificaConfigurazione	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione delle notifiche dei metadati. Contiene uno o più elementi Rule.	Sì
Regola	Tag contenitore 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 per la regola. Incluso nell'elemento Regola.	NO
Stato	Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilite. Incluso nell'elemento Regola.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata. Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Regola.	Sì
Destinazione	Tag contenitore per la destinazione di una regola. Incluso nell'elemento Regola.	Sì

Nome	Descrizione	Necessario
Urna	URN della destinazione a cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • <code>`es`</code> deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono archiviati i metadati, nel formato <code>domain-name/myindex/mytype</code>. Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma: • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404. L'urna è inclusa nell'elemento Destinazione.	Sì

Esempio di risposta

L'XML incluso tra

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags mostra come l'integrazione con un endpoint di integrazione della ricerca è configurata per il bucket. In questo esempio, i metadati dell'oggetto vengono inviati a un indice Elasticsearch denominato `current` e digitati denominato `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-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Informazioni correlate

["Utilizzare un account tenant"](#)

Configurazione della notifica dei metadati del bucket PUT

La richiesta di configurazione della notifica dei metadati del bucket PUT consente di abilitare il servizio di integrazione della ricerca per singoli bucket. Il codice 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 oppure essere l'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 a cui StorageGRID deve inviare i metadati degli oggetti.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, potresti inviare metadati per oggetti con il prefisso `/images` verso una destinazione e oggetti con il prefisso `/videos` all'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 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, altrimenti la richiesta fallisce come

400 Bad Request Il messaggio di errore afferma: 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 presenti nel file XML di configurazione delle notifiche dei metadati.

Nome	Descrizione	Necessario
MetadatiNotificaConfigurazione	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione delle notifiche dei metadati. Contiene uno o più elementi Rule.	Sì
Regola	Tag contenitore 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 per la regola. Incluso nell'elemento Regola.	NO
Stato	Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilite. Incluso nell'elemento Regola.	Sì

Nome	Descrizione	Necessario
Prefisso	Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata. Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Regola.	Sì
Destinazione	Tag contenitore per la destinazione di una regola. Incluso nell'elemento Regola.	Sì
Urna	URN della destinazione a 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 archiviati i metadati, nel formato <code>domain-name/myindex/mytype</code>. Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma: • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404. L'urna è inclusa nell'elemento Destinazione.	Sì

Esempi di richiesta

Questo esempio mostra come abilitare l'integrazione della ricerca per un bucket. In questo esempio, i metadati di 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, metadati degli oggetti per gli oggetti che corrispondono al prefisso `/images` viene inviato a una destinazione, mentre i metadati degli oggetti 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-1:33333333: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 abilita il servizio di integrazione della ricerca per un bucket, ogni volta che vengono aggiunti, aggiornati o eliminati metadati o tag di un oggetto, viene generato un documento JSON che viene inviato all'endpoint di destinazione.

Questo esempio mostra un esempio del JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. Il `test` il bucket non è sottoposto a `versioning`, quindi `versionId` il tag è 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

Nella tabella sono elencati tutti i campi inclusi nel documento JSON inviato all'endpoint di destinazione quando è abilitata 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'articolo	Descrizione
Informazioni su bucket e oggetti	secchio	Nome del bucket
Informazioni su bucket e oggetti	chiave	Nome chiave oggetto
Informazioni su bucket e oggetti	ID versione	Versione dell'oggetto, per gli oggetti nei bucket con versione
Informazioni su bucket e oggetti	regione	Regione del bucket, ad esempio us-east-1
Metadati di sistema	misurare	Dimensione dell'oggetto (in byte) visibile a un client HTTP
Metadati di sistema	md5	Hash dell'oggetto
Metadati utente	metadati <i>key:value</i>	Tutti i metadati utente per l'oggetto, come coppie chiave-valore
Etichette	etichette <i>key:value</i>	Tutti i tag oggetto definiti per l'oggetto, come coppie chiave-valore



Per i tag e i metadati utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo che interpreti queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per la mappatura dei formati di data. È necessario abilitare i mapping dei campi dinamici sull'indice prima di configurare il servizio di integrazione della ricerca. Dopo aver indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Informazioni correlate

["Utilizzare un account tenant"](#)

Richiesta di utilizzo dello spazio di archiviazione GET

La richiesta GET Storage Usage indica la quantità totale di spazio di archiviazione utilizzato da un account e per ciascun bucket associato all'account.

La quantità di spazio di archiviazione utilizzata da un account e dai suoi bucket può essere ottenuta tramite una richiesta ListBuckets modificata con `x-ntap-sg-usage` parametro di query. L'utilizzo dello spazio di archiviazione del bucket viene monitorato separatamente dalle richieste PUT e DELETE 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 elevato.

Per impostazione predefinita, StorageGRID tenta di recuperare le informazioni sull'utilizzo utilizzando la coerenza globale forte. Se non è possibile ottenere una coerenza globale forte, StorageGRID tenta di recuperare le informazioni sull'utilizzo con una coerenza del sito forte.

Per completare questa operazione è necessario disporre dell'autorizzazione `s3:ListAllMyBuckets` oppure essere l'account root.

Richiedi esempio

```
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>
```

Controllo delle versioni

Ogni versione dell'oggetto memorizzata contribuirà a `ObjectCount` E `DataBytes` valori nella risposta. I marcatori di eliminazione non vengono aggiunti al `ObjectCount` totale.

Informazioni correlate

["Valori di coerenza"](#)

Richieste di bucket deprecate per la conformità legacy

Richieste di bucket deprecate per la conformità legacy

Potrebbe essere necessario utilizzare l'API REST StorageGRID S3 per gestire i bucket creati utilizzando la funzionalità di conformità legacy.

Funzionalità di conformità deprecata

La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock.

Se in precedenza è stata abilitata l'impostazione Conformità globale, in StorageGRID 11.6 è abilitata l'impostazione Blocco oggetto S3 globale. Non è più possibile creare nuovi bucket con la conformità abilitata; tuttavia, se necessario, è possibile utilizzare l'API REST StorageGRID S3 per gestire eventuali bucket conformi legacy esistenti.

- ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#)
- ["Gestire gli oggetti con ILM"](#)
- ["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"](#)

Richieste di conformità deprecate:

- ["Obsoleto - Modifiche alla richiesta PUT Bucket per conformità"](#)

L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML facoltativo delle richieste PUT Bucket per creare un bucket conforme.

- ["Obsoleto - Conformità al bucket GET"](#)

La richiesta di conformità del bucket GET è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket Conforme legacy esistente.

- ["Obsoleto - Conformità al bucket PUT"](#)

La richiesta di conformità del bucket PUT è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket Conforme legacy esistente. Ad esempio, è possibile mettere in attesa per motivi legali un bucket esistente o aumentarne il periodo di conservazione.

Obsoleto: modifiche alla richiesta CreateBucket per conformità

L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML facoltativa delle richieste CreateBucket per creare un bucket conforme.



La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:

- ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#)
- ["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"](#)

Non è più possibile creare nuovi bucket con la Conformità abilitata. Se si tenta di utilizzare le modifiche alla richiesta CreateBucket per la conformità per creare un nuovo bucket conforme, viene restituito il seguente messaggio di errore:

```
The Compliance feature is deprecated.  
Contact your StorageGRID administrator if you need to create new Compliant  
buckets.
```

Obsoleto: richiesta di conformità del bucket GET

La richiesta di conformità del bucket GET è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket Conforme legacy esistente.



La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:

- ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#)
- ["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"](#)

Per completare questa operazione è necessario disporre dell'autorizzazione `s3:GetBucketCompliance` oppure essere l'account root.

Richiedi esempio

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 conformità in vigore per il bucket. Questa risposta di esempio mostra le impostazioni di conformità per un bucket in cui ogni oggetto verrà conservato per un anno (525.600 minuti), a partire dal momento in cui l'oggetto viene inserito nella griglia. Al momento non esiste alcun blocco legale su questo bucket. Ogni oggetto verrà automaticamente eliminato 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
Periodo di conservazioneMinuti	Durata del periodo di conservazione degli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene inserito nella griglia.
LegalHold	• Vero: questo bucket è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché non viene revocata la sospensione legale, anche se il periodo di conservazione è scaduto. • Falso: questo bucket non è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket possono essere eliminati alla scadenza del periodo di conservazione.
Eliminazione automatica	• Vero: gli oggetti in questo bucket verranno eliminati automaticamente alla scadenza del periodo di conservazione, a meno che il bucket non sia soggetto a conservazione legale. • Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Se vuoi eliminarli, devi eliminarli manualmente.

Risposte di errore

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 .

Obsoleto: richiesta di conformità del bucket PUT

La richiesta di conformità del bucket PUT è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket Conforme legacy esistente. Ad esempio, è possibile mettere in attesa per motivi legali un bucket esistente o aumentarne il periodo di conservazione.



La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:

- ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#)
- ["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"](#)

Per completare questa operazione è necessario disporre dell'autorizzazione s3:PutBucketCompliance oppure essere l'account root.

Quando si invia una richiesta di conformità del bucket PUT, è necessario specificare un valore per ogni campo delle impostazioni di conformità.

Richiedi esempio

Questa richiesta di esempio modifica le impostazioni di conformità per il bucket denominato `mybucket` . In questo esempio, gli oggetti in `mybucket` verranno ora conservati per due anni (1.051.200 minuti) anziché uno, a partire dal momento in cui l'oggetto viene inserito nella griglia. Non esiste alcun vincolo legale su questo

secchio. Ogni oggetto verrà automaticamente eliminato 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
Periodo di conservazioneMinuti	Durata del periodo di conservazione degli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene inserito nella griglia. Importante Quando si specifica un nuovo valore per <code>RetentionPeriodMinutes</code>, è necessario specificare un valore uguale o maggiore del periodo di conservazione corrente del bucket. Dopo aver impostato il periodo di conservazione del bucket, non è possibile diminuire tale valore; è possibile solo aumentarlo.
LegalHold	• Vero: questo bucket è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché non viene revocata la sospensione legale, anche se il periodo di conservazione è scaduto. • Falso: questo bucket non è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket possono essere eliminati alla scadenza del periodo di conservazione.
Eliminazione automatica	• Vero: gli oggetti in questo bucket verranno eliminati automaticamente alla scadenza del periodo di conservazione, a meno che il bucket non sia soggetto a conservazione legale. • Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Se vuoi eliminarli, devi eliminarli manualmente.

Coerenza per le impostazioni di conformità

Quando si aggiornano le impostazioni di conformità per un bucket S3 con una richiesta di conformità del bucket PUT, StorageGRID tenta di aggiornare i metadati del bucket in tutta la griglia. Per impostazione predefinita, StorageGRID utilizza la coerenza **Strong-global** per garantire che tutti i siti dei data center e tutti i nodi di archiviazione che contengono metadati dei 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 del 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 della rete per assicurarsi che i servizi di archiviazione richiesti siano resi disponibili il prima possibile. Se l'amministratore della rete non è in grado di rendere disponibili sufficienti nodi di archiviazione in ciascun sito, il supporto tecnico potrebbe consigliarti 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 ti sia stato chiesto di farlo dal supporto tecnico e a meno che tu non comprenda le potenziali conseguenze dell'utilizzo di questo livello.

Quando la coerenza viene ridotta a **Strong-site**, StorageGRID garantisce che le impostazioni di conformità aggiornate avranno coerenza di lettura dopo scrittura solo per le richieste client all'interno di un sito. Ciò significa che il sistema StorageGRID potrebbe avere temporaneamente più impostazioni incoerenti per questo bucket finché tutti i siti e i nodi di archiviazione non saranno disponibili. Impostazioni incoerenti possono dare luogo a comportamenti inaspettati e indesiderati. Ad esempio, se si sottopone un bucket a un blocco legale e si impone una minore coerenza, le precedenti impostazioni di conformità del bucket (ovvero il blocco legale) potrebbero continuare a essere valide in alcuni siti di data center. Di conseguenza, gli oggetti che ritieni siano in sospeso a fini legali potrebbero essere eliminati alla scadenza del periodo di conservazione, dall'utente o tramite l'eliminazione automatica, se abilitata.

Per forzare l'uso della coerenza **Strong-site**, rimettere la richiesta di conformità del bucket PUT e includere `Consistency-Control` Intestazione della richiesta HTTP, come segue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Risposte di errore

- Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è 404 `Not Found`.
- Se `RetentionPeriodMinutes` nella richiesta è inferiore al periodo di conservazione corrente del bucket, il codice di stato HTTP è 400 `Bad Request`.

Informazioni correlate

["Obsoleto: modifiche alla richiesta PUT Bucket per conformità"](#)

Criteri di accesso a bucket e gruppi

Utilizzare criteri 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 di policy dell'API REST S3. Le policy di accesso per l'API S3 sono scritte in JSON.

StorageGRID supporta due tipi di criteri di accesso.

- **Politiche bucket**, gestite tramite le operazioni API S3 GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy oppure tramite l'API Tenant Manager o Tenant Management. I criteri dei bucket sono associati ai bucket e sono quindi configurati per controllare l'accesso degli utenti nell'account proprietario del bucket o di altri account al bucket e agli oggetti in esso contenuti. Una policy basata su bucket si applica a un solo bucket e, possibilmente, a più gruppi.
- **Criteri di gruppo**, configurati tramite Tenant Manager o Tenant Management API. I criteri di gruppo sono associati a un gruppo nell'account e sono quindi configurati per consentire a tale gruppo di accedere a risorse specifiche di proprietà di tale account. Un criterio di gruppo si applica a un solo gruppo e, possibilmente, a più bucket.



Non vi è alcuna differenza di priorità tra i criteri di gruppo e quelli di bucket.

I criteri di gruppo e bucket StorageGRID seguono una grammatica specifica definita da Amazon. All'interno di ogni policy è presente una serie di dichiarazioni di policy e ciascuna dichiarazione contiene i seguenti elementi:

- ID dichiarazione (Sid) (facoltativo)
- Effetto
- Principale/Non Principale
- Risorsa/Non Risorsa
- Azione/Non azione
- Condizione (facoltativa)

Le istruzioni di policy vengono create utilizzando questa struttura per specificare le autorizzazioni: Concedi <Effetto> per consentire/negare a <Principale> di eseguire <Azione> su <Risorsa> quando si applica <Condizione>.

Ogni elemento della policy viene utilizzato per una funzione specifica:

Elemento	Descrizione
Sid	L'elemento Sid è facoltativo. Il Sid è inteso solo come descrizione per l'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID .
Effetto	Utilizzare l'elemento Effetto per stabilire se le operazioni specificate sono consentite o negate. È necessario identificare le operazioni consentite (o negate) sui bucket o sugli oggetti utilizzando le parole chiave dell'elemento Azione supportate.

Elemento	Descrizione
Principale/Non Principale	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 un criterio bucket. Per i criteri di gruppo, il gruppo a cui è associato il criterio è l'elemento Principal implicito.
Risorsa/Non Risorsa	L'elemento Risorsa identifica bucket e oggetti. È possibile concedere o negare autorizzazioni a bucket e oggetti utilizzando l'Amazon Resource Name (ARN) per identificare la risorsa.
Azione/Non azione	Gli elementi Azione ed Effetto 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 autorizzazioni specifiche, ma è possibile utilizzare la negazione esplicita per ignorare un'autorizzazione concessa da un altro criterio.
Condizione	L'elemento Condizione è facoltativo. Le condizioni consentono di creare espressioni per determinare quando applicare una policy.

Nell'elemento Azione, è possibile utilizzare il carattere jolly (*) per specificare tutte le operazioni o un sottoinsieme di operazioni. Ad esempio, questa azione corrisponde ad autorizzazioni quali `s3:GetObject`, `s3:PutObject` e `s3:DeleteObject`.

```
s3:*Object
```

Nell'elemento Risorsa 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, tranne che per impostare l'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, si imposta il carattere jolly (*) come valore Principale.

```
"Principal": ""
```

```
"Principal": {"AWS": ""}
```

Nell'esempio seguente, l'istruzione utilizza gli elementi Effetto, Principale, Azione e Risorsa. Questo esempio mostra un'istruzione completa della policy del bucket che utilizza l'effetto "Consenti" per fornire ai Principals, il gruppo di amministrazione `federated-group/admin` e il gruppo finanziario `federated-group/finance`, autorizzazioni per eseguire l'azione `s3:ListBucket` sul secchio denominato `mybucket` e l'azione `s3:GetObject` su tutti gli oggetti all'interno di quel contenitore.

```
{
  "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:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

Il criterio del bucket ha un limite di dimensione di 20.480 byte, mentre il criterio del gruppo ha un limite di dimensione di 5.120 byte.

Coerenza per le politiche

Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri di gruppo sono coerenti. Quando un criterio di gruppo diventa coerente, le modifiche potrebbero richiedere altri 15 minuti per diventare effettive, a causa della memorizzazione nella cache dei criteri. Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri dei bucket sono fortemente coerenti.

Se necessario, è possibile modificare le garanzie di coerenza per gli aggiornamenti dei criteri dei bucket. Ad esempio, potresti voler rendere disponibile una modifica ai criteri di un bucket durante un'interruzione del sito.

In questo caso, è possibile impostare il `Consistency-Control` intestazione nella richiesta `PutBucketPolicy` oppure puoi utilizzare la richiesta di coerenza `PUT Bucket`. Quando un criterio di bucket diventa coerente, le modifiche potrebbero richiedere altri 8 secondi per diventare effettive, a causa della memorizzazione nella cache dei criteri.



Se si imposta la coerenza su un valore diverso per risolvere una situazione temporanea, assicurarsi di ripristinare l'impostazione a livello di bucket al valore originale al termine dell'operazione. In caso contrario, tutte le future richieste di bucket utilizzeranno l'impostazione modificata.

Utilizzare ARN nelle dichiarazioni di policy

Nelle dichiarazioni di policy, l'ARN viene utilizzato negli elementi `Principal` e `Resource`.

- Utilizzare questa sintassi per specificare l'ARN della risorsa S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilizzare questa sintassi per specificare l'ARN della risorsa 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 trovare la corrispondenza con zero o più caratteri all'interno della chiave dell'oggetto.
- I caratteri internazionali, che possono essere specificati nella chiave dell'oggetto, devono essere codificati utilizzando JSON UTF-8 o sequenze di escape JSON \u. La codifica 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 una policy

Nelle istruzioni dei criteri, è possibile utilizzare l'elemento `Risorsa` per specificare il bucket o l'oggetto per cui sono concesse o negate le autorizzazioni.

- Ogni dichiarazione di policy richiede un elemento `Risorsa`. In una policy, le risorse sono indicate dall'elemento `Resource`, o in alternativa, `NotResource` per l'esclusione.
- È possibile specificare le risorse con un ARN di risorsa S3. Per esempio:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- È anche possibile utilizzare variabili di policy all'interno della chiave dell'oggetto. Per esempio:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- Il valore della risorsa può specificare un bucket che non esiste ancora al momento della creazione di un criterio di gruppo.

Specificare i principi in una policy

Utilizzare l'elemento `Principal` per identificare l'utente, il gruppo o l'account tenant a cui è consentito/negato

l'accesso alla risorsa in base all'istruzione di policy.

- Ogni istruzione di policy in una policy di bucket deve includere un elemento Principal. Le istruzioni di policy in un criterio di gruppo non necessitano dell'elemento Principal perché il gruppo è considerato il principale.
- In una policy, i mandanti sono indicati dall'elemento "Manager" o, in alternativa, "NotManager" 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 nell'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 un gruppo federato specifico ("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 dell'utente anziché il 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 eliminato. Se un nuovo Alex si unisce all'organizzazione e gli viene assegnato lo stesso Alex nome utente, il nuovo utente

potrebbe ereditare involontariamente i permessi concessi all'utente originale.

- Il valore principale può specificare un nome di gruppo/utente che non esiste ancora al momento della creazione di un criterio bucket.

Specificare le autorizzazioni in una policy

In una policy, l'elemento Azione viene utilizzato per concedere/negare le autorizzazioni a una risorsa. Esiste una serie di autorizzazioni che è possibile specificare in una policy, contrassegnate dall'elemento "Azione" o, in alternativa, "NonAzione" per l'esclusione. Ciascuno di questi elementi è mappato a specifiche operazioni dell'API REST S3.

Nelle tabelle sono elencate le autorizzazioni che si applicano ai bucket e le autorizzazioni che si applicano agli oggetti.



Amazon S3 ora utilizza l'autorizzazione s3:PutReplicationConfiguration per entrambe le azioni PutBucketReplication e DeleteBucketReplication. StorageGRID utilizza autorizzazioni separate per ogni azione, in linea con le specifiche originali di Amazon S3.



Un'operazione di eliminazione viene eseguita quando si utilizza un'istruzione put per sovrascrivere un valore esistente.

Autorizzazioni applicabili ai bucket

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:CreaBucket	CreaBucket	Sì. Nota: utilizzare solo nei criteri di gruppo.
s3:EliminaBucket	EliminaBucket	
s3>DeleteBucketMetadataNotification	ELIMINA la configurazione della notifica dei metadati del bucket	Sì
s3:EliminaBucketPolicy	DeleteBucketPolicy	
s3:EliminaConfigurazioneReplicazione	DeleteBucketReplication	Sì, autorizzazioni separate per PUT e DELETE
s3:GetBucketAcl	OttieniBucketAcl	
s3:GetBucketCompliance	Conformità GET Bucket (obsoleto)	Sì
s3:GetBucketConsistency	OTTIENI la coerenza del bucket	Sì
s3:GetBucketCORS	GetBucketCors	

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:Ottieni configurazione crittografia	Ottieni crittografia dei bucket	
s3:GetBucketLastAccessTime	GET Ora dell'ultimo accesso al bucket	Sì
s3:OttieniPosizioneBucket	OttieniPosizioneBucket	
s3:GetBucketMetadataNotification	Configurazione della notifica dei metadati del bucket GET	Sì
s3:OttieniNotificaBucket	Configurazione di notifica di GetBucket	
s3:GetBucketObjectLockConfiguration	Ottieni configurazione blocco oggetto	
s3:GetBucketPolicy	OttieniPoliticaBucket	
s3:OttieniTaggingBucket	OttieniBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:OttieniConfigurazioneReplicazione	OttieniReplicazioneBucket	
s3:ElencaTuttiIBucket	- ListBuckets - Utilizzo dello spazio di archiviazione GET	Sì, per l'utilizzo dello spazio di archiviazione GET. Nota: utilizzare solo nei criteri di gruppo.
s3:ElencoBucket	- ElencoOggetti - HeadBucket - Ripristina oggetto	
s3:ListBucketMultipartUploads	- Caricamenti multipart di List - Ripristina oggetto	
s3:ListBucketVersions	Versioni GET Bucket	
s3:PutBucketCompliance	Conformità al bucket PUT (obsoleto)	Sì
s3:PutBucketConsistency	PUT Consistenza del secchio	Sì

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:PutBucketCORS	- DeleteBucketCors† - PutBucketCors	
s3:PutEncryptionConfiguration	- DeleteBucketEncryption - PutBucketEncryption	
s3:PutBucketLastAccessTime	Ora dell'ultimo accesso al bucket PUT	Sì
s3:PutBucketMetadataNotification	Configurazione della notifica dei metadati del bucket PUT	Sì
s3:PutBucketNotification	Configurazione della notifica PutBucket	
s3:PutBucketObjectLockConfiguration	- CreateBucket con il <code>x-amz-bucket-object-lock-enabled: true</code> intestazione della richiesta (richiede anche l'autorizzazione s3:CreateBucket) - PutObjectLockConfiguration	
s3:PoliticaPutBucket	PutBucketPolicy	
s3:PutBucketTagging	- EliminaBucketTagging† - PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	- DeleteBucketLifecycle† - Configurazione del ciclo di vita di PutBucket	
s3:PutReplicationConfiguration	PutBucketReplication	Sì, autorizzazioni separate per PUT e DELETE

Autorizzazioni applicabili agli oggetti

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:AnnullaCaricamentoMultipart	- Annulla caricamento multiparte - Ripristina oggetto	

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:BypassGovernanceRetention	- EliminaOggetto - EliminaOggetti - PutObjectRetention	
s3:EliminaOggetto	- EliminaOggetto - EliminaOggetti - Ripristina oggetto	
s3:EliminaTaggingOggetto	DeleteObjectTagging	
s3:EliminaObjectVersionTagging	DeleteObjectTagging (una versione specifica dell'oggetto)	
s3:EliminaVersioneOggetto	DeleteObject (una versione specifica dell'oggetto)	
s3:OttieniOggetto	- OttieniOggetto - HeadObject - Ripristina oggetto - SelezionaOggettoContenuto	
s3:GetObjectAcl	OttieniOggettoAcl	
s3:GetObjectLegalHold	OttieniOggettoLegaleHold	
s3:OttieniRitenzioneOggetto	Ottieni conservazione oggetto	
s3:OttieniTaggingOggetto	OttieniTaggingOggetto	
s3:GetObjectVersionTagging	GetObjectTagging (una versione specifica dell'oggetto)	
s3:GetObjectVersion	GetObject (una versione specifica dell'oggetto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:PutObject	• MettiOggetto • CopiaOggetto • Ripristina oggetto • CreaCaricamentoMultiparte • Caricamento multiparte completo • CaricaParte • CaricaParteCopia	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (una versione specifica dell'oggetto)	
s3:PutOverwriteObject	• MettiOggetto • CopiaOggetto • PutObjectTagging • DeleteObjectTagging • Caricamento multiparte completo	Sì
s3:RipristinaOggetto	Ripristina oggetto	

Utilizzare 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 possibili impostazioni per questa autorizzazione includono:

- **Consenti:** il client può sovrascrivere un oggetto. Questa è l'impostazione predefinita.
- **Nega:** Il client non può sovrascrivere un oggetto. Se impostato 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 i tag degli oggetti S3 non possono essere sovrascritti.
 - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
 - Se è abilitato il controllo delle versioni S3, l'impostazione Nega impedisce alle operazioni

PutObjectTagging o DeleteObjectTagging di modificare il TagSet per un oggetto e le sue 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 che si avrebbe se fosse impostato Consenti.



Se l'attuale policy S3 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 i tag degli oggetti. Inoltre, se è selezionata la casella di controllo **Impedisci modifica client** (**CONFIGURAZIONE > Impostazioni di sicurezza > Rete e oggetti**), tale impostazione sostituisce l'impostazione dell'autorizzazione PutOverwriteObject.

Specificare le condizioni in una policy

Le condizioni definiscono quando una politica entrerà in vigore. Le condizioni sono costituite da operatori e coppie chiave-valore.

Le condizioni utilizzano coppie chiave-valore per la valutazione. Un elemento Condizione può contenere più condizioni e ogni condizione può contenere più coppie chiave-valore. Il blocco di condizione utilizza il seguente formato:

```
Condition: {  
  condition_type: {  
    condition_key: condition_values
```

Nell'esempio seguente, la condizione IpAddress utilizza la chiave di condizione SourceIp.

```
"Condition": {  
  "IpAddress": {  
    "aws:SourceIp": "54.240.143.0/24"  
    ...  
  },  
  ...
```

Operatori di condizione supportati

Gli operatori condizionali sono classificati come segue:

- Corda
- Numerico
- Booleano
- indirizzo IP
- Controllo nullo

Operatori di condizione	Descrizione
StringEquals	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (con distinzione tra maiuscole e minuscole).
Stringa non uguale	Confronta una chiave con un valore stringa in base alla corrispondenza negata (sensibile alle maiuscole e alle minuscole).
StringEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora la distinzione tra maiuscole e minuscole).
StringNotEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza negata (ignora la distinzione tra maiuscole e minuscole).
StringLike	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (con distinzione tra maiuscole e minuscole). Può includere i caratteri jolly * e ?.
Stringa non piace	Confronta una chiave con un valore stringa in base alla corrispondenza negata (sensibile alle maiuscole e alle minuscole). Può includere i caratteri jolly * e ?.
NumericEquals	Confronta una chiave con un valore numerico in base alla corrispondenza esatta.
NumericoNonUguale	Confronta una chiave con un valore numerico in base alla corrispondenza negata.
NumericoMaggioreDi	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore di".
NumericoMaggioreDiUguale	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore o uguale a".
NumericoMenoDi	Confronta una chiave con un valore numerico in base alla corrispondenza "minore di".
NumericoMinoreUguale	Confronta una chiave con un valore numerico in base alla corrispondenza "minore o uguale".
Bool	Confronta una chiave con un valore booleano in base alla corrispondenza "vero o falso".
Indirizzo IP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP.
NonIndirizzoIP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata.

Operatori di condizione	Descrizione
Nulla	Controlla se una chiave di condizione è presente nel contesto della richiesta corrente.

Chiavi di condizione supportate

Chiavi di condizione	Azioni	Descrizione
aws:SourceIp	operatori IP	Verrà confrontato con l'indirizzo IP da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti. Nota: se la richiesta S3 è stata inviata tramite il servizio Load Balancer sui nodi amministrativi e sui nodi gateway, questa verrà confrontata con l'indirizzo IP a monte del servizio Load Balancer. Nota: se viene utilizzato un bilanciatore del carico di terze parti non trasparente, questo verrà confrontato con l'indirizzo IP di tale bilanciatore del carico. Qualunque X-Forwarded-For l'intestazione verrà ignorata perché non è possibile accertarne la validità.
aws:nome utente	Risorsa/Identità	Verrà confrontato con il nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti.
s3:delimiter	s3:ListBucket e s3:permessi ListBucketVersions	Verrà confrontato con il parametro delimitatore specificato in una richiesta ListObjects o ListObjectVersions.

Chiavi di condizione	Azioni	Descrizione
s3:ExistingObjectTag/<chiave-tag>	s3:EliminaTaggingOggetto s3:EliminaObjectVersionTagging s3:OttieniOggetto s3:GetObjectAcl 3: Ottieni tag oggetto s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Richiederà che l'oggetto esistente abbia la chiave e il valore del tag specifici.
s3:max-chiavi	s3:ListBucket e s3:permessi ListBucketVersions	Verrà confrontato con il parametro max-keys specificato in una richiesta ListObjects o ListObjectVersions.
s3:giorni di conservazione rimanenti del blocco dell'oggetto	s3:PutObject	Confronta con la data di conservazione specificata in <code>x-amz-object-lock-retain-until-date</code> intestazione della richiesta o calcolata dal periodo di conservazione predefinito del bucket per assicurarsi che questi valori siano compresi nell'intervallo consentito per le seguenti richieste: • MettiOggetto • CopiaOggetto • CreaCaricamentoMultiparte
s3:giorni di conservazione rimanenti del blocco dell'oggetto	s3:PutObjectRetention	Confronta con la <code>retain-until-date</code> specificata nella richiesta PutObjectRetention per garantire che rientri nell'intervallo consentito.

Chiavi di condizione	Azioni	Descrizione
s3:prefisso	s3:ListBucket e s3:permessi ListBucketVersions	Verrà confrontato con il parametro prefisso specificato in una richiesta ListObjects o ListObjectVersions.
s3:RequestObjectTag/<chiave-tag>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Richiederà una chiave e un valore tag specifici quando la richiesta dell'oggetto include il tagging.

Specificare le variabili in una policy

È possibile utilizzare le variabili nelle policy per popolare le informazioni sulle policy quando sono disponibili. È possibile utilizzare le variabili di policy in `Resource` elemento e nei confronti di stringhe in `Condition` elemento.

In questo esempio, la variabile `${aws:username}` fa parte dell'elemento `Risorsa`:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In questo esempio, la variabile `${aws:username}` fa parte del valore della condizione nel blocco di condizioni:

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

Variabile	Descrizione
<code>\${aws:SourceIp}</code>	Utilizza la chiave <code>SourceIp</code> come variabile fornita.
<code>\${aws:username}</code>	Utilizza la chiave nome utente come variabile fornita.
<code>\${s3:prefix}</code>	Utilizza la chiave del prefisso specifico del servizio come variabile fornita.
<code>\${s3:max-keys}</code>	Utilizza la chiave <code>max-keys</code> specifica del servizio come variabile fornita.

Variabile	Descrizione
\$ { * }	Carattere speciale. Utilizza il carattere come carattere letterale *.
\$ { ? }	Carattere speciale. Utilizza il carattere come carattere ? letterale.
\$ { \$ }	Carattere speciale. Utilizza il carattere come carattere \$ letterale.

Creare politiche che richiedono una gestione speciale

Talvolta una policy può concedere autorizzazioni pericolose per la sicurezza o per il proseguimento delle operazioni, ad esempio bloccando l'utente root dell'account. L'implementazione dell'API REST S3 StorageGRID è meno restrittiva durante la convalida delle policy rispetto ad Amazon, ma altrettanto rigorosa durante la valutazione delle policy.

Descrizione della politica	Tipo di polizza	Comportamento di Amazon	Comportamento StorageGRID
Nega a te stesso qualsiasi autorizzazione all'account root	Secchio	Valido e applicato, ma l'account utente root mantiene l'autorizzazione per tutte le operazioni dei criteri del bucket S3	Stesso
Nega a te stesso qualsiasi autorizzazione all'utente/gruppo	Gruppo	Valido e applicato	Stesso
Consentire qualsiasi autorizzazione a un gruppo di account esteri	Secchio	Principale non valido	Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito quando consentito da una policy
Consentire a un account esterno root o utente qualsiasi autorizzazione	Secchio	Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito quando consentito da una policy	Stesso

Descrizione della politica	Tipo di polizza	Comportamento di Amazon	Comportamento StorageGRID
Consenti a tutti i permessi per tutte le azioni	Secchio	Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito per l'account esterno root e gli utenti	Stesso
Nega a tutti i permessi per tutte le azioni	Secchio	Valido e applicato, ma l'account utente root mantiene l'autorizzazione per tutte le operazioni dei criteri del bucket S3	Stesso
Il principale è un utente o un gruppo inesistente	Secchio	Principale non valido	Valido
La risorsa è un bucket S3 inesistente	Gruppo	Valido	Stesso
Principal è un gruppo locale	Secchio	Principale non valido	Valido
La policy concede a un account non proprietario (inclusi gli account anonimi) l'autorizzazione a inserire oggetti.	Secchio	Valido. Gli oggetti sono di proprietà dell'account del creatore e la policy del bucket non si applica. L'account del creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL degli oggetti.	Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la politica dei 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. È possibile configurare i bucket WORM per consentire la creazione di nuovi oggetti e impedire la sovrascrittura o l'eliminazione di contenuti esistenti. Utilizzare uno degli approcci descritti qui.

Per garantire che le sovrascritture vengano sempre negate, puoi:

- Da Grid Manager, vai su **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza > Rete e oggetti** e seleziona la casella di controllo **Impedisci modifiche client**.
- Applicare le seguenti regole e policy S3:
 - Aggiungere un'operazione PutOverwriteObject DENY al criterio S3.
 - Aggiungere un'operazione DeleteObject DENY al criterio S3.
 - Aggiungere un'operazione PutObject ALLOW al criterio S3.



L'impostazione di DeleteObject su DENY in un criterio S3 non impedisce a ILM di eliminare oggetti quando esiste una regola come "zero copie dopo 30 giorni".



Anche quando vengono applicate tutte queste regole e policy, non proteggono dalle scritture simultanee (vedere Situazione A). 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 (protette contro)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

Informazioni correlate

- ["Come le regole StorageGRID ILM gestiscono gli oggetti"](#)
- ["Criteri di esempio per i bucket"](#)
- ["Criteri di gruppo di esempio"](#)
- ["Gestire gli oggetti con ILM"](#)
- ["Utilizzare un account tenant"](#)

Criteri di esempio per i bucket

Utilizzare gli esempi in questa sezione per creare policy di accesso StorageGRID per i bucket.

I criteri dei bucket specificano le autorizzazioni di accesso per il bucket a cui è associato il criterio. È possibile configurare un criterio bucket utilizzando l'API S3 PutBucketPolicy tramite uno di questi strumenti:

- ["Responsabile degli inquilini"](#) .
- AWS CLI utilizzando questo comando (fare riferimento a ["Operazioni sui bucket"](#)):

```
> 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 l'utente anonimo, è consentito elencare gli oggetti nel bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket. Tutte le altre operazioni saranno negate. Si noti che questa policy potrebbe non essere particolarmente utile perché nessuno, eccetto l'account root, ha i permessi per

scrivere 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 di elencare il bucket ed eseguire operazioni `GetObject` sugli oggetti nel bucket a partire da `shared/` prefisso della chiave dell'oggetto.



In StorageGRID, gli oggetti creati da un account non proprietario (inclusi gli account anonimi) sono di proprietà dell'account proprietario del bucket. A questi oggetti si applica la policy bucket.

```

{
  "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 al gruppo specificato

In questo esempio, a tutti, incluso l'utente anonimo, è consentito elencare il bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket, mentre solo gli utenti appartenenti 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 è nell'intervallo IP

In questo esempio, a tutti, compresi gli utenti anonimi, è consentito elencare il bucket ed eseguire qualsiasi operazione sugli oggetti 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 negate e tutte le richieste al di fuori dell'intervallo IP verranno negate.


```

{
  "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 a un utente federato specificato

In questo esempio, all'utente federato Alex è consentito l'accesso completo a `examplebucket` secchio e i suoi oggetti. A tutti gli altri utenti, compreso 'root', viene esplicitamente negata qualsiasi operazione. Si noti tuttavia che a 'root' non vengono mai negati i permessi 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` L'effetto di `PutOverwriteObject` e `DeleteObject` garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e il tagging dell'oggetto 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 in 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 nella politica perché è implicito. I criteri di gruppo vengono configurati tramite Tenant Manager o API.

Esempio: impostare i criteri di gruppo utilizzando Tenant Manager

Quando aggiungi o modifichi un gruppo in Tenant Manager, puoi selezionare un criterio 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 venga concesso tramite un criterio bucket. Se si seleziona questa opzione, per impostazione predefinita solo l'utente root avrà accesso alle risorse S3.
- **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 oggetti e leggere dati, metadati e tag degli oggetti. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Non puoi 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 con accesso completo. Non puoi modificare questa stringa.
- **Mitigazione del ransomware:** 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 definitivamente gli oggetti dai bucket in cui è abilitato il controllo delle versioni degli oggetti.

Gli utenti Tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono ignorare questo criterio di gruppo. Limitare l'autorizzazione Gestisci tutti i bucket agli utenti attendibili e utilizzare l'autenticazione a più fattori (MFA) laddove disponibile.

- **Personalizzato:** agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

Esempio: consentire al gruppo l'accesso completo 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 venga esplicitamente negato dalla policy del bucket.

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

Esempio: consentire al gruppo l'accesso 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 venga esplicitamente negato dai criteri del bucket. Ad esempio, gli utenti di questo gruppo possono elencare oggetti e leggere dati, metadati e tag degli oggetti.

```

{
  "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: consentire ai membri del gruppo l'accesso completo solo alla loro "cartella" in un bucket

In questo esempio, ai membri del gruppo è consentito solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato. Si noti che quando si determina la privacy di queste cartelle, è necessario prendere in considerazione le autorizzazioni di accesso provenienti da altri criteri di gruppo e dai criteri del bucket.

```
{
  "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 tracciate nei registri di controllo

I messaggi di controllo vengono generati dai servizi StorageGRID e archiviati in file di registro di testo. È possibile esaminare i messaggi di controllo specifici di S3 nel registro di controllo per ottenere dettagli sulle operazioni di bucket e oggetti.

Operazioni del bucket monitorate nei log di controllo

- CreaBucket
- EliminaBucket
- DeleteBucketTagging
- EliminaOggetti
- OttieniBucketTagging
- HeadBucket
- ElencoOggetti
- ListObjectVersions
- Conformità del bucket PUT
- PutBucketTagging
- PutBucketVersioning

Operazioni sugli oggetti tracciate nei registri di controllo

- Caricamento multiparte completo
- CopiaOggetto
- EliminaOggetto
- OttieniOggetto
- HeadObject
- MettiOggetto
- Ripristina oggetto
- SelezionaOggetto
- UploadPart (quando una regola ILM utilizza l'acquisizione bilanciata o rigorosa)
- UploadPartCopy (quando una regola ILM utilizza l'acquisizione bilanciata o rigorosa)

Informazioni correlate

- ["Accedi al file di registro di controllo"](#)
- ["Il cliente scrive messaggi di audit"](#)
- ["Il cliente ha letto i messaggi di controllo"](#)

Utilizzare Swift REST API (fine del ciclo di vita)

Utilizzare Swift REST API

Il supporto per l'API Swift ha raggiunto la fine del suo ciclo di vita e verrà rimosso in una versione futura.



I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere ["StorageGRID 11.8: utilizzare Swift REST API"](#).

Monitorare e risolvere i problemi di un sistema StorageGRID

Monitorare il sistema StorageGRID

Monitorare un sistema StorageGRID

Monitora regolarmente il tuo sistema StorageGRID per assicurarti che funzioni come previsto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .



Per modificare le unità di misura per i valori di archiviazione visualizzati in Grid Manager, selezionare il menu a discesa dell'utente in alto a destra di Grid Manager, quindi selezionare **Preferenze utente**.

Informazioni su questo compito

Queste istruzioni descrivono come:

- ["Visualizza e gestisci la dashboard"](#)
- ["Visualizza la pagina Nodi"](#)
- ["Monitorare regolarmente questi aspetti del sistema:"](#)
 - ["Salute del sistema"](#)
 - ["Capacità di stoccaggio"](#)
 - ["Gestione del ciclo di vita delle informazioni"](#)
 - ["Risorse di rete e di sistema"](#)
 - ["Attività degli inquilini"](#)
 - ["Operazioni di bilanciamento del carico"](#)
 - ["Connessioni di federazione della rete"](#)
- ["Gestisci gli avvisi"](#)
- ["Visualizza i file di registro"](#)
- ["Configurare i messaggi di controllo e le destinazioni dei registri"](#)
- ["Utilizzare un server syslog esterno"](#) per raccogliere informazioni di audit
- ["Utilizzare SNMP per il monitoraggio"](#)
- ["Ottieni dati StorageGRID aggiuntivi"](#), comprese metriche e diagnostica

Visualizza e gestisci la dashboard

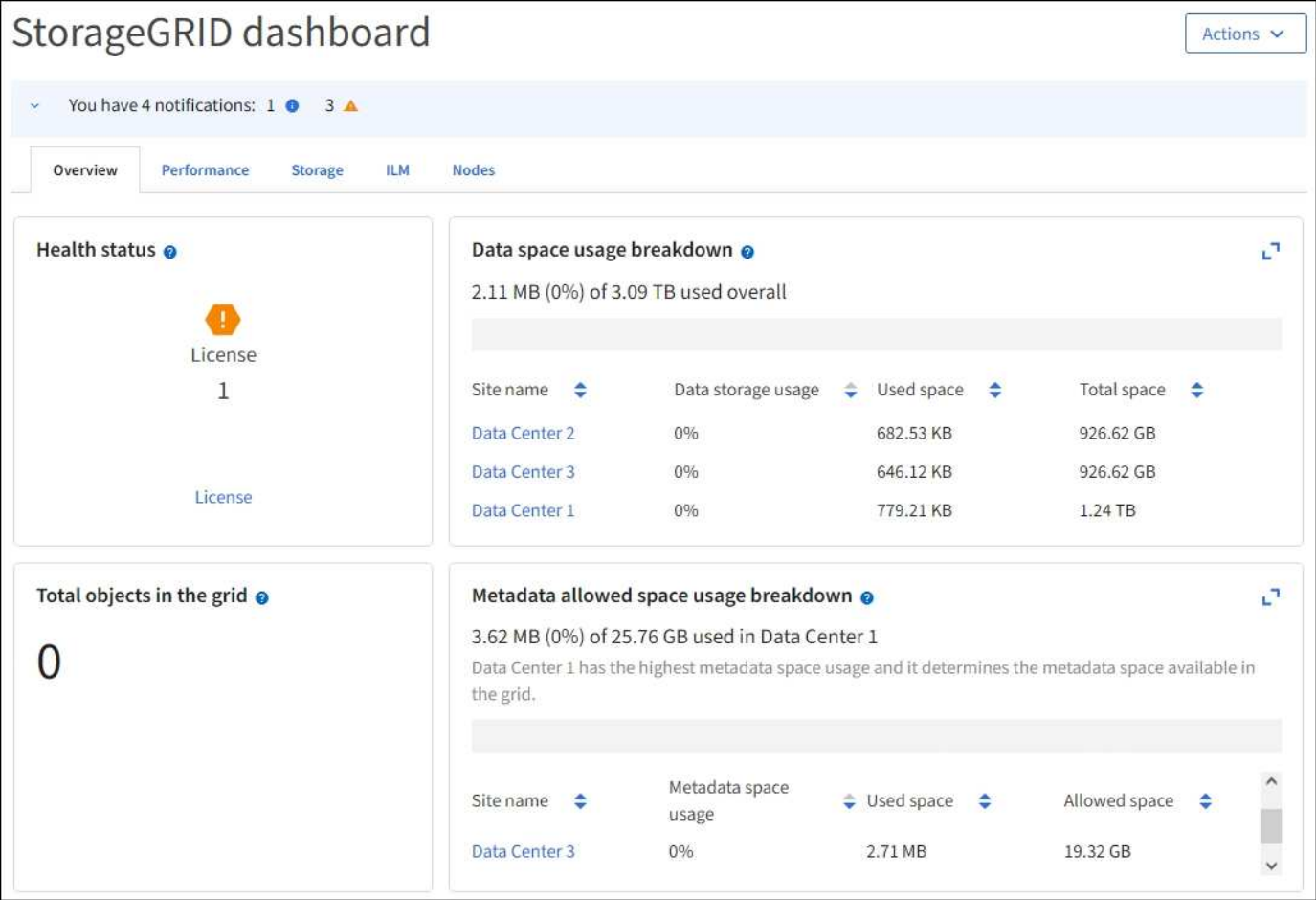
È possibile utilizzare la dashboard per monitorare a colpo d'occhio le attività del sistema. È possibile creare dashboard personalizzate per monitorare l'implementazione di

StorageGRID.



Per modificare le unità di misura per i valori di archiviazione visualizzati in Grid Manager, selezionare il menu a discesa dell'utente in alto a destra di Grid Manager, quindi selezionare **Preferenze utente**.

La dashboard potrebbe variare in base alla configurazione del sistema.



Visualizza la dashboard

La dashboard è composta da schede che contengono informazioni specifiche sul sistema StorageGRID . Ogni scheda contiene categorie di informazioni visualizzate sulle schede.

È possibile utilizzare la dashboard fornita dal sistema così com'è. Inoltre, è possibile creare dashboard personalizzate contenenti solo le schede e le 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, come avvisi attivi, utilizzo dello spazio e numero totale di oggetti nella griglia.

Scheda sulla dashboard fornita dal sistema	Contiene
Prestazione	Utilizzo dello spazio, spazio di archiviazione utilizzato nel tempo, operazioni S3, durata della richiesta, tasso di errore.
Magazzinaggio	Utilizzo delle quote dei tenant e utilizzo dello spazio logico. Previsioni sull'utilizzo dello spazio per i dati e i metadati degli utenti.
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 per nodo. Distribuzione dal nodo al sito.

Alcune schede possono essere ingrandite per una visualizzazione più semplice. Seleziona l'icona di massimizzazione  nell'angolo in alto a destra della carta. Per chiudere una scheda ingrandita, seleziona l'icona di riduzione a icona  oppure seleziona **Chiudi**.

Gestire i dashboard

Se hai accesso Root (vedi "[Autorizzazioni del gruppo amministratore](#)"), è possibile eseguire le seguenti attività di gestione per i dashboard:

- Crea una dashboard personalizzata da zero. È possibile utilizzare dashboard personalizzate per controllare quali informazioni StorageGRID vengono visualizzate e come vengono organizzate.
- Clona una dashboard per creare dashboard personalizzate.
- Imposta una dashboard attiva per un utente. La dashboard attiva può essere quella fornita dal sistema o una dashboard personalizzata.
- Imposta una dashboard predefinita, che è quella che tutti gli utenti vedono a meno che non attivino la propria dashboard.
- Modifica il nome di una dashboard.
- Modifica una dashboard per aggiungere o rimuovere schede e schede. Puoi avere un minimo di 1 e un massimo di 20 schede.
- Rimuovere un cruscotto.



Se si dispone di altri permessi oltre all'accesso Root, è possibile impostare solo una dashboard attiva.

Per gestire le dashboard, seleziona **Azioni > Gestisci dashboard**.



Configurare i dashboard

Per creare una nuova dashboard clonando la dashboard attiva, seleziona **Azioni > Clona dashboard attiva**.

Per modificare o clonare una dashboard esistente, seleziona **Azioni > Gestisci dashboard**.



La dashboard fornita dal sistema non può essere modificata o rimossa.

Quando si configura una dashboard, è possibile:

- Aggiungere o rimuovere schede
- Rinomina le schede e assegna nomi univoci alle nuove schede
- Aggiungi, rimuovi o riorganizza (trascina) le schede per ogni scheda
- Seleziona la dimensione delle singole carte selezionando **S**, **M**, **L** o **XL** nella parte superiore della carta

Site name	Data storage usage	Used space	Total space
Data Center 1	0%	1.79 MB	1.24 TB
Data Center 2	0%	921.11 KB	926.62 GB
Data Center 3	0%	790.21 KB	926.62 GB

Visualizza la pagina Nodi

Visualizza la pagina Nodi

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

Nella tabella Nodi sono elencate le informazioni riepilogative per l'intera griglia, per ciascun sito e per ciascun nodo. Se un nodo è disconnesso o ha un avviso attivo, accanto al nome del nodo viene visualizzata un'icona. Se il nodo è connesso e non ha avvisi attivi, non viene visualizzata alcuna icona.



Quando un nodo non è connesso alla rete, ad esempio durante un aggiornamento o in uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della rete. Dopo che un nodo si è ricollegato alla rete, attendere alcuni minuti affinché i valori si stabilizzino.



Per modificare le unità di misura per i valori di archiviazione visualizzati in Grid Manager, selezionare il menu a discesa dell'utente in alto a destra di Grid Manager, quindi selezionare **Preferenze utente**.



Gli screenshot mostrati sono esempi. I risultati potrebbero variare a seconda della versione StorageGRID .

Nodes

View the list and status of sites and grid nodes.

Total node count: 12

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

Icone dello stato della connessione

Se un nodo è disconnesso dalla rete, accanto al nome del nodo viene visualizzata una delle seguenti icone.

Icona	Descrizione	Azione richiesta
	Non connesso - Sconosciuto Per un motivo sconosciuto, un nodo è disconnesso oppure i servizi sul nodo sono inaspettatamente inattivi. Ad esempio, un servizio sul nodo potrebbe essere interrotto oppure il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione di corrente o di un'interruzione imprevista. Potrebbe anche essere attivato l'avviso Impossibile comunicare con il nodo. Potrebbero essere attivi anche altri avvisi.	Richiede attenzione immediata. "Seleziona ogni avviso" e seguire le azioni consigliate. Ad esempio, potrebbe essere necessario riavviare un servizio che si è arrestato o riavviare l'host per il nodo. Nota: un nodo potrebbe apparire come Sconosciuto durante le operazioni di arresto gestito. In questi casi è possibile ignorare lo stato Sconosciuto.
	Non connesso - Amministrativamente inattivo Per un motivo prevedibile, il nodo non è connesso alla griglia. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi. In base al problema di fondo, questi nodi spesso tornano online senza alcun intervento.	Determina se ci sono avvisi che interessano questo nodo. Se uno o più avvisi sono attivi, "Seleziona ogni avviso" e seguire le azioni consigliate.

Se un nodo è disconnesso dalla rete, potrebbe essere visualizzato un avviso sottostante, ma viene visualizzata solo l'icona "Non connesso". Per visualizzare gli avvisi attivi per un nodo, seleziona 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 è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. Bisogna affrontare immediatamente il problema di fondo. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.

 **Grave:** Esiste una condizione anomala che sta influenzando le operazioni in corso o che si sta avvicinando alla soglia di un avviso critico. È necessario esaminare gli avvisi principali e risolvere eventuali problemi sottostanti per garantire che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID.

 **Minore:** Il sistema funziona normalmente, ma si verifica una condizione anomala che potrebbe compromettere la capacità del sistema di funzionare se continua a verificarsi tale condizione. È opportuno monitorare e risolvere gli avvisi minori che non si risolvono da soli, per evitare che diano origine a problemi più seri.

Visualizza i dettagli di un sistema, sito o nodo

Per filtrare le informazioni mostrate nella tabella Nodi, immettere una stringa di ricerca nel campo **Cerca**. È possibile effettuare la ricerca per nome del sistema, nome visualizzato o tipo (ad esempio, immettere **gat** per individuare rapidamente tutti i nodi gateway).

Per visualizzare le informazioni sulla griglia, sul sito o sul nodo:

- Selezionare il nome della griglia per visualizzare un riepilogo aggregato delle statistiche dell'intero sistema StorageGRID .
- Seleziona un sito specifico del data center per visualizzare un riepilogo aggregato delle statistiche per tutti i nodi di quel sito.
- Seleziona un nodo specifico per visualizzare informazioni dettagliate su quel nodo.

Visualizza la scheda Panoramica

La scheda Panoramica fornisce informazioni di base su ciascun nodo. Mostra anche tutti gli avvisi che interessano attualmente il nodo.

La scheda Panoramica viene visualizzata per tutti i nodi.

Informazioni sul nodo

La sezione Informazioni sul nodo della scheda Panoramica elenca le informazioni di base sul nodo.

NYC-ADM1 (Primary Admin Node) [🔗](#)

Overview

Hardware

Network

Storage

Load balancer

Tasks

Node information [?](#)

Display name:	NYC-ADM1
System name:	DC1-ADM1
Type:	Primary Admin Node
ID:	3adb1aa8-9c7a-4901-8074-47054aa06ae6
Connection state:	✔ Connected
Software version:	11.7.0
IP addresses:	10.96.105.85 - eth0 (Grid Network)
Show additional IP addresses ▼	

Le informazioni generali per un nodo includono quanto segue:

- **Nome visualizzato** (mostrato solo se il nodo è stato rinominato): il nome visualizzato corrente per il nodo. Utilizzare il "[Rinomina griglia, siti e nodi](#)" procedura per aggiornare questo valore.
- **Nome del sistema**: il nome immesso per il nodo durante l'installazione. I nomi di sistema vengono utilizzati per le operazioni interne StorageGRID e non possono essere modificati.
- **Tipo**: il tipo di nodo: nodo amministrativo, nodo amministrativo primario, nodo di archiviazione o nodo gateway.
- **ID**: Identificatore univoco del nodo, noto anche come UUID.
- **Stato della connessione**: uno dei tre stati. Viene mostrata l'icona per lo stato più grave.

- **Sconosciuto* ** : Per un motivo sconosciuto, il nodo non è connesso alla rete oppure uno o più servizi sono inaspettatamente inattivi. Ad esempio, la connessione di rete tra i nodi è stata interrotta, l'alimentazione è interrotta o un servizio non è disponibile. Potrebbe anche essere attivato 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 arresto gestito. In questi casi è possibile ignorare lo stato Sconosciuto.

- ***Amministrativamente inattivo* ** : Il nodo non è connesso alla rete per un motivo prevedibile. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.

- ***Collegato* ** : Il nodo è connesso alla rete.

- **Archiviazione utilizzata**: solo per nodi di archiviazione.
 - **Dati oggetto**: percentuale dello spazio totale utilizzabile per i dati oggetto che è stato utilizzato sul nodo di archiviazione.
 - **Metadati oggetto**: percentuale dello spazio totale consentito per i metadati oggetto utilizzato sul nodo di archiviazione.
- **Versione software**: la versione di StorageGRID installata sul nodo.
- **Gruppi HA**: solo per nodi amministrativi e nodi gateway. Viene mostrato 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 **Mostra indirizzi IP aggiuntivi** per visualizzare gli indirizzi IPv4 e IPv6 del nodo e le mappature delle interfacce.

Avvisi

La sezione Avvisi della scheda Panoramica elenca tutti gli "[avvisi che attualmente interessano questo nodo e che non sono stati silenziati](#)". Selezionare il nome dell'avviso per visualizzare ulteriori dettagli e azioni consigliate.

Alerts

Alert name	Severity	Time triggered	Current values
Low installed node memory	✖ Critical	11 hours ago	Total RAM size: 8.37 GB
The amount of installed memory on a node is low.			

Sono inclusi anche gli avvisi per "stati di connessione del nodo".

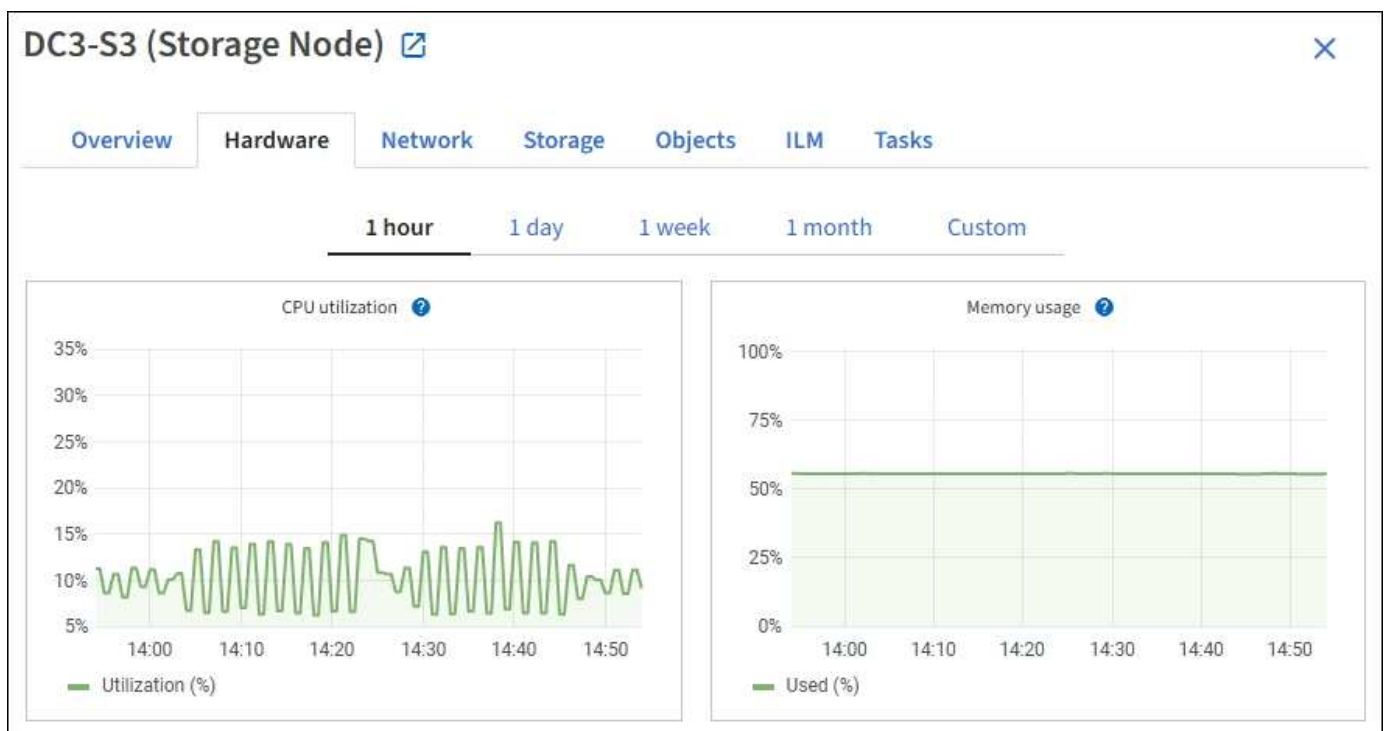
Visualizza la scheda Hardware

La scheda Hardware visualizza l'utilizzo della CPU e della memoria per ciascun nodo, nonché informazioni hardware aggiuntive sugli apparecchi.



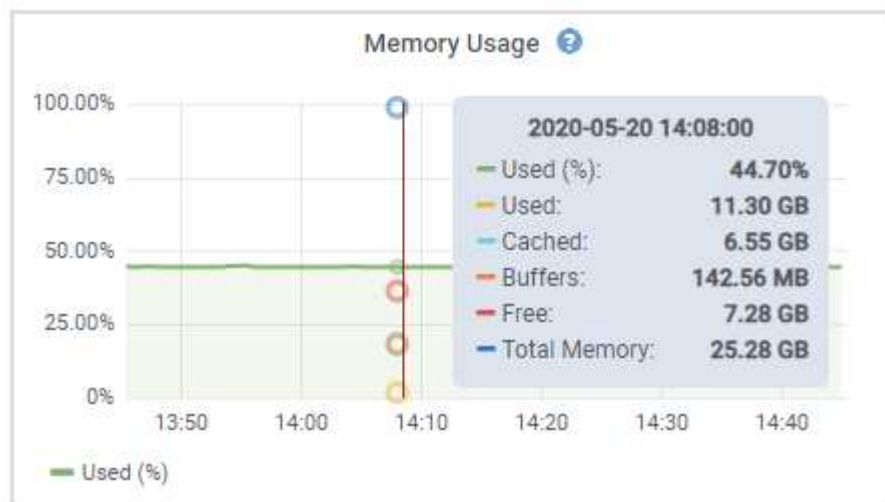
Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere agli screenshot di esempio presenti in questa pagina.

La scheda Hardware viene visualizzata per tutti i nodi.



Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È anche possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.

Per visualizzare i dettagli sull'utilizzo della CPU e della memoria, posiziona il cursore su ciascun grafico.



Se il nodo è un nodo appliance, questa scheda include anche una sezione con maggiori informazioni sull'hardware dell'appliance.

Visualizza informazioni sui nodi di archiviazione dell'appliance

Nella pagina Nodi sono elencate le informazioni sullo stato del servizio e su tutte le risorse di calcolo, dei dispositivi disco e di rete per ciascun nodo di archiviazione dell'appliance. È inoltre possibile visualizzare la memoria, l'hardware di archiviazione, la versione del firmware del controller, le risorse di rete, le interfacce di rete, gli indirizzi di rete e la ricezione e la trasmissione dei dati.

Passi

1. Dalla pagina Nodi, seleziona un nodo di archiviazione dell'appliance.
2. Selezionare **Panoramica**.

La sezione Informazioni nodo della scheda Panoramica visualizza informazioni riepilogative sul nodo, come il nome, il tipo, l'ID e lo stato della connessione. L'elenco degli indirizzi IP include il nome dell'interfaccia per ciascun indirizzo, come segue:

- **eth**: Rete Grid, Rete di amministrazione o Rete client.
- **hic**: Una delle porte fisiche da 10, 25 o 100 GbE sull'appliance. Queste porte possono essere collegate tra loro e connesse alla rete StorageGRID Grid (eth0) e alla rete client (eth2).
- **mtc**: Una delle porte fisiche da 1 GbE sull'appliance. Una o più interfacce mtc sono collegate per formare l'interfaccia di rete di amministrazione StorageGRID (eth1). È possibile lasciare disponibili altre interfacce mtc per la connettività locale temporanea di un tecnico nel data center.

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used:

Object data		7%	?
Object metadata		5%	?

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ⬆	IP address ⬆
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

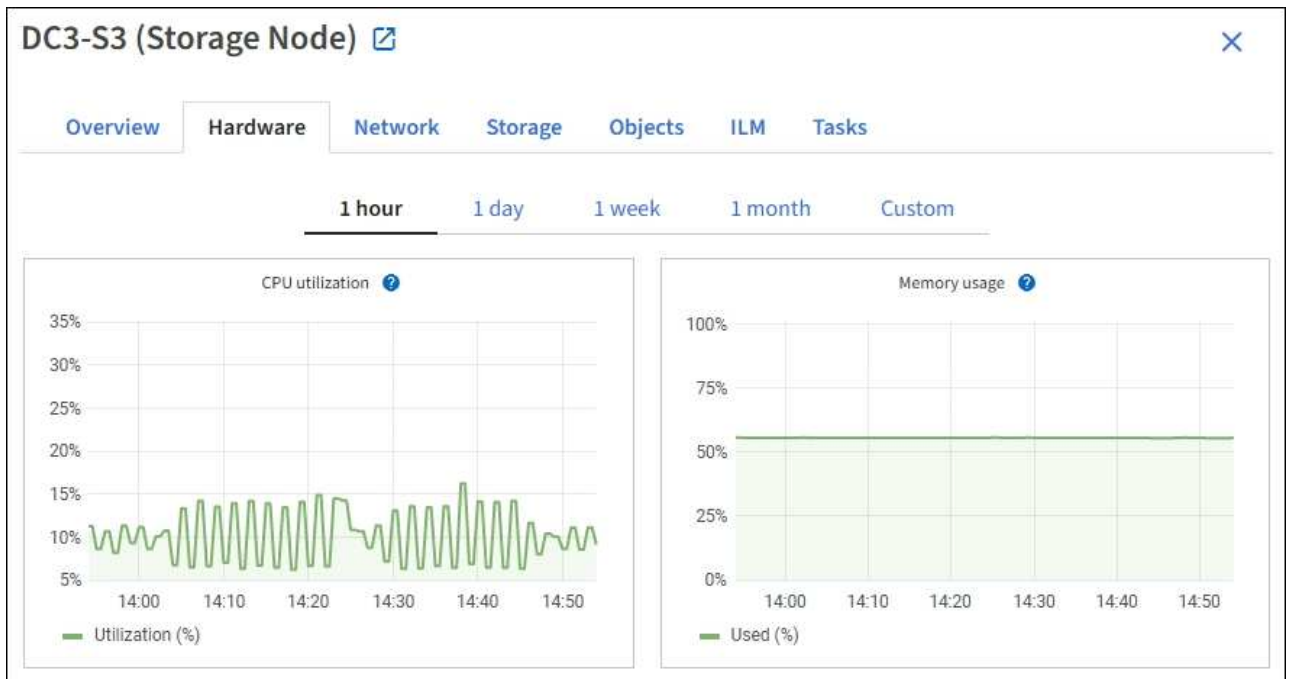
Alerts

Alert name ⬆	Severity ? ⬆	Time triggered ⬆	Current values
ILM placement unachievable 🔗	 Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

La sezione Avvisi della scheda Panoramica visualizza tutti gli avvisi attivi per il nodo.

3. Selezionare **Hardware** per visualizzare maggiori informazioni sull'apparecchio.

- Visualizza i grafici di 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, seleziona uno dei controlli sopra il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È anche 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'apparecchio. Questa tabella contiene informazioni quali il nome del modello dell'apparecchio, i nomi dei controller, i numeri di serie e gli indirizzi IP, nonché lo stato di ciascun componente.



Alcuni campi, come Compute controller BMC IP e Compute hardware, vengono visualizzati solo per gli apparecchi dotati di tale funzionalità.

I componenti per i ripiani di stoccaggio e i ripiani di espansione, se fanno parte dell'installazione, vengono visualizzati in una tabella separata sotto la tabella degli elettrodomestici.

StorageGRID Appliance

Appliance model:	SG6060
Storage controller name:	StorageGRID-Lab79-SG6060-7-134
Storage controller A management IP:	10.2
Storage controller B management IP:	10.2
Storage controller WWID:	6d039ea0000173e50000000065b7b761
Storage appliance chassis serial number:	721924500068
Storage controller firmware version:	08.53.00.09
Storage controller SANtricity OS version:	11.50.3R2
Storage controller NVRAM version:	N280X-853834-DG1
Storage hardware:	Nominal
Storage controller failed drive count:	0
Storage controller A:	Nominal
Storage controller B:	Nominal
Storage controller power supply A:	Nominal
Storage controller power supply B:	Nominal
Storage data drive type:	NL-SAS HDD
Storage data drive size:	4.00 TB
Storage RAID mode:	DDP16
Storage connectivity:	Nominal
Overall power supply:	Degraded
Compute controller BMC IP:	10.2
Compute controller serial number:	721917500060
Compute hardware:	Needs Attention
Compute controller CPU temperature:	Nominal
Compute controller chassis temperature:	Nominal
Compute controller power supply A:	Failed
Compute controller power supply B:	Nominal

Storage shelves

Shelf chassis serial number	Shelf ID	Shelf status	IOM status	Power supply status	Drawer status	Fan status
721924500068	99	Nominal	N/A	Nominal	Nominal	Nominal

Campo nella tabella Appliance	Descrizione
Modello di elettrodomestico	Il numero di modello per questo dispositivo StorageGRID mostrato in SANtricity OS.
Nome del controller di archiviazione	Nome di questo dispositivo StorageGRID mostrato in SANtricity OS.
Controller di archiviazione A IP di gestione	Indirizzo IP per la porta di gestione 1 sul controller di archiviazione A. Utilizzare questo IP per accedere a SANtricity OS per risolvere i problemi di archiviazione.
IP di gestione del controller di archiviazione B	Indirizzo IP per la porta di gestione 1 sul controller di archiviazione B. Utilizzare questo IP per accedere a SANtricity OS per risolvere i problemi di archiviazione. Alcuni modelli di elettrodomestici non dispongono di un controller di archiviazione B.

Campo nella tabella Appliance	Descrizione
WWID del controller di archiviazione	Identificatore mondiale del controller di archiviazione mostrato in SANtricity OS.
Numero di serie del telaio dell'apparecchio di archiviazione	Numero di serie del telaio dell'apparecchio.
Versione del firmware del controller di archiviazione	La versione del firmware sul controller di archiviazione per questo dispositivo.
Versione del sistema operativo SANtricity del controller di archiviazione	La versione SANtricity OS del controller di archiviazione A.
Versione NVSRAM del controller di archiviazione	Versione NVSRAM del controller di archiviazione come riportato da SANtricity System Manager. Per SG6060 e SG6160, se c'è una mancata corrispondenza della versione NVSRAM tra i due controller, viene visualizzata la versione del controller A. Se il controller A non è installato o non è operativo, viene visualizzata la versione del controller B.
Hardware di archiviazione	Stato generale dell'hardware del controller di archiviazione. Se SANtricity System Manager segnala lo stato "Necessita attenzione" per l'hardware di archiviazione, anche il sistema StorageGRID segnala questo valore. Se lo stato è "richiede attenzione", controllare prima il controller di archiviazione utilizzando SANtricity OS. Quindi, assicurarsi che non vi siano altri avvisi applicabili al controller di elaborazione.
Conteggio unità non riuscite del controller di archiviazione	Numero di unità non ottimali.
Controllore di archiviazione A	Lo stato del controller di archiviazione A.
Controllore di archiviazione B	Lo stato del controller di archiviazione B. Alcuni modelli di appliance non dispongono di un controller di archiviazione B.
Alimentatore del controller di archiviazione A	Lo stato dell'alimentatore A per il controller di archiviazione.
Alimentatore del controller di archiviazione B	Lo stato dell'alimentatore B per il controller di archiviazione.
Tipo di unità di archiviazione dati	Il tipo di unità presenti nell'appliance, ad esempio HDD (disco rigido) o SSD (unità a stato solido).

Campo nella tabella Appliances	Descrizione
Dimensioni dell'unità di archiviazione dati	La dimensione effettiva di un'unità dati. Per il modello SG6160 viene visualizzata anche la dimensione dell'unità cache. Nota: Per i nodi con ripiani di espansione, utilizzare Dimensioni dell'unità dati per ogni ripiano Invece. Le dimensioni effettive dell'unità potrebbero variare a seconda dello scaffale.
Modalità RAID di archiviazione	Modalità RAID configurata per l'appliance.
Connettività di archiviazione	Lo stato di connettività dell'archiviazione.
Alimentazione elettrica complessiva	Lo stato di tutte le alimentazioni elettriche dell'apparecchio.
Controller di calcolo BMC IP	L'indirizzo IP della porta del controller di gestione della scheda madre (BMC) nel controller di elaborazione. 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	Numero di serie del controller di elaborazione.
Hardware di calcolo	Lo stato dell'hardware del controller di elaborazione. Questo campo non viene visualizzato per i modelli di appliance che non dispongono di hardware di elaborazione e hardware di archiviazione separati.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di elaborazione.
Calcola la temperatura del telaio del controller	Lo stato della temperatura del controller di calcolo.

+

Colonna nella tabella Scaffali portaoggetti	Descrizione
Numero di serie del telaio dello scaffale	Numero di serie del telaio del ripiano portaoggetti.

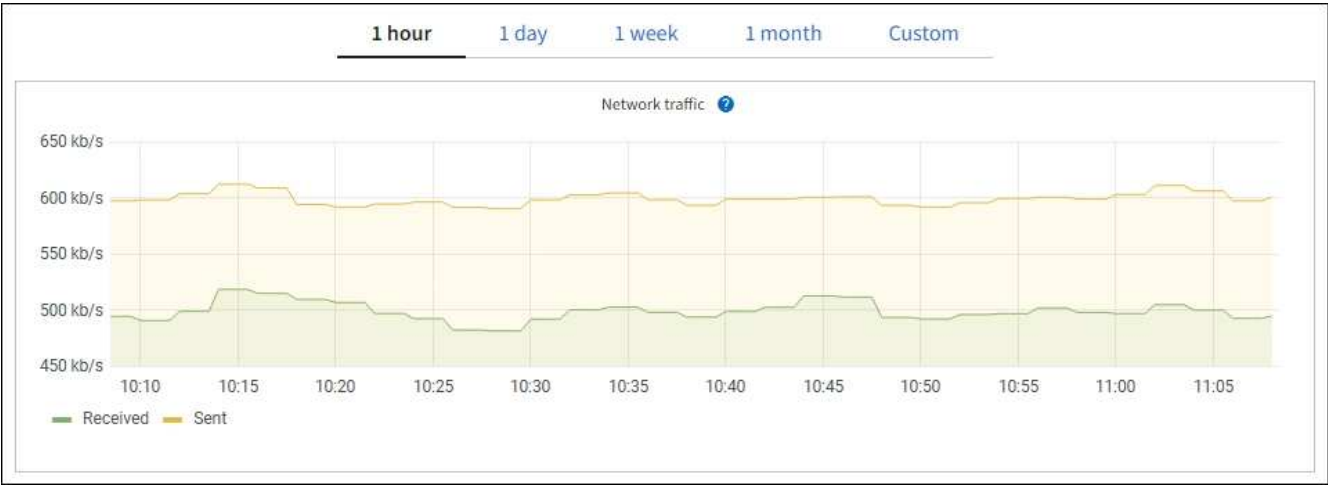
Colonna nella tabella Scaffali portaoggetti	Descrizione
ID scaffale	Identificatore numerico per lo scaffale di stoccaggio. • 99: Ripiano del controller di archiviazione • 0: Primo scaffale di espansione • 1: Secondo ripiano di espansione Nota: i ripiani di espansione sono disponibili solo per i modelli SG6060 e SG6160.
Stato di conservazione	Lo stato generale dello scaffale di stoccaggio.
Stato dell'IOM	Lo stato dei moduli di input/output (IOM) in tutti gli scaffali di espansione. N/D se non si tratta di uno scaffale di espansione.
Stato dell'alimentazione	Lo stato generale degli alimentatori per lo scaffale di stoccaggio.
Stato del cassetto	Lo stato dei cassettei nello scaffale portaoggetti. N/D se lo scaffale non contiene cassettei.
Stato del fan	Stato generale delle ventole di raffreddamento nel ripiano portaoggetti.
Slot di unità	Numero totale di slot per unità nello scaffale di archiviazione.
Unità dati	Numero di unità nello spazio di archiviazione utilizzate per l'archiviazione dei dati.
Dimensione dell'unità dati	La dimensione effettiva di un'unità dati nello spazio di archiviazione.
Unità cache	Numero di unità nello spazio di archiviazione utilizzate come cache.
Dimensioni dell'unità cache	La dimensione dell'unità cache più piccola nello spazio di archiviazione. Di solito, le unità cache hanno tutte le stesse dimensioni.
Stato di configurazione	Lo stato di configurazione dello scaffale di stoccaggio.

a. Verificare che tutti gli stati siano "Nominali".

Se uno stato non è "Nominale", rivedere tutti gli avvisi correnti. È anche possibile utilizzare SANtricity System Manager per saperne di più su alcuni di questi valori hardware. Consultare le istruzioni per l'installazione e la manutenzione dell'apparecchio.

4. Selezionare **Rete** per visualizzare le informazioni per 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 **Velocità** nella tabella Interfacce di rete per determinare se le porte di rete 10/25-GbE sull'appliance sono state configurate per utilizzare la modalità attiva/backup o la modalità LACP.

 I valori indicati nella tabella presuppongono l'utilizzo di tutti e quattro i collegamenti.

Modalità di collegamento	Modalità Bond	Velocità di collegamento HIC individuale (hic1, hic2, hic3, hic4)	Velocità di rete prevista per Grid/Client (eth0,eth2)
Aggregato	LACP	25	100
Fisso	LACP	25	50
Fisso	Attivo/Backup	25	25
Aggregato	LACP	10	40
Fisso	LACP	10	20
Fisso	Attivo/Backup	10	10

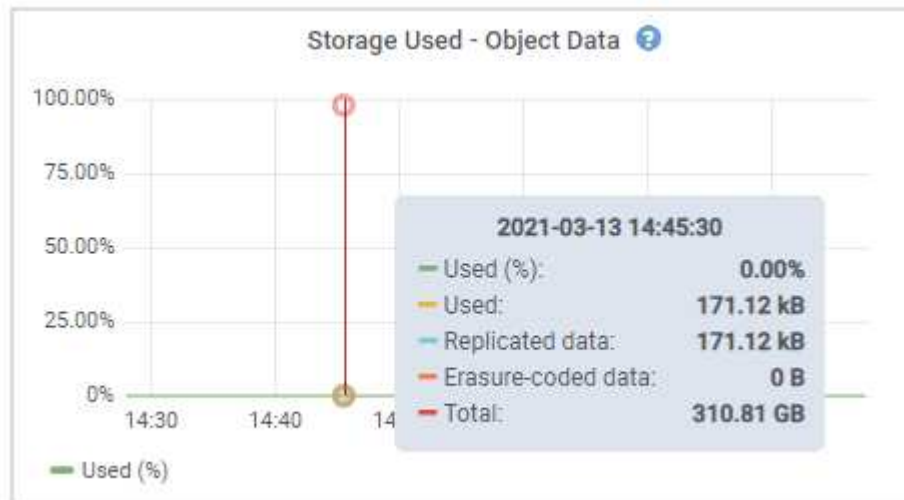
Vedere ["Configurare i collegamenti di rete"](#) per ulteriori informazioni sulla configurazione delle porte 10/25-GbE.

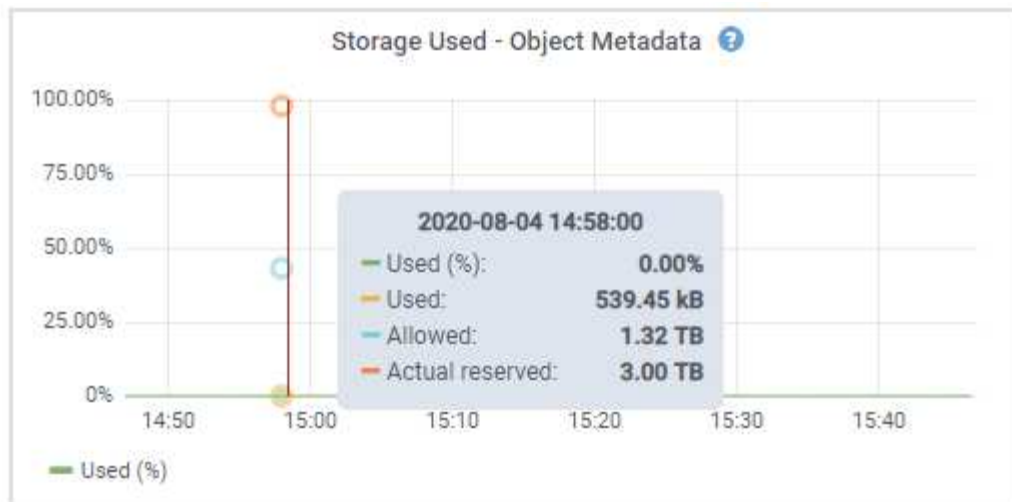
b. Rivedere la sezione Comunicazione di rete.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati su 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 **Archiviazione** per visualizzare grafici che mostrano le percentuali di spazio di archiviazione utilizzato nel tempo per i dati degli oggetti e i metadati degli oggetti, nonché informazioni su dispositivi disco, volumi e archivi di oggetti.





- a. Scorrere verso il basso per visualizzare la quantità di spazio di archiviazione disponibile per ciascun volume e archivio oggetti.

Il nome mondiale di ciascun disco corrisponde all'identificatore mondiale del volume (WWID) visualizzato quando si visualizzano le proprietà standard del volume in SANtricity OS (il software di gestione connesso al controller di archiviazione dell'appliance).

Per aiutarti a interpretare le statistiche di lettura e scrittura del disco relative ai punti di montaggio del volume, la prima parte del nome mostrato nella colonna **Nome** della tabella Dispositivi disco (ovvero *sdc*, *sdd*, *sde* e così via) corrisponde al valore mostrato nella colonna **Dispositivo** della tabella 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 Nodi elenca le informazioni sullo stato del servizio e su tutte le risorse di calcolo, dei dispositivi disco e di rete per ogni appliance di servizi utilizzata come nodo di amministrazione o nodo gateway. È inoltre possibile visualizzare la memoria, l'hardware di archiviazione, le risorse di rete, le interfacce di rete, gli indirizzi di rete e la ricezione e la trasmissione di dati.

Passi

1. Dalla pagina Nodi, seleziona un nodo di amministrazione dell'appliance o un nodo gateway dell'appliance.
2. Selezionare **Panoramica**.

La sezione Informazioni nodo della scheda Panoramica visualizza informazioni riepilogative sul nodo, come il nome, il tipo, l'ID e lo stato della connessione. L'elenco degli indirizzi IP include il nome

dell'interfaccia per ciascun indirizzo, come segue:

- **adllb** e **adlli**: visualizzati se viene utilizzato il bonding attivo/di backup per l'interfaccia di rete di amministrazione
- **eth**: Rete Grid, Rete di amministrazione o Rete client.
- **hic**: Una delle porte fisiche da 10, 25 o 100 GbE sull'appliance. Queste porte possono essere collegate tra loro e connesse alla rete StorageGRID Grid (eth0) e alla rete client (eth2).
- **mtc**: Una delle porte fisiche da 1 GbE sull'appliance. Una o più interfacce mtc sono collegate per formare l'interfaccia di rete di amministrazione (eth1). È possibile lasciare disponibili altre interfacce mtc per la connettività locale temporanea di un tecnico nel data center.

The screenshot displays the 'Node information' section of the SANtricity System Manager. The node is identified as '10-224-6-199-ADM1 (Primary Admin Node)'. It is a 'Primary Admin Node' with ID '6fdc1890-ca0a-4493-acdd-72ed317d95fb'. The connection state is 'Connected'. The software version is '11.6.0 (build 20210928.1321.6687ee3)'. The IP addresses are listed as follows:

- 172.16.6.199 - eth0 (Grid Network)
- 10.224.6.199 - eth1 (Admin Network)
- 47.47.7.241 - eth2 (Client Network)

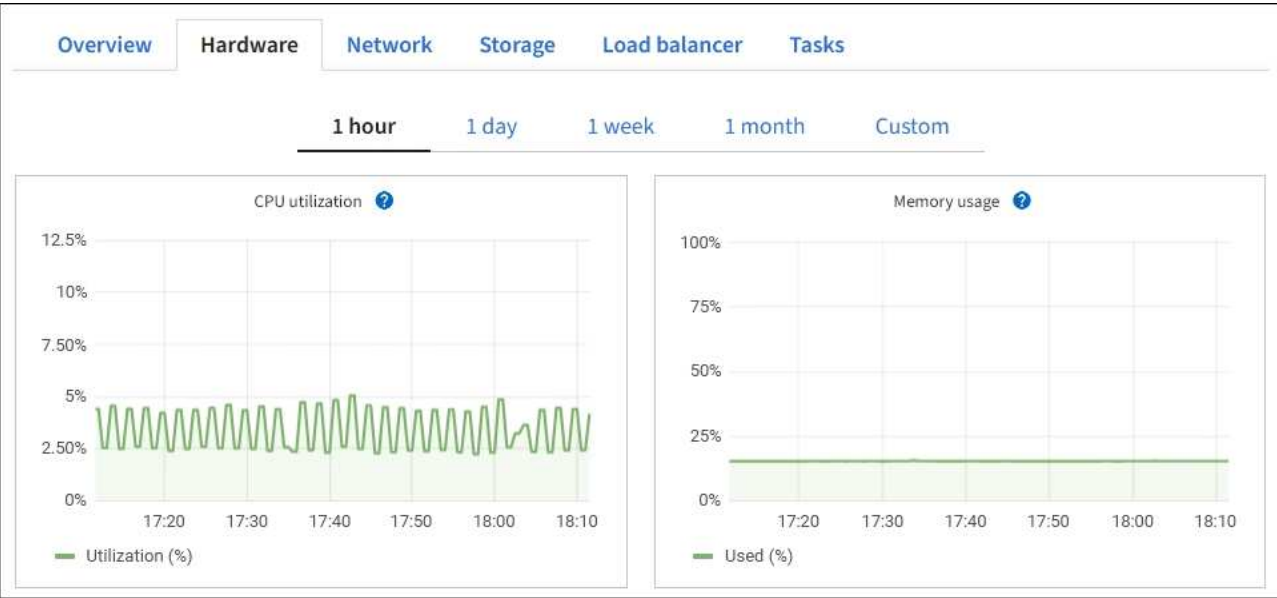
Below the IP addresses, there is a table showing the network interfaces and their corresponding IP addresses:

Interface	IP address
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

La sezione Avvisi della scheda Panoramica visualizza tutti gli avvisi attivi per il nodo.

3. Selezionare **Hardware** per visualizzare maggiori informazioni sull'apparecchio.

- Visualizza i grafici di 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, seleziona uno dei controlli sopra il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È anche 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'apparecchio. Questa tabella contiene informazioni quali il nome del modello, il numero di serie, la versione del firmware del controller e lo stato di ciascun componente.

StorageGRID Appliance		
Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

Campo nella tabella Appliance	Descrizione
Modello di elettrodomestico	Numero di modello per questo dispositivo StorageGRID .

Campo nella tabella Appliances	Descrizione
Conteggio unità non riuscite del controller di archiviazione	Numero di unità non ottimali.
Tipo di unità di archiviazione dati	Il tipo di unità presenti nell'appliance, ad esempio HDD (disco rigido) o SSD (unità a stato solido).
Dimensioni dell'unità di archiviazione dati	La dimensione effettiva di un'unità dati.
Modalità RAID di archiviazione	La modalità RAID per l'appliance.
Alimentazione elettrica complessiva	Lo stato di tutti gli alimentatori dell'apparecchio.
Controller di calcolo BMC IP	L'indirizzo IP della porta del controller di gestione della scheda madre (BMC) nel controller di elaborazione. 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	Numero di serie del controller di elaborazione.
Hardware di calcolo	Lo stato dell'hardware del controller di elaborazione.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di elaborazione.
Calcola la temperatura del telaio del controller	Lo stato della temperatura del controller di calcolo.

a. Verificare che tutti gli stati siano "Nominali".

Se uno stato non è "Nominale", rivedere tutti gli avvisi correnti.

4. Selezionare **Rete** per visualizzare le informazioni per 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 **Velocità** nella tabella Interfacce di rete per determinare se le quattro porte di rete 40/100-GbE sull'apppliance sono state configurate per utilizzare la modalità attiva/backup o la modalità LACP.



I valori indicati nella tabella presuppongono l'utilizzo di tutti e quattro i collegamenti.

Modalità di collegamento	Modalità Bond	Velocità di collegamento HIC individuale (hic1, hic2, hic3, hic4)	Velocità prevista della rete Grid/Client (eth0, eth2)
Aggregato	LACP	100	400
Fisso	LACP	100	200
Fisso	Attivo/Backup	100	100
Aggregato	LACP	40	160
Fisso	LACP	40	80
Fisso	Attivo/Backup	40	40

b. Rivedere la sezione Comunicazione di rete.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati su 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 **Archiviazione** per visualizzare informazioni sui dispositivi disco e sui volumi nell'appliance dei servizi.

Disk devices

Name ? ↕	World Wide Name ? ↕	I/O load ? ↕	Read rate ? ↕	Write rate ? ↕
croot(8:1,sda1)	N/A	0.02%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.03%	0 bytes/s	6 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	84.63 GB 	Unknown

Visualizza la scheda Rete

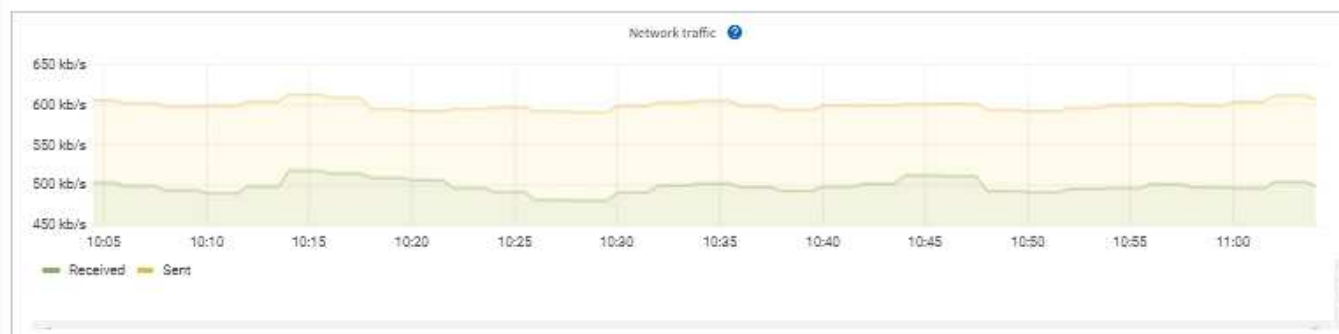
La scheda Rete visualizza un grafico che mostra il traffico di rete ricevuto e inviato su tutte le interfacce di rete sul nodo, sul sito o sulla griglia.

La scheda Rete viene visualizzata per tutti i nodi, per ciascun sito e per l'intera griglia.

Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È anche 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 su eventuali contatori di errori segnalati dal driver.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

Informazioni correlate

["Monitorare le connessioni e le prestazioni di rete"](#)

Visualizza la scheda Archiviazione

La scheda Archiviazione riassume la disponibilità di archiviazione e altre metriche di archiviazione.

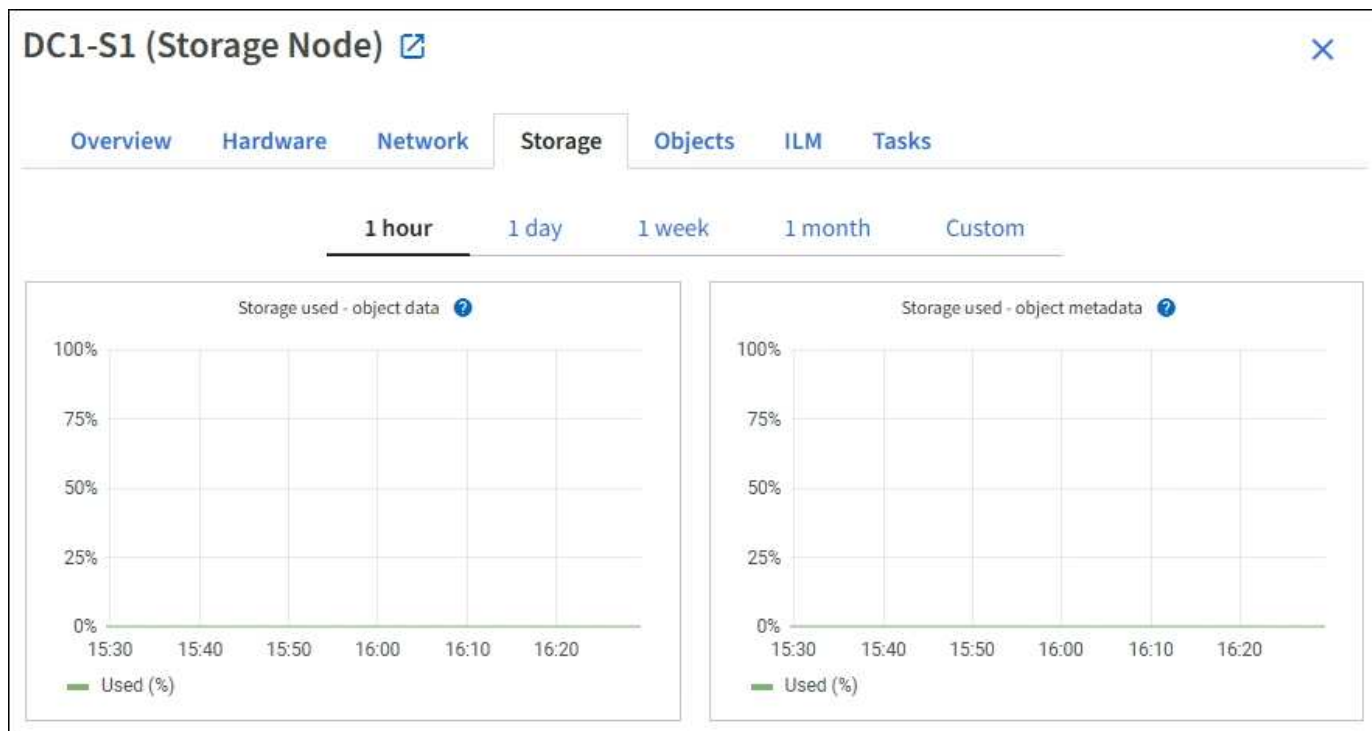
La scheda Archiviazione viene visualizzata per tutti i nodi, per ciascun sito e per l'intera griglia.

Grafici di archiviazione utilizzati

Per i nodi di archiviazione, ciascun sito e l'intera griglia, la scheda Archiviazione include grafici che mostrano la quantità di spazio di archiviazione utilizzata dai dati degli oggetti e dai metadati degli oggetti nel tempo.



Quando un nodo non è connesso alla rete, ad esempio durante un aggiornamento o in uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della rete. Dopo che un nodo si è ricollegato alla rete, attendere alcuni minuti affinché i valori si stabilizzino.



Dispositivi disco, volumi e tabelle di archiviazione oggetti

Per tutti i nodi, la scheda Archiviazione contiene i dettagli sui dispositivi disco e sui volumi presenti sul nodo. Per i nodi di archiviazione, la tabella Archivi oggetti fornisce informazioni su ciascun volume di archiviazione.

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 di archiviazione"](#)

Visualizza la scheda Oggetti

La scheda Oggetti fornisce informazioni su ["Velocità di acquisizione e recupero S3"](#).

La scheda Oggetti viene visualizzata per ogni nodo di archiviazione, ogni sito e l'intera griglia. Per i nodi di archiviazione, la scheda Oggetti fornisce anche conteggi degli oggetti e informazioni sulle query dei metadati e sulla verifica in background.

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

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

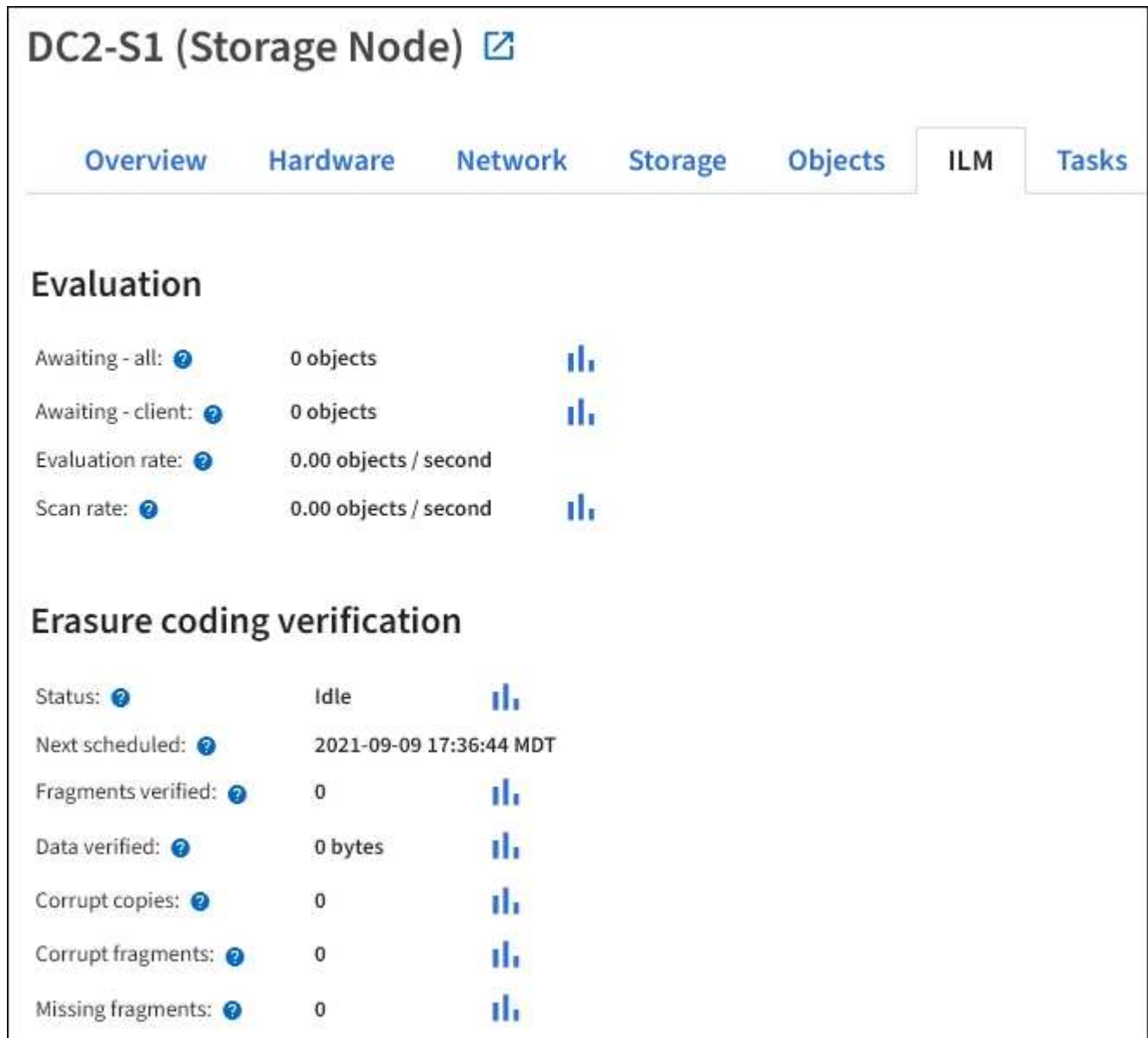
Quarantined objects: ? 0

Visualizza la scheda ILM

La scheda ILM fornisce informazioni sulle operazioni di gestione del ciclo di vita delle informazioni (ILM).

La scheda ILM viene visualizzata per ogni nodo di archiviazione, ogni 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 di archiviazione, la scheda ILM fornisce dettagli sulla valutazione ILM e sulla verifica in background per gli oggetti con codice di cancellazione.



Informazioni correlate

- ["Monitorare la gestione del ciclo di vita delle informazioni"](#)
- ["Amministra StorageGRID"](#)

Utilizzare la scheda Attività

La scheda Attività viene visualizzata per tutti i nodi. È possibile utilizzare questa scheda per rinominare o riavviare un nodo oppure per mettere un nodo appliance in modalità di manutenzione.

Per i requisiti completi e le istruzioni per ciascuna opzione in questa scheda, vedere quanto segue:

- ["Rinomina griglia, siti e nodi"](#)
- ["Riavvia il nodo della griglia"](#)
- ["Mettere l'apparecchio in modalità manutenzione"](#)

Visualizza la scheda Bilanciatore del carico

La scheda Load Balancer include grafici delle prestazioni e della diagnostica relativi al funzionamento del servizio Load Balancer.

La scheda Load Balancer viene visualizzata per i nodi di amministrazione e i nodi gateway, per ciascun sito e per l'intera griglia. Per ogni sito, la scheda Load Balancer fornisce un riepilogo aggregato delle statistiche per tutti i nodi di quel sito. Per l'intera griglia, la scheda Load Balancer fornisce un riepilogo aggregato delle statistiche per tutti i siti.

Se non viene eseguito alcun I/O tramite il servizio Load Balancer o non è configurato alcun load balancer, i grafici visualizzano "Nessun dato".



Richiedi traffico

Questo grafico fornisce una media mobile di 3 minuti della velocità di trasmissione dei dati tra gli endpoint del bilanciatore del carico e i client che effettuano le richieste, in bit al secondo.



Questo valore viene aggiornato al completamento di ogni richiesta. Di conseguenza, questo valore potrebbe differire dalla produttività in tempo reale in caso di basse frequenze di richiesta o per richieste di durata molto lunga. È possibile consultare la scheda Rete per avere una visione più realistica del comportamento attuale della rete.

Tasso di richiesta in arrivo

Questo grafico fornisce una media mobile di 3 minuti del numero di nuove richieste al secondo, suddivise 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 (senza errori)

Questo grafico fornisce una media mobile di 3 minuti delle durate delle richieste, suddivise per tipo di richiesta (GET, PUT, HEAD e DELETE). La durata di ogni richiesta inizia quando un'intestazione della richiesta viene analizzata dal servizio Load Balancer e termina quando il corpo completo della risposta viene restituito al

client.

Tasso di risposta agli errori

Questo grafico fornisce una media mobile di 3 minuti del numero di risposte di errore restituite ai client al secondo, suddivise in base al codice di risposta di errore.

Informazioni correlate

- ["Monitorare le operazioni di bilanciamento del carico"](#)
- ["Amministra StorageGRID"](#)

Visualizza la scheda Servizi della piattaforma

La scheda Servizi della piattaforma fornisce informazioni su tutte le operazioni dei servizi della piattaforma S3 in un sito.

Per ogni sito viene visualizzata la scheda Servizi della piattaforma. Questa scheda fornisce informazioni sui servizi della piattaforma S3, come la replica CloudMirror e il servizio di integrazione della ricerca. I grafici in questa scheda mostrano parametri quali il numero di richieste in sospeso, la percentuale di completamento delle richieste e la percentuale di errore delle richieste.

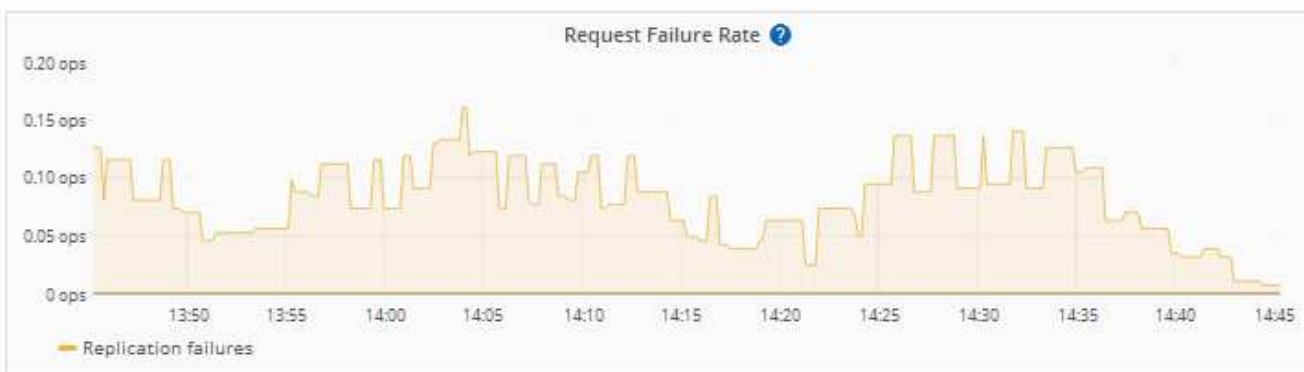
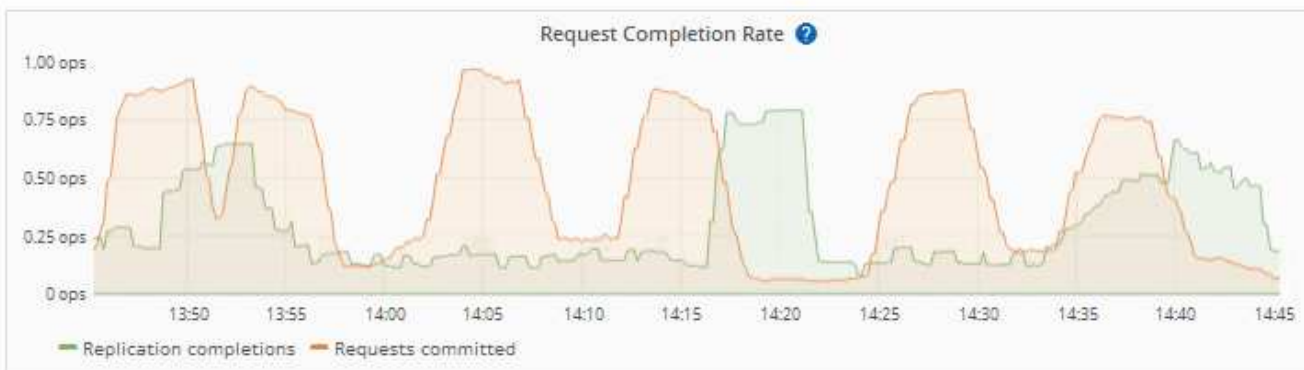
1 hour

1 day

1 week

1 month

Custom



Per ulteriori informazioni sui servizi della piattaforma S3, inclusi i dettagli sulla risoluzione dei problemi, vedere ["Istruzioni per l'amministrazione StorageGRID"](#).

Visualizza la scheda Gestisci unità

La scheda Gestisci unità consente di accedere ai dettagli ed eseguire attività di risoluzione dei problemi e manutenzione sulle unità negli apparecchi che supportano questa funzionalità.

Utilizzando la scheda Gestisci unità, puoi effettuare le seguenti operazioni:

- Visualizza un layout delle unità di archiviazione dati nell'appliance
- Visualizza una tabella che elenca ciascuna posizione dell'unità, tipo, stato, versione del firmware e numero di serie
- Eseguire funzioni di risoluzione dei problemi e manutenzione su ciascuna unità

Per accedere alla scheda Gestisci unità, è necessario disporre di ["Amministratore dell'appliance di archiviazione o autorizzazione di accesso root"](#) .

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 SANtricity System Manager consente di accedere a SANtricity System Manager senza dover configurare o connettere la porta di gestione dell'appliance di archiviazione. È possibile utilizzare questa scheda per esaminare le informazioni diagnostiche e ambientali dell'hardware, nonché i problemi relativi alle unità.



L'accesso a SANtricity System Manager da Grid Manager è in genere destinato solo al monitoraggio dell'hardware dell'appliance e alla configurazione di E-Series AutoSupport. Molte funzionalità e operazioni di SANtricity System Manager, come l'aggiornamento del firmware, non sono applicabili al monitoraggio dell'appliance StorageGRID . Per evitare problemi, seguire sempre le istruzioni di manutenzione hardware del proprio elettrodomestico. Per aggiornare il firmware SANtricity , vedere ["Procedure di configurazione della manutenzione"](#) per il tuo dispositivo di archiviazione.



La scheda SANtricity System Manager viene visualizzata solo per i nodi degli storage appliance che utilizzano hardware E-Series.

Utilizzando SANtricity System Manager, è possibile effettuare le seguenti operazioni:

- Visualizza i dati sulle prestazioni, come le prestazioni a livello di array di archiviazione, la latenza di I/O, l'utilizzo della CPU del controller di archiviazione e la velocità effettiva.
- 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 SANtricity System Manager per configurare un proxy per E-Series AutoSupport, vedere ["Inviare pacchetti E-Series AutoSupport tramite StorageGRID"](#) .

Per accedere a SANtricity System Manager tramite Grid Manager, è necessario disporre di ["Amministratore dell'appliance di archiviazione o autorizzazione di accesso root"](#) .



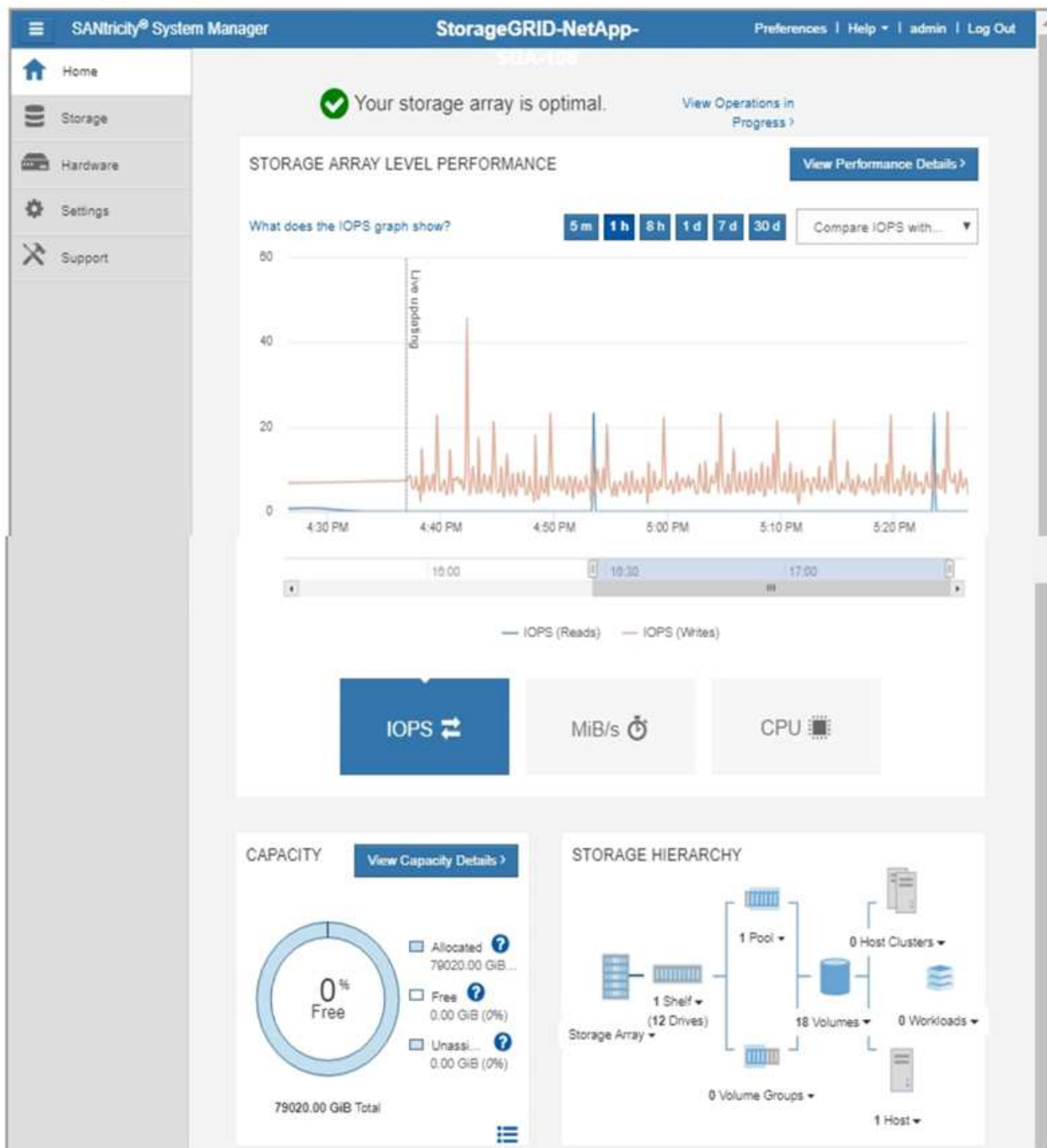
Per accedere a SANtricity System Manager tramite Grid Manager è necessario disporre del firmware SANtricity 8.70 o superiore.

La scheda visualizza la home page di SANtricity System Manager.

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

Note: Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open **SANtricity System Manager** in a new browser tab.



È possibile utilizzare il collegamento SANtricity System Manager per aprire SANtricity System Manager in una nuova finestra del browser per una visualizzazione più semplice.

Per visualizzare i dettagli sulle prestazioni a livello di array di archiviazione e sull'utilizzo della capacità,

posizionare il cursore su ciascun grafico.

Per maggiori dettagli sulla visualizzazione delle informazioni accessibili dalla scheda SANtricity System Manager, vedere ["Documentazione 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 rete non sono disponibili, è opportuno monitorare e risolvere i 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"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Informazioni sulle attività di monitoraggio

Un sistema occupato genera grandi quantità di informazioni. L'elenco seguente fornisce indicazioni sulle informazioni più importanti da monitorare costantemente.

Cosa monitorare	Frequenza
"Stato di salute del sistema"	Quotidiano
Tasso a cui "Capacità degli oggetti e dei metadati del nodo di archiviazione" viene consumato	Settimanale
"Operazioni di gestione del ciclo di vita delle informazioni"	Settimanale
"Risorse di rete e di sistema"	Settimanale
"Attività degli inquilini"	Settimanale
"Operazioni client S3"	Settimanale
"Operazioni di bilanciamento del carico"	Dopo la configurazione iniziale e dopo eventuali modifiche alla configurazione
"Connessioni di federazione della rete"	Settimanale

Monitorare lo stato di salute del sistema

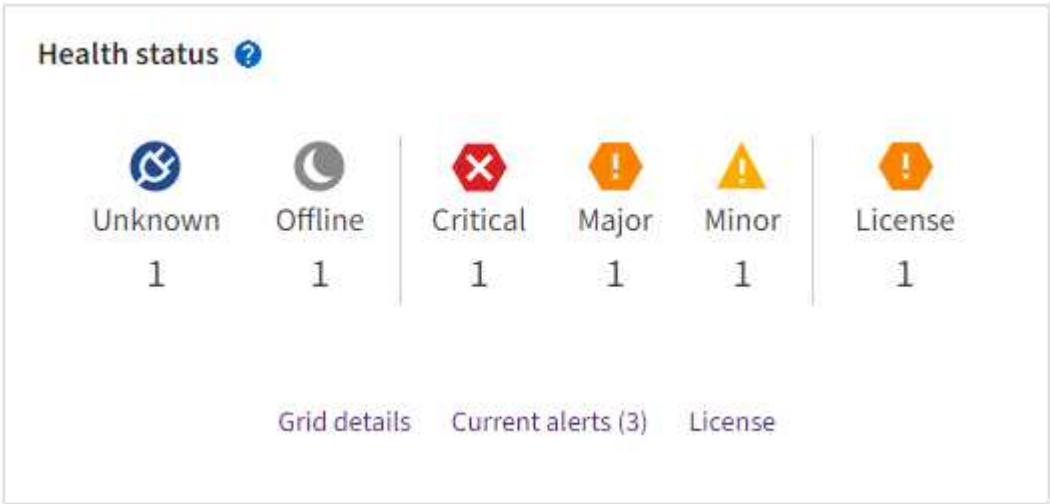
Monitora quotidianamente lo stato di salute generale del tuo sistema StorageGRID.

Informazioni su questo compito

Il sistema StorageGRID può continuare a funzionare anche quando alcune parti della rete non sono disponibili. I potenziali problemi segnalati dagli avvisi non sono necessariamente problemi con le operazioni del sistema.

Esaminare i problemi riepilogati nella scheda Stato di integrità della dashboard di Grid Manager.

Per essere avvisato degli avvisi non appena vengono attivati, puoi ["impostare notifiche e-mail per gli avvisi"](#) O ["configurare trappole SNMP"](#) .



Quando si verificano problemi, vengono visualizzati dei link che consentono di visualizzare ulteriori dettagli:

Collegamento	Appare quando...
Dettagli della griglia	Alcuni nodi sono disconnessi (stato di connessione Sconosciuto o Amministrativamente inattivo).
Avvisi attuali (critici, gravi, minori)	Gli avvisi sono attualmente attivo .
Avvisi risolti di recente	Avvisi attivati nell'ultima settimana sono ora risolti .
Licenza	Si è verificato un problema con la licenza software per questo sistema StorageGRID . È possibile "aggiornare le informazioni sulla licenza secondo necessità" Potrebbe

Monitorare gli stati di connessione dei nodi

Se uno o più nodi vengono disconnessi dalla rete, le operazioni critiche StorageGRID potrebbero essere compromesse. 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 è disconnesso oppure i servizi sul nodo sono inaspettatamente inattivi. Ad esempio, un servizio sul nodo potrebbe essere interrotto oppure il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione di corrente o di un'interruzione imprevista. Potrebbe anche essere attivato l'avviso Impossibile comunicare con il nodo. Potrebbero essere attivi anche altri avvisi.	Richiede attenzione immediata. Seleziona ogni avviso e seguire le azioni consigliate. Ad esempio, potrebbe essere necessario riavviare un servizio che si è arrestato o riavviare l'host per il nodo. Nota: un nodo potrebbe apparire come Sconosciuto durante le operazioni di arresto gestito. In questi casi è possibile ignorare lo stato Sconosciuto.
	Non connesso - Amministrativamente inattivo Per un motivo prevedibile, il nodo non è connesso alla griglia. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi. In base al problema di fondo, questi nodi spesso tornano online senza alcun intervento.	Determina se ci sono avvisi che interessano questo nodo. Se uno o più avvisi sono attivi, seleziona ogni avviso e seguire le azioni consigliate.
	Collegato Il nodo è collegato alla rete.	Nessuna azione richiesta.

Visualizza gli avvisi correnti e risolti

Avvisi attuali: quando viene attivato un avviso, sulla dashboard viene visualizzata un'icona di avviso. Nella pagina Nodi viene visualizzata anche un'icona di avviso per il nodo. Se ["le notifiche e-mail di avviso sono configurate"](#), verrà inviata anche una notifica via e-mail, a meno che l'avviso non sia stato disattivato.

Avvisi risolti: puoi cercare e visualizzare la cronologia degli avvisi che sono stati risolti.

Facoltativamente, hai guardato il video: ["Video: Panoramica degli avvisi"](#)



Nella tabella seguente vengono descritte 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 sua descrizione.
Gravità	La gravità dell'allerta. Per gli avvisi correnti, se vengono raggruppati più avvisi, la riga del titolo mostra quante istanze di quell'avviso si verificano per ogni livello di gravità.  Critico: si è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID . Bisogna affrontare immediatamente il problema di fondo. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.  Grave: Esiste una condizione anomala che sta influenzando le operazioni in corso o che si sta avvicinando alla soglia di un avviso critico. È necessario esaminare gli avvisi principali e risolvere eventuali problemi sottostanti per garantire che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID .  Minore: Il sistema funziona normalmente, ma si verifica una condizione anomala che potrebbe compromettere la capacità del sistema di funzionare se continua a verificarsi tale condizione. È opportuno monitorare e risolvere gli avvisi minori che non si risolvono da soli, per evitare che diano origine a problemi più seri.
Tempo attivato	Avvisi attuali: data e ora in cui è stato attivato l'avviso, in base all'ora locale e all'ora UTC. Se vengono raggruppati più avvisi, la riga del titolo mostra gli orari dell'istanza più recente dell'avviso (<i>newest</i>) e dell'istanza più vecchia dell'avviso (<i>oldest</i>). Avvisi risolti: da quanto tempo è stato attivato l'avviso.
Sito/Nodo	Nome del sito e del nodo in cui si sta verificando o si è verificato l'avviso.

Intestazione di colonna	Descrizione
Stato	Se l'avviso è attivo, disattivato o risolto. Se vengono raggruppati più avvisi e nel menu a discesa è selezionato Tutti gli avvisi , la riga del titolo mostra quante istanze di quell'avviso sono attive e quante istanze sono state silenziate.
Tempo di risoluzione (solo avvisi risolti)	Da quanto tempo è stato risolto l'avviso.
Valori correnti o <i>valori di dati</i>	Il valore della metrica che ha causato l'attivazione dell'avviso. Per alcuni avvisi vengono visualizzati valori aggiuntivi per aiutarti a comprendere e analizzare l'avviso. Ad esempio, i valori mostrati per un avviso Archiviazione dati oggetto insufficiente 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.
Valori attivati (solo avvisi risolti)	Il valore della metrica che ha causato l'attivazione dell'avviso. Per alcuni avvisi vengono visualizzati valori aggiuntivi per aiutarti a comprendere e analizzare l'avviso. Ad esempio, i valori mostrati per un avviso Archiviazione dati oggetto insufficiente includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata.

Passi

1. Selezionare il collegamento **Avvisi correnti** o **Avvisi risolti** per visualizzare un elenco degli avvisi in quelle categorie. È anche possibile visualizzare i dettagli di un avviso selezionando **Nodi > nodo > Panoramica** e quindi selezionando l'avviso dalla tabella Avvisi.

Per impostazione predefinita, gli avvisi correnti vengono visualizzati come segue:

- Vengono mostrati per primi gli avvisi attivati più di recente.
- Più avvisi dello stesso tipo vengono visualizzati come gruppo.
- Gli avvisi disattivati non vengono visualizzati.
- Per un avviso specifico su un nodo specifico, se vengono raggiunte le soglie per più di una gravità, viene visualizzato solo l'avviso più grave. Ciò significa che se vengono raggiunte le soglie di allerta per le gravità minore, maggiore e critica, viene visualizzato solo l'avviso critico.

La pagina Avvisi correnti viene aggiornata ogni due minuti.

2. Per espandere i gruppi di avvisi, selezionare il cursore verso il basso . Per comprimere i singoli avvisi in un gruppo, selezionare il cursore verso l'alto  oppure seleziona il nome del gruppo.
3. Per visualizzare avvisi individuali anziché gruppi di avvisi, deselezionare la casella di controllo **Avvisi di gruppo**.
4. Per ordinare gli avvisi correnti o i gruppi di avvisi, selezionare le frecce su/giù  in ogni intestazione di colonna.
 - Quando si seleziona **Avvisi di gruppo**, vengono ordinati sia i gruppi di avvisi sia i singoli avvisi all'interno di ciascun gruppo. Ad esempio, potresti voler ordinare gli avvisi in un gruppo in base all'**ora di attivazione** per trovare l'istanza più recente di un avviso specifico.

- Quando si cancella **Avvisi di gruppo**, viene ordinato l'intero elenco degli avvisi. Ad esempio, potresti voler ordinare tutti gli avvisi per **Nodo/Sito** per visualizzare tutti gli avvisi che interessano 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 "[Disattiva le notifiche di avviso](#)".

6. Per ordinare gli avvisi risolti:

- Selezionare un periodo di tempo dal menu a discesa **Quando attivato**.
- Selezionare uno o più livelli di gravità dal menu a discesa **Gravità**.
- 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, seleziona l'avviso. Una finestra di dialogo fornisce dettagli e azioni consigliate per l'avviso selezionato.

8. (Facoltativo) Per un avviso specifico, seleziona **Disattiva questo avviso** per disattivare la regola di avviso che ha causato l'attivazione dell'avviso.

Devi avere il "[Gestisci avvisi o autorizzazione di accesso root](#)" per silenziare una regola di avviso.



Prestare attenzione quando si decide di disattivare una regola di avviso. Se una regola di avviso viene disattivata, potresti non rilevare un problema di fondo finché non impedisce il completamento di un'operazione critica.

9. Per visualizzare le condizioni attuali per la regola di avviso:

- a. Dai dettagli dell'avviso, seleziona **Visualizza condizioni**.

Viene visualizzata una finestra pop-up che elenca l'espressione Prometheus per ogni gravità definita.

- b. Per chiudere il pop-up, fare clic in un punto qualsiasi al di fuori del pop-up.

10. Facoltativamente, seleziona **Modifica regola** per modificare la regola di avviso che ha causato l'attivazione di questo avviso.

Devi avere il "[Gestisci avvisi o autorizzazione di accesso root](#)" per modificare una regola di avviso.



Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, è possibile che non venga rilevato un problema di fondo finché non si impedisce il completamento di un'operazione critica.

11. Per chiudere i dettagli dell'avviso, seleziona **Chiudi**.

Monitorare la capacità di archiviazione

Monitorare lo spazio utilizzabile totale disponibile per garantire che il sistema StorageGRID non esaurisca lo spazio di archiviazione per gli oggetti o per i metadati degli oggetti.

StorageGRID archivia separatamente i dati degli oggetti e i metadati degli oggetti e riserva una quantità specifica di spazio per un database Cassandra distribuito che contiene i metadati degli oggetti. Monitora la quantità totale di spazio occupato dagli oggetti e dai metadati degli oggetti, nonché le tendenze nella quantità di spazio occupato per ciascuno. Ciò ti consentirà di pianificare in anticipo l'aggiunta di nodi ed evitare eventuali interruzioni del servizio.

Puoi [visualizza le informazioni sulla capacità di archiviazione](#) per l'intera griglia, per ciascun sito e per ciascun nodo di archiviazione nel sistema StorageGRID .

Monitorare la capacità di archiviazione per l'intera rete

Monitora la capacità di archiviazione complessiva della tua griglia per assicurarti che rimanga spazio libero adeguato per i dati degli oggetti e i metadati degli oggetti. Comprendere come la capacità di archiviazione cambia nel tempo può aiutarti a pianificare l'aggiunta di nodi di archiviazione o volumi di archiviazione prima che la capacità di archiviazione utilizzabile della griglia venga esaurita.

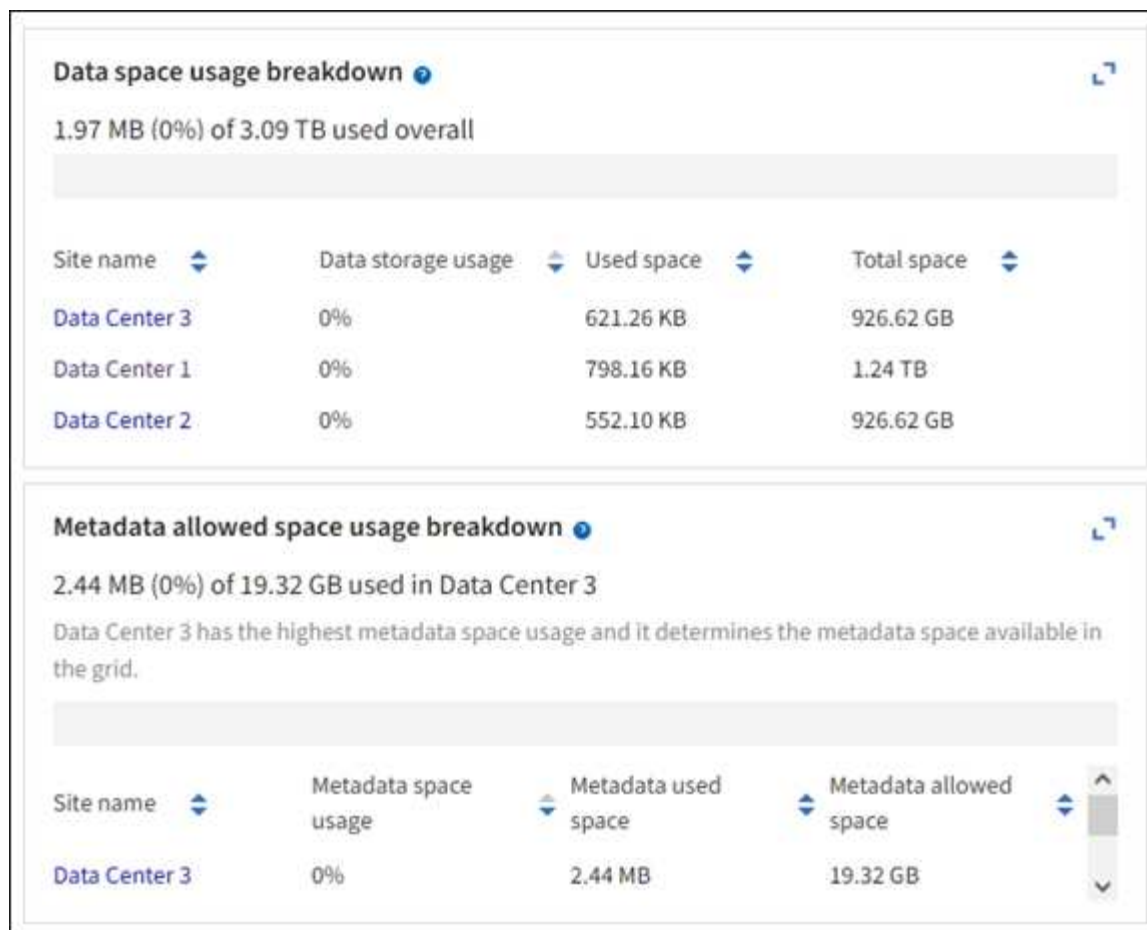
La dashboard di Grid Manager consente di valutare rapidamente la quantità di spazio di archiviazione disponibile per l'intera griglia e per ciascun data center. La pagina Nodi fornisce valori più dettagliati per i dati degli oggetti e i metadati degli oggetti.

Passi

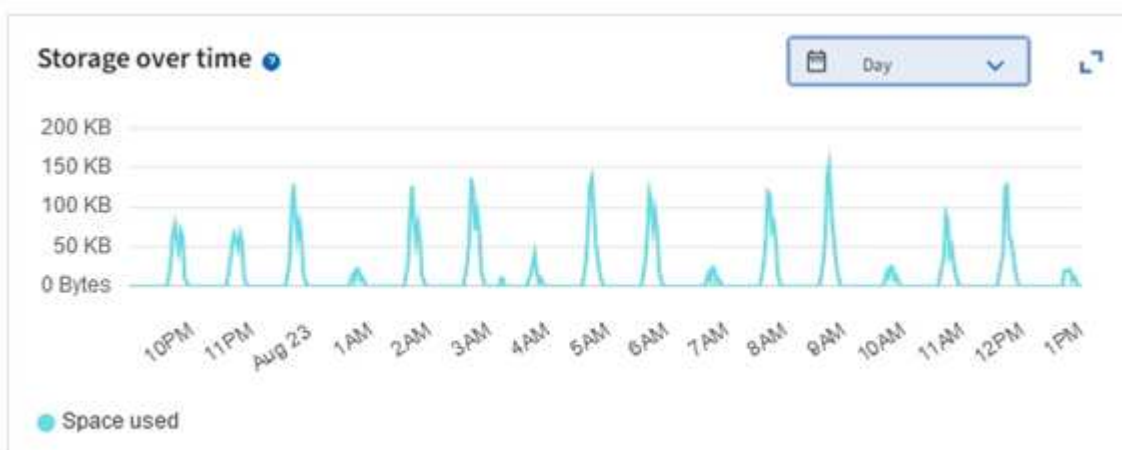
1. Valutare la quantità di spazio di archiviazione disponibile per l'intera rete e per ciascun data center.
 - a. Selezionare **Dashboard > Panoramica**.
 - b. Prendere nota dei valori nelle schede Ripartizione utilizzo spazio dati e Ripartizione utilizzo spazio metadati consentito. Ogni scheda elenca la percentuale di utilizzo dello spazio di archiviazione, la capacità dello spazio utilizzato e lo spazio totale disponibile o consentito dal sito.



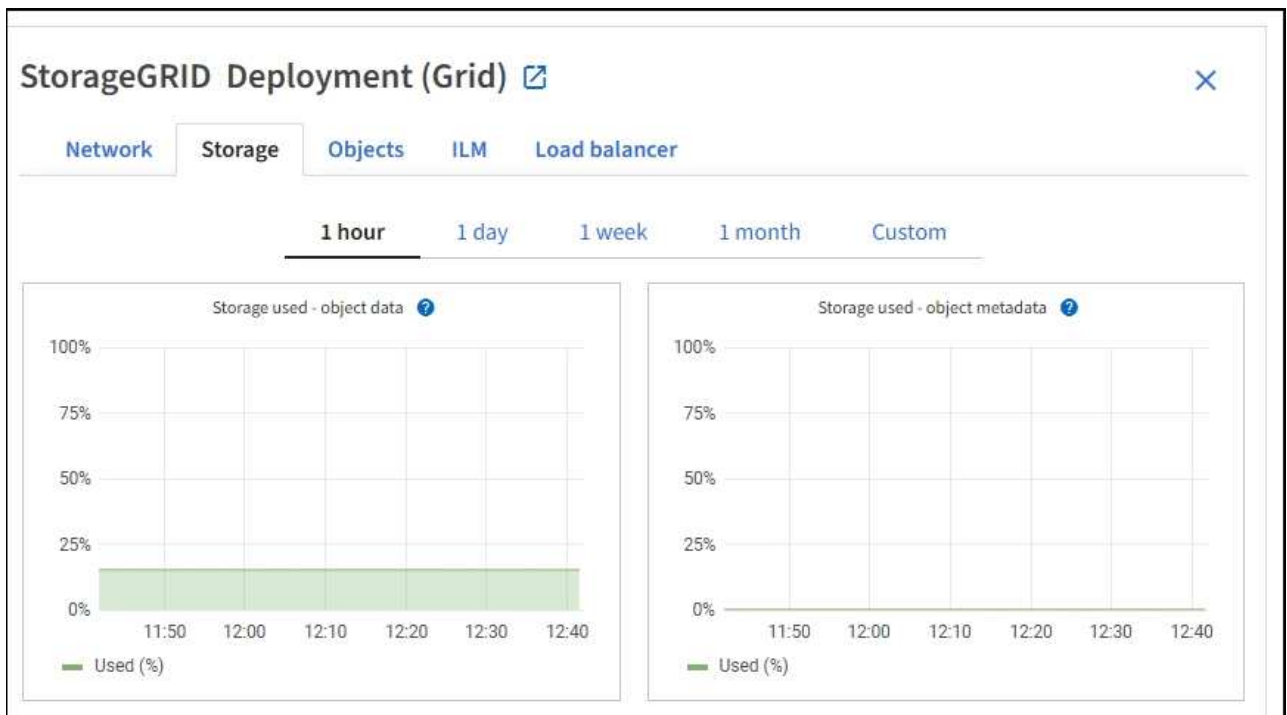
Il riassunto non include supporti d'archivio.



- a. Notare il grafico sulla scheda Conservazione nel tempo. Utilizza il menu a discesa del periodo di tempo per determinare la rapidità con cui viene consumato lo spazio di archiviazione.



2. Utilizzare la pagina Nodi per ulteriori dettagli sulla quantità di spazio di archiviazione utilizzata e su quanto spazio di archiviazione rimane disponibile sulla griglia per i dati degli oggetti e i metadati degli oggetti.
 - a. Selezionare **NODES**.
 - b. Selezionare **grid** > **Archiviazione**.



- c. Posiziona il cursore sui grafici **Spazio di archiviazione utilizzato - dati oggetto** e **Spazio di archiviazione utilizzato - metadati oggetto** per vedere quanto spazio di archiviazione oggetto e spazio di archiviazione metadati oggetto è disponibile per l'intera griglia e quanto è stato utilizzato nel tempo.



I valori totali per un sito o per la griglia non includono i nodi che non hanno segnalato metriche per almeno cinque minuti, come i nodi offline.

3. Pianificare l'esecuzione di un'espansione per aggiungere nodi di archiviazione o volumi di archiviazione prima che la capacità di archiviazione utilizzabile della griglia venga esaurita.

Quando si pianifica la tempistica di un'espansione, bisogna considerare quanto tempo ci vorrà per procurarsi e installare ulteriore spazio di archiviazione.



Se la policy ILM utilizza la codifica di cancellazione, potrebbe essere preferibile espandere quando i nodi di archiviazione esistenti sono pieni al 70% circa, per ridurre il numero di nodi da aggiungere.

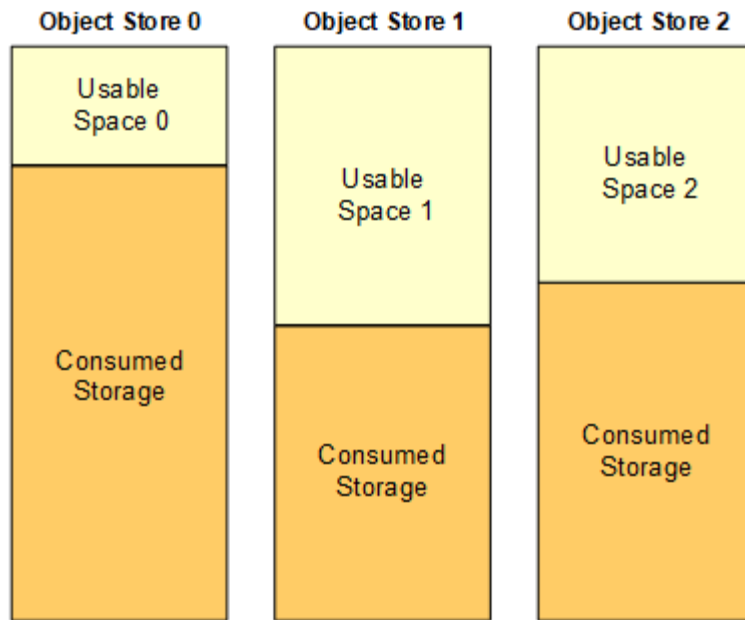
Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, vedere ["Istruzioni per espandere StorageGRID"](#).

Monitorare la capacità di archiviazione per ogni nodo di archiviazione

Monitorare lo spazio totale utilizzabile per ciascun nodo di archiviazione per garantire che il nodo disponga di spazio sufficiente per i nuovi dati degli oggetti.

Informazioni su questo compito

Lo spazio utilizzabile è la quantità di spazio di archiviazione disponibile per riporre gli oggetti. Lo spazio totale utilizzabile per un nodo di archiviazione viene calcolato sommando lo spazio disponibile su tutti gli archivi di oggetti all'interno del nodo.



Total Usable Space = Usable Space 0 + Usable Space 1 + Usable Space 2

Passi

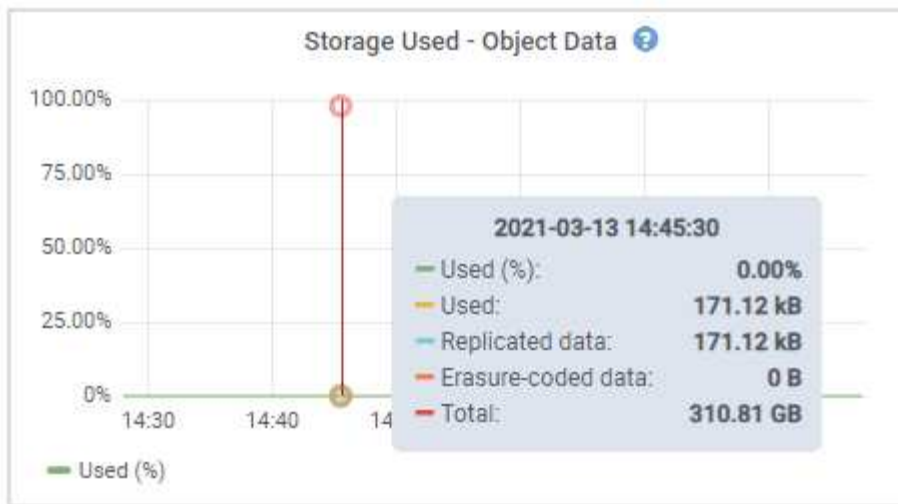
1. Selezionare **NODI** > **Nodo di archiviazione** > **Archiviazione**.

Vengono visualizzati i grafici e le tabelle per il nodo.

2. Posiziona il cursore sul grafico dei dati dell'oggetto Spazio di archiviazione utilizzato.

Vengono mostrati i seguenti valori:

- **Utilizzato (%)**: la percentuale dello spazio utilizzabile totale che è stata utilizzata per i dati dell'oggetto.
- **Utilizzato**: quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
- **Dati replicati**: una stima della quantità di dati di oggetti replicati su questo nodo, sito o griglia.
- **Dati con codice di cancellazione**: una stima della quantità di dati di oggetti con codice di cancellazione su questo nodo, sito o griglia.
- **Totale**: quantità totale di spazio utilizzabile su questo nodo, sito o griglia. Il valore utilizzato è il `storagegrid_storage_utilization_data_bytes` metrica.



3. Esaminare i valori disponibili nelle tabelle Volumi e Archivi 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

- Monitorare i valori nel tempo per stimare la velocità con cui viene consumato lo spazio di archiviazione utilizzabile.
- Per mantenere il normale funzionamento del sistema, aggiungere nodi di archiviazione, aggiungere volumi di archiviazione o archiviare i dati degli oggetti prima che lo spazio utilizzabile venga consumato.

Quando si pianifica la tempistica di un'espansione, bisogna considerare quanto tempo ci vorrà per procurarsi e installare ulteriore spazio di archiviazione.



Se la policy ILM utilizza la codifica di cancellazione, potrebbe essere preferibile espandere quando i nodi di archiviazione esistenti sono pieni al 70% circa, per ridurre il numero di nodi da aggiungere.

Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, vedere ["istruzioni per](#)

[espandere StorageGRID](#) .

IL ["Bassa capacità di archiviazione dei dati degli oggetti"](#) L'avviso viene attivato quando non rimane spazio sufficiente per archiviare i dati degli oggetti su un nodo di archiviazione.

Monitorare la capacità dei metadati degli oggetti per ogni nodo di archiviazione

Monitorare l'utilizzo dei metadati per ciascun nodo di archiviazione per garantire che rimanga disponibile spazio adeguato per le operazioni essenziali del database. È necessario aggiungere nuovi nodi di archiviazione in ogni sito prima che i metadati degli oggetti superino il 100% dello spazio metadati consentito.

Informazioni su questo compito

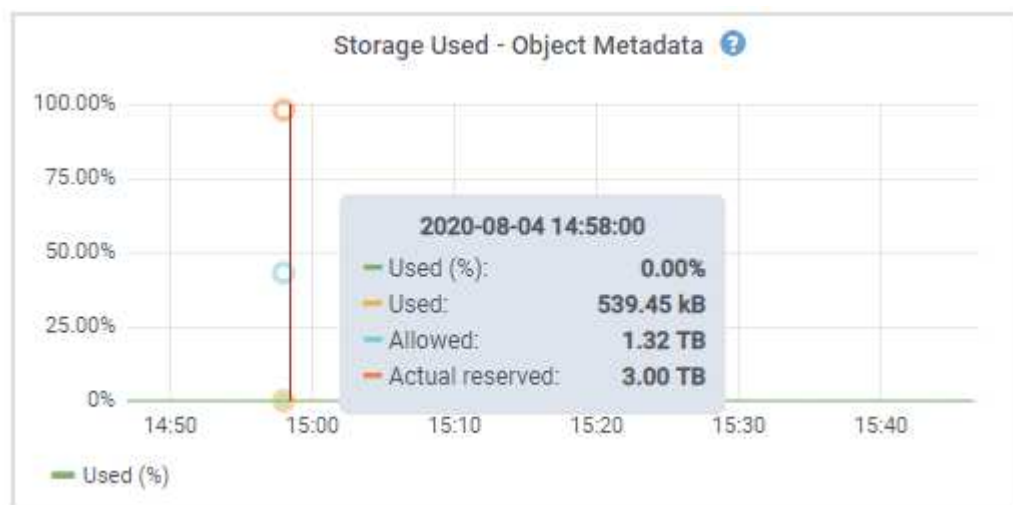
StorageGRID conserva tre copie dei metadati degli oggetti in ogni sito per garantire ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie vengono distribuite uniformemente su tutti i nodi di archiviazione in ciascun sito, utilizzando lo spazio riservato ai metadati sul volume di archiviazione 0 di ciascun nodo di archiviazione.

In alcuni casi, la capacità dei metadati degli oggetti della griglia potrebbe essere consumata più velocemente della sua capacità di archiviazione degli oggetti. Ad esempio, se in genere si acquisiscono grandi quantità di piccoli oggetti, potrebbe essere necessario aggiungere nodi di archiviazione per aumentare la capacità dei metadati, anche se rimane una capacità di archiviazione degli oggetti sufficiente.

Alcuni dei fattori che possono aumentare l'utilizzo dei metadati includono le dimensioni e la quantità di metadati e tag utente, il numero totale di parti in un caricamento multiparte e la frequenza delle modifiche alle posizioni di archiviazione ILM.

Passi

1. Selezionare **NODI > Nodo di archiviazione > Archiviazione**.
2. Posiziona il cursore sul grafico dei metadati dell'oggetto Spazio di archiviazione utilizzato per visualizzare i valori per un periodo di tempo specifico.



Usato (%)

Percentuale dello spazio metadati consentito che è stato utilizzato su questo nodo di archiviazione.

Metriche di Prometheus: `storagegrid_storage_utilization_metadata_bytes` E `storagegrid_storage_utilization_metadata_allowed_bytes`

Usato

I byte dello spazio metadati consentito che sono stati utilizzati su questo nodo di archiviazione.

Metrica di Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Consentito

Lo spazio consentito per i metadati degli oggetti su questo nodo di archiviazione. Per sapere come viene determinato questo valore per ogni nodo di archiviazione, vedere ["descrizione completa dello spazio metadati consentito"](#).

Metrica di Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Effettivo riservato

Lo spazio effettivamente riservato ai metadati su questo nodo di archiviazione. Include lo spazio consentito e lo spazio richiesto per le operazioni essenziali sui metadati. Per sapere come viene calcolato questo valore per ogni nodo di archiviazione, vedere ["descrizione completa dello spazio effettivamente riservato per i metadati"](#).

La metrica Prometheus verrà aggiunta in una versione futura.



I valori totali per un sito o per la griglia non includono i nodi che non hanno segnalato metriche per almeno cinque minuti, come i nodi offline.

- Se il valore **Utilizzato (%)** è pari o superiore al 70%, espandere il sistema StorageGRID aggiungendo nodi di archiviazione a ciascun sito.



L'avviso **Archiviazione metadati insufficiente** viene attivato quando il valore **Utilizzato (%)** raggiunge determinate soglie. Se i metadati degli oggetti utilizzano più del 100% dello spazio consentito, si possono verificare risultati indesiderati.

Quando si aggiungono nuovi nodi, il sistema ribilancia automaticamente i metadati degli oggetti su tutti i nodi di archiviazione all'interno del sito. Vedi il ["istruzioni per espandere un sistema StorageGRID"](#).

Monitorare le previsioni di utilizzo dello spazio

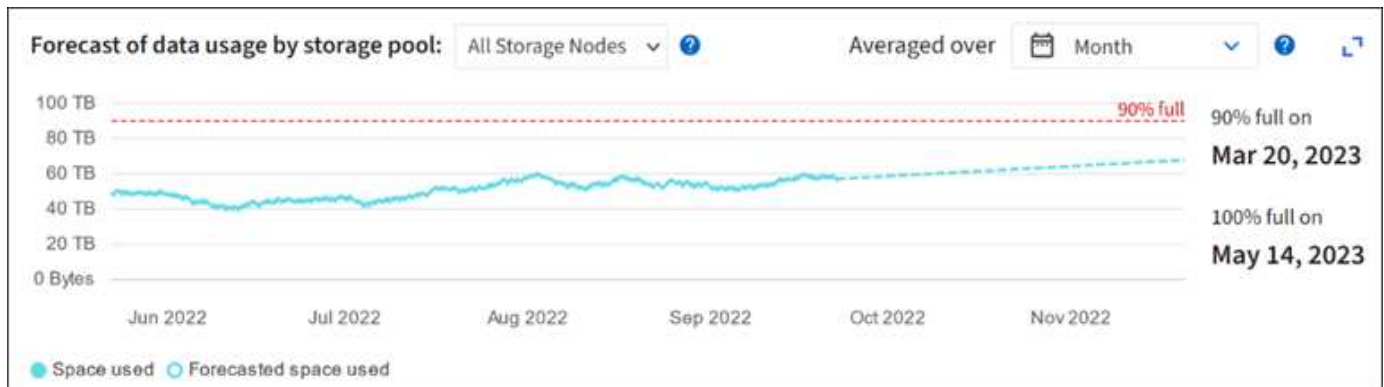
Monitorare le previsioni di utilizzo dello spazio per i dati utente e i metadati per stimare quando sarà necessario ["espandere una griglia"](#).

Se noti che il tasso di consumo cambia nel tempo, seleziona un intervallo più breve dal menu a discesa **Media su** per riflettere solo i modelli di consumo più recenti. Se noti modelli stagionali, seleziona 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.

Passi

- Nella dashboard, seleziona **Archiviazione**.
- Visualizza le schede della dashboard, Previsione dell'utilizzo dei dati per pool di archiviazione e Previsione dell'utilizzo dei metadati per sito.
- Utilizzare questi valori per stimare quando sarà necessario aggiungere nuovi nodi di archiviazione per l'archiviazione di dati e metadati.



Monitorare la gestione del ciclo di vita delle informazioni

Il sistema di gestione del ciclo di vita delle informazioni (ILM) garantisce la gestione dei dati per tutti gli oggetti memorizzati nella griglia. È necessario monitorare le operazioni ILM per capire se la rete è in grado di gestire il carico attuale o se sono necessarie più risorse.

Informazioni su questo compito

Il sistema StorageGRID gestisce gli oggetti applicando le policy ILM attive. Le policy ILM e le regole ILM associate determinano quante copie vengono effettuate, il tipo di copie create, dove vengono posizionate le copie e per quanto tempo ciascuna copia viene conservata.

L'acquisizione di oggetti e altre attività correlate agli oggetti possono superare la velocità con cui StorageGRID può valutare ILM, facendo sì che il sistema metta in coda oggetti le cui istruzioni di posizionamento ILM non possono essere soddisfatte quasi in tempo reale. È necessario monitorare se StorageGRID sta tenendo il passo con le azioni del client.

Utilizzare la scheda dashboard di Grid Manager

Passi

Utilizzare la scheda ILM nella dashboard di Grid Manager per monitorare le operazioni ILM:

1. Sign in a Grid Manager.
2. Dalla dashboard, seleziona la scheda ILM e prendi nota dei valori nella scheda Coda ILM (Oggetti) e nella scheda Velocità di valutazione ILM.

Sono previsti picchi temporanei nella scheda Coda ILM (Oggetti) sulla dashboard. Ma se la coda continua ad aumentare e non diminuisce mai, la griglia ha bisogno di più risorse per funzionare in modo efficiente: più nodi di archiviazione oppure, se la politica ILM colloca gli oggetti in posizioni remote, più larghezza di banda di rete.

Utilizzare la pagina NODI

Passi

Inoltre, esaminare le code ILM utilizzando la pagina **NODES**:



I grafici nella pagina **NODI** verranno sostituiti con le schede della dashboard corrispondenti in una futura versione StorageGRID .

1. Selezionare **NODES**.
2. Selezionare **nome griglia > ILM**.
3. Posiziona il cursore sul grafico della coda ILM per visualizzare il valore dei seguenti attributi in un dato momento:
 - **Oggetti in coda (da operazioni client)**: numero totale di oggetti in attesa di valutazione ILM a causa di operazioni client (ad esempio, acquisizione).
 - **Oggetti in coda (da tutte le operazioni)**: numero totale di oggetti in attesa di valutazione ILM.
 - **Frequenza di scansione (oggetti/sec)**: la velocità con cui gli oggetti nella griglia vengono scansionati e messi in coda per ILM.
 - **Frequenza di valutazione (oggetti/sec)**: la frequenza attuale con cui gli oggetti vengono valutati in base alla policy ILM nella griglia.
4. Nella sezione Coda ILM, osservare i seguenti attributi.



La sezione della coda ILM è inclusa solo per la griglia. Queste informazioni non vengono visualizzate nella scheda ILM per un sito o un nodo di archiviazione.

- **Periodo di scansione - stimato**: 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**: numero totale di operazioni di riparazione degli oggetti per i dati replicati che sono state tentate. Questo conteggio aumenta ogni volta che un nodo di archiviazione tenta di riparare un oggetto ad alto rischio. Le riparazioni ILM ad alto rischio hanno la priorità se la rete diventa sovraccarica.



La riparazione dello stesso oggetto potrebbe incrementarsi nuovamente se la replica fallisce dopo la riparazione.

Questi attributi possono essere utili quando si monitora l'avanzamento del ripristino del volume del nodo di archiviazione. Se il numero di tentativi di riparazione ha smesso di aumentare ed è stata completata una scansione completa, è probabile che la riparazione sia 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 della griglia, sono fondamentali per l'efficienza delle operazioni.

Monitorare le connessioni e le prestazioni di rete

La connettività di rete e la larghezza di banda sono particolarmente importanti se la policy di gestione del ciclo di vita delle informazioni (ILM) copia oggetti replicati tra siti o archivia oggetti con codice di cancellazione utilizzando uno schema che fornisce protezione contro la perdita del sito. Se la rete tra i siti non è disponibile, la latenza di rete è troppo elevata o la larghezza di banda di rete è insufficiente, alcune regole ILM potrebbero non essere in grado di posizionare gli oggetti dove previsto. Ciò può causare errori di acquisizione (quando è selezionata l'opzione di acquisizione rigorosa per le regole ILM) o scarse prestazioni di acquisizione e arretrati ILM.

Utilizza Grid Manager per monitorare la connettività e le prestazioni della rete, in modo da poter risolvere

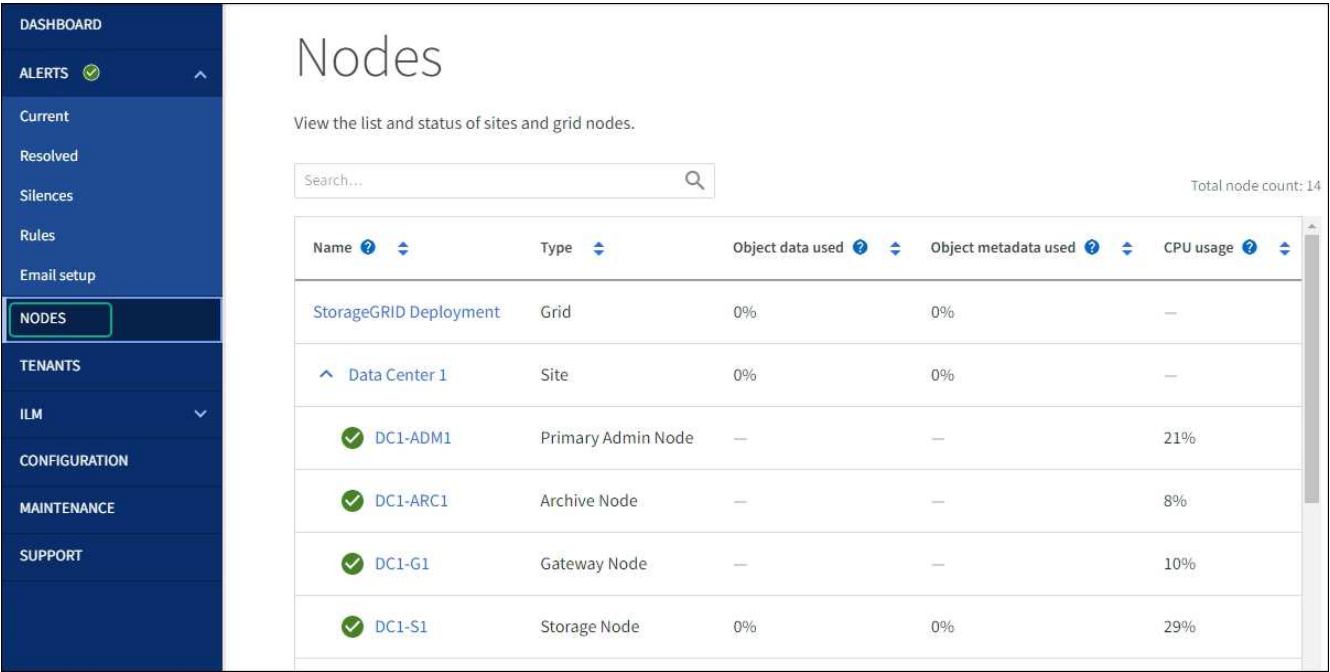
tempestivamente eventuali problemi.

Inoltre, considera "creazione di policy di classificazione del traffico di rete" in modo da poter monitorare il traffico correlato a tenant, bucket, subnet o endpoint del bilanciatore del carico specifici. È possibile impostare criteri di limitazione del traffico in base alle proprie esigenze.

Passi

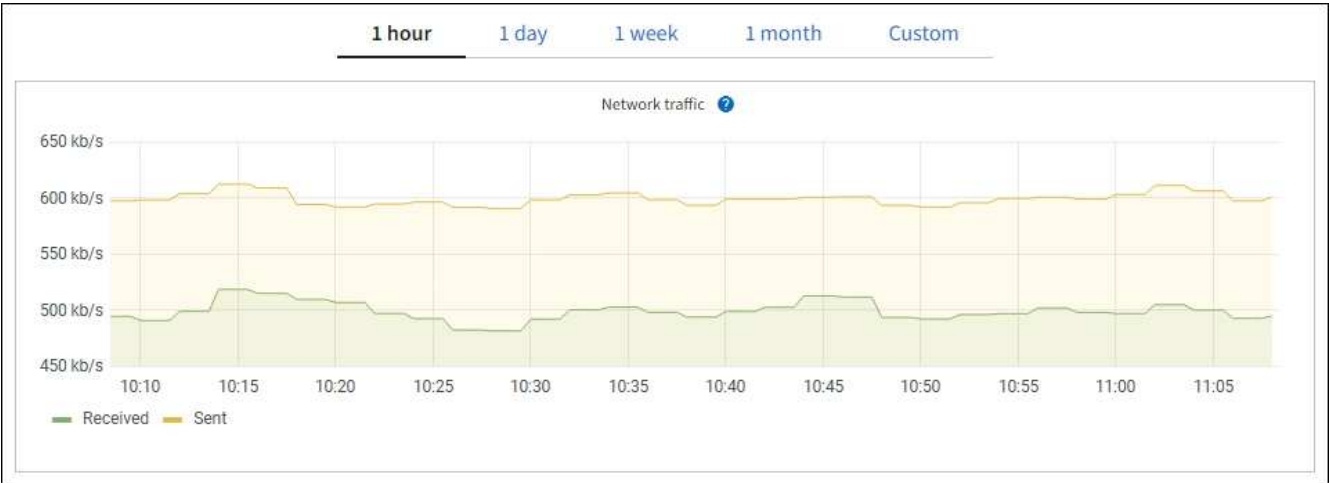
- 1. Selezionare **NODES**.

Viene visualizzata la pagina Nodi. Ogni nodo nella griglia è elencato in formato tabella.



- 2. Selezionare il nome della griglia, un sito specifico del data center o un nodo della griglia, quindi selezionare la scheda **Rete**.

Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo per la griglia nel suo complesso, per il sito del data center o per il nodo.



- a. Se hai selezionato un nodo della griglia, scorri verso il basso per esaminare la sezione **Interfacce di rete** della pagina.

Network interfaces					
Name ?	Hardware address ?	Speed ?	Duplex ?	Auto-negotiation ?	Link status ?
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

- b. Per i nodi della griglia, scorrere verso il basso per esaminare la sezione **Comunicazione di rete** della pagina.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati su 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

3. Utilizza le metriche associate alle tue policy di classificazione del traffico per monitorare il traffico di rete.

- a. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti sono elencati nella tabella.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create Edit ✕ Remove Metrics		
Name	Description	ID
☐ ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒ Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b
Displaying 2 traffic classification policies.		

- a. Per visualizzare i grafici che mostrano le metriche di rete associate a una policy, selezionare il pulsante di opzione a sinistra della policy, quindi fare clic su **Metriche**.
- b. Esaminare i grafici per comprendere il traffico di rete associato alla policy.

Se una policy di classificazione del traffico è progettata per limitare il traffico di rete, analizza la

frequenza con cui il traffico viene limitato e decidi se la policy continua a soddisfare le tue esigenze. Di tanto in tanto, ["adattare ogni politica di classificazione del traffico secondo necessità"](#).

Informazioni correlate

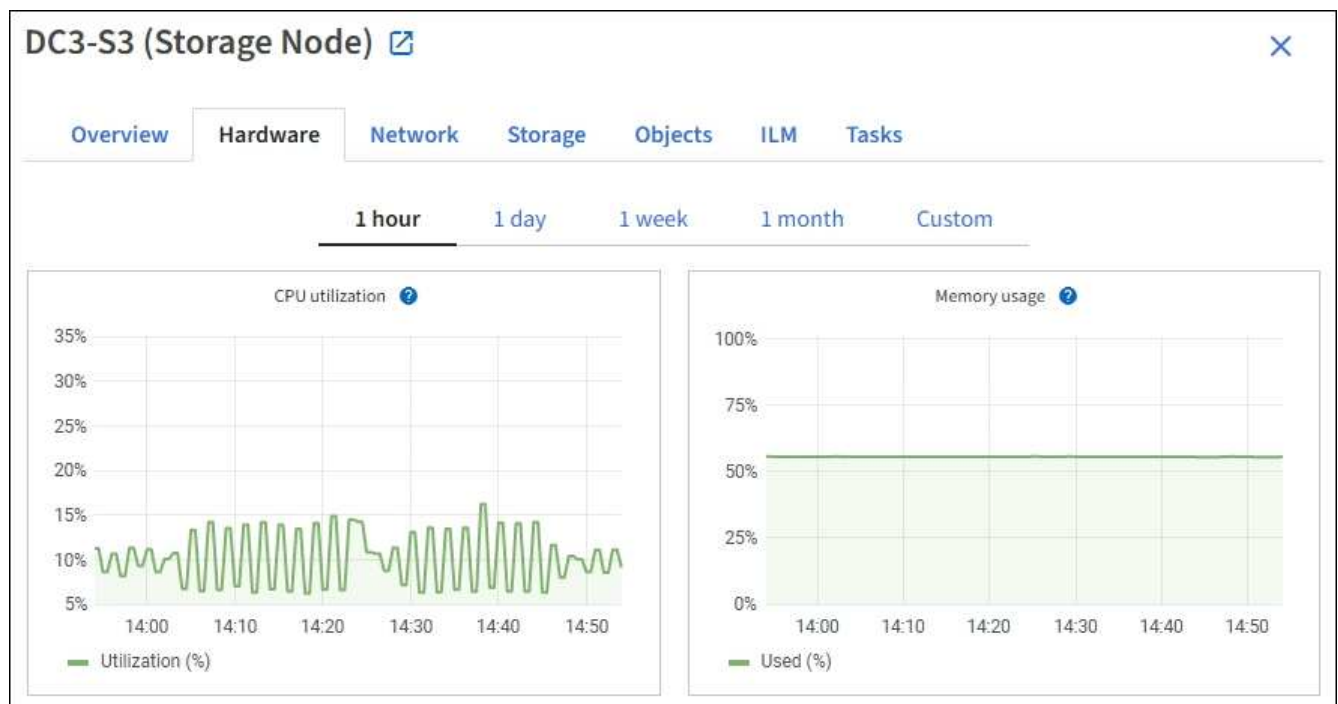
- ["Visualizza la scheda Rete"](#)
- ["Monitorare gli stati di connessione dei nodi"](#)

Monitorare le risorse a livello di nodo

Monitorare i singoli nodi della griglia per verificare i livelli di utilizzo delle risorse. Se i nodi sono costantemente sovraccarichi, potrebbero essere necessari più nodi per operazioni efficienti.

Passi

1. Dalla pagina **NODI**, seleziona il nodo.
2. Selezionare la scheda **Hardware** per visualizzare i grafici dell'utilizzo della CPU e della memoria.



3. Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È anche possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.
4. Se il nodo è ospitato su un'appliance di archiviazione o su un'appliance di servizi, scorrere verso il basso per visualizzare le tabelle dei componenti. Lo stato di tutti i componenti dovrebbe essere "Nominale". Esaminare i componenti che presentano qualsiasi altro stato.

Informazioni correlate

- ["Visualizza informazioni sui nodi di archiviazione dell'appliance"](#)
- ["Visualizza informazioni sui nodi di amministrazione dell'appliance e sui nodi gateway"](#)

Monitorare l'attività degli inquilini

Tutte le attività del client S3 sono associate agli account tenant StorageGRID . È

possibile utilizzare Grid Manager per monitorare l'utilizzo dello storage o il traffico di rete per tutti i tenant o per un tenant specifico. È possibile utilizzare il registro di controllo o le dashboard di Grafana per raccogliere informazioni più dettagliate su come i tenant utilizzano StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Accesso root o autorizzazione account tenant" .

Visualizza tutti gli inquilini

La pagina Inquilini mostra le informazioni di base per tutti gli account degli inquilini attuali.

Passi

1. Selezionare **INQUILINI**.
2. Esaminare le informazioni mostrate nelle pagine dedicate agli inquilini.

Per ogni tenant vengono elencati lo spazio logico utilizzato, l'utilizzo della quota, la quota e il conteggio degli oggetti. Se non è impostata una quota per un tenant, i campi Utilizzo quota e Quota contengono un trattino (—).



I valori dello spazio utilizzato sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

CreateExport to CSVActions

Search tenants by name or ID

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

3. Facoltativamente, accedi a un account tenant selezionando il collegamento di accesso→ nella colonna * Sign in/Copia URL*.
4. Facoltativamente, copia l'URL della pagina di accesso di un tenant selezionando il collegamento Copia URL📄 nella colonna * Sign in/Copia URL*.
5. Facoltativamente, seleziona **Esporta in CSV** per visualizzare ed esportare un .csv file contenente i valori di utilizzo per tutti gli inquilini.

Ti verrà chiesto di aprire o salvare il `.csv` file.

Il contenuto del `.csv` il file appare come nell'esempio seguente:

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

Puoi aprire il `.csv` file in un'applicazione di fogli di calcolo o utilizzarlo nell'automazione.

6. Se non è elencato alcun oggetto, facoltativamente, selezionare **Azioni > Elimina** per rimuovere uno o più tenant. Vedere ["Elimina account inquilino"](#).

Non è possibile rimuovere un account tenant se l'account include bucket o contenitori.

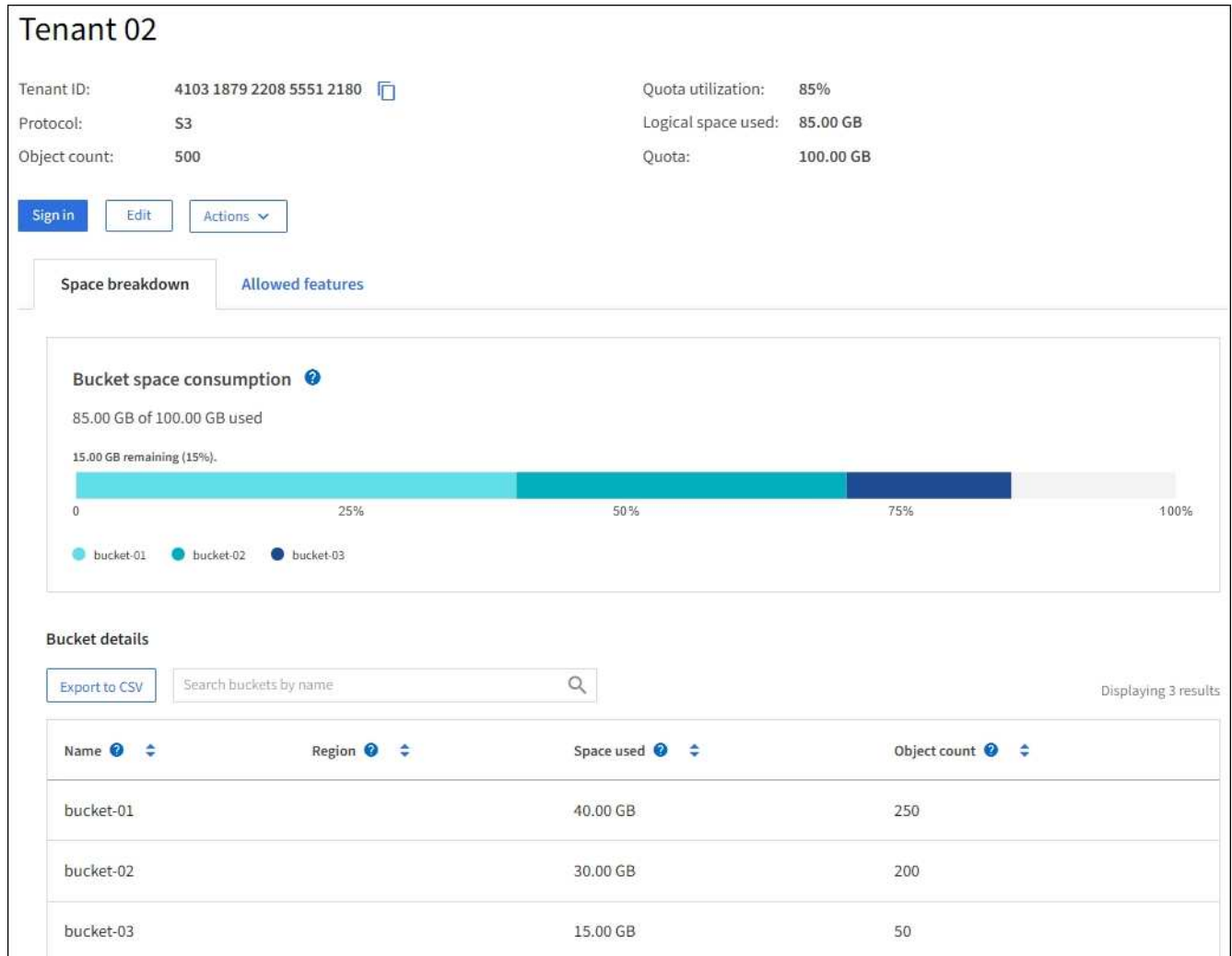
Visualizza un inquilino specifico

È possibile visualizzare i dettagli di un inquilino specifico.

Passi

1. Selezionare il nome dell'inquilino dalla pagina Inquilini.

Viene visualizzata la pagina dei dettagli dell'inquilino.



2. Consulta la panoramica degli inquilini nella parte superiore della pagina.

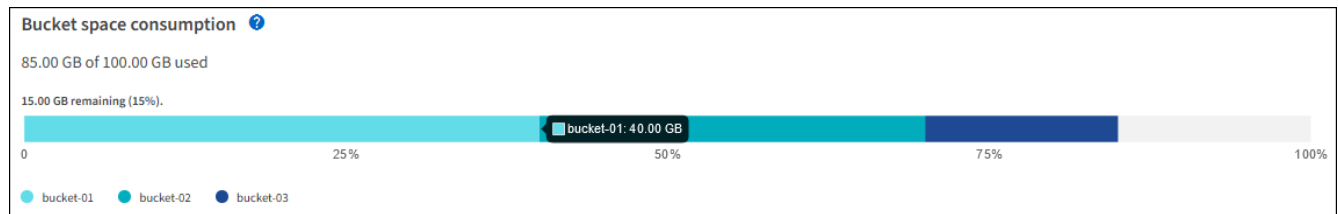
Questa sezione della pagina dei dettagli fornisce informazioni riepilogative per il tenant, tra cui il conteggio degli oggetti del tenant, l'utilizzo della quota, lo spazio logico utilizzato e l'impostazione della quota.

3. Dalla scheda **Ripartizione dello spazio**, esamina il grafico **Consumo di spazio**.

Questo grafico mostra il consumo totale di spazio per tutti i bucket S3 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 utilizzata (ad esempio, 85.00 GB used). Il grafico a barre mostra la percentuale di quota in ciascun bucket o contenitore. Se il tenant ha superato la quota di archiviazione di oltre l'1% e di almeno 1 GB, il grafico mostra la quota totale e la quantità eccedente.

È possibile posizionare il cursore sul grafico a barre per visualizzare lo spazio di archiviazione utilizzato da ciascun bucket o contenitore. È possibile posizionare il cursore sul segmento di spazio libero per visualizzare la quota di archiviazione 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 inizia a caricare oggetti e rifiuta nuovi ingest 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 finché non viene ricalcolato l'utilizzo della quota. I calcoli dell'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 su StorageGRID (dimensione logica). L'utilizzo della quota non rappresenta lo spazio utilizzato per archiviare copie di tali oggetti e dei relativi metadati (dimensioni fisiche).



È possibile abilitare la regola di avviso **Utilizzo elevato della quota tenant** per determinare se i tenant stanno consumando le loro quote. Se abilitato, questo avviso viene attivato quando un tenant ha utilizzato il 90% della sua quota. Per le istruzioni, vedere ["Modifica le regole di avviso"](#).

4. Dalla scheda **Ripartizione dello spazio**, rivedere i **Dettagli del bucket**.

Questa tabella elenca i bucket S3 per il tenant. Lo spazio utilizzato è la quantità totale di dati oggetto nel bucket o nel contenitore. Questo valore non rappresenta lo spazio di archiviazione richiesto per le copie ILM e i metadati degli oggetti.

5. Facoltativamente, seleziona **Esporta in CSV** per visualizzare ed esportare un file .csv contenente i valori di utilizzo per ciascun bucket o contenitore.

Il contenuto di un singolo tenant S3 .csv il file appare come nell'esempio seguente:

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

Puoi aprire il .csv file in un'applicazione di fogli di calcolo o utilizzarlo nell'automazione.

6. Facoltativamente, seleziona la scheda **Funzionalità consentite** per visualizzare un elenco delle autorizzazioni e delle funzionalità abilitate per il tenant. Vedere ["Modifica account inquilino"](#) se è necessario modificare una di queste impostazioni.

7. Se il tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, selezionare facoltativamente la scheda **Federazione griglia** per saperne di più sulla connessione.

Vedere ["Che cos'è la federazione di rete?"](#) E ["Gestire gli inquilini autorizzati per la federazione della rete"](#).

Visualizza il traffico di rete

Se per un tenant sono in atto criteri di classificazione del traffico, esaminare il traffico di rete per quel tenant.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti sono elencati nella tabella.

2. Esaminare l'elenco delle policy per identificare quelle che si applicano a un inquilino specifico.
3. Per visualizzare le metriche associate a una policy, selezionare il pulsante di opzione a sinistra della policy e selezionare **Metriche**.
4. Analizza i grafici per determinare la frequenza con cui la policy limita il traffico e se è necessario modificarla.

Vedere ["Gestire le policy di classificazione del traffico"](#) per maggiori informazioni.

Utilizzare il registro di controllo

Facoltativamente, è possibile utilizzare il registro di controllo per un monitoraggio più dettagliato 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 client

I registri di controllo vengono scritti in file di testo che è possibile analizzare utilizzando lo strumento di analisi dei registri scelto. Ciò consente di comprendere meglio le attività dei clienti o di implementare modelli sofisticati di addebito e fatturazione.

Vedere ["Esaminare i registri di controllo"](#) per maggiori informazioni.

Utilizzare le metriche di Prometheus

Facoltativamente, utilizzare le metriche di Prometheus per generare report sull'attività dei tenant.

- Nel Grid Manager, seleziona **SUPPORTO > Strumenti > Metriche**. È possibile utilizzare dashboard esistenti, come S3 Overview, per esaminare le attività dei clienti.



Gli strumenti disponibili nella pagina Metriche sono destinati principalmente all'uso da parte del supporto tecnico. Alcune funzionalità e voci di menu di questi strumenti sono intenzionalmente non funzionali.

- Nella parte superiore di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API**. È possibile utilizzare le metriche nella sezione Metriche dell'API di gestione della griglia per creare regole di avviso e dashboard personalizzate per l'attività dei tenant.

Vedere ["Esaminare le metriche di supporto"](#) per maggiori informazioni.

Monitorare le operazioni del client S3

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

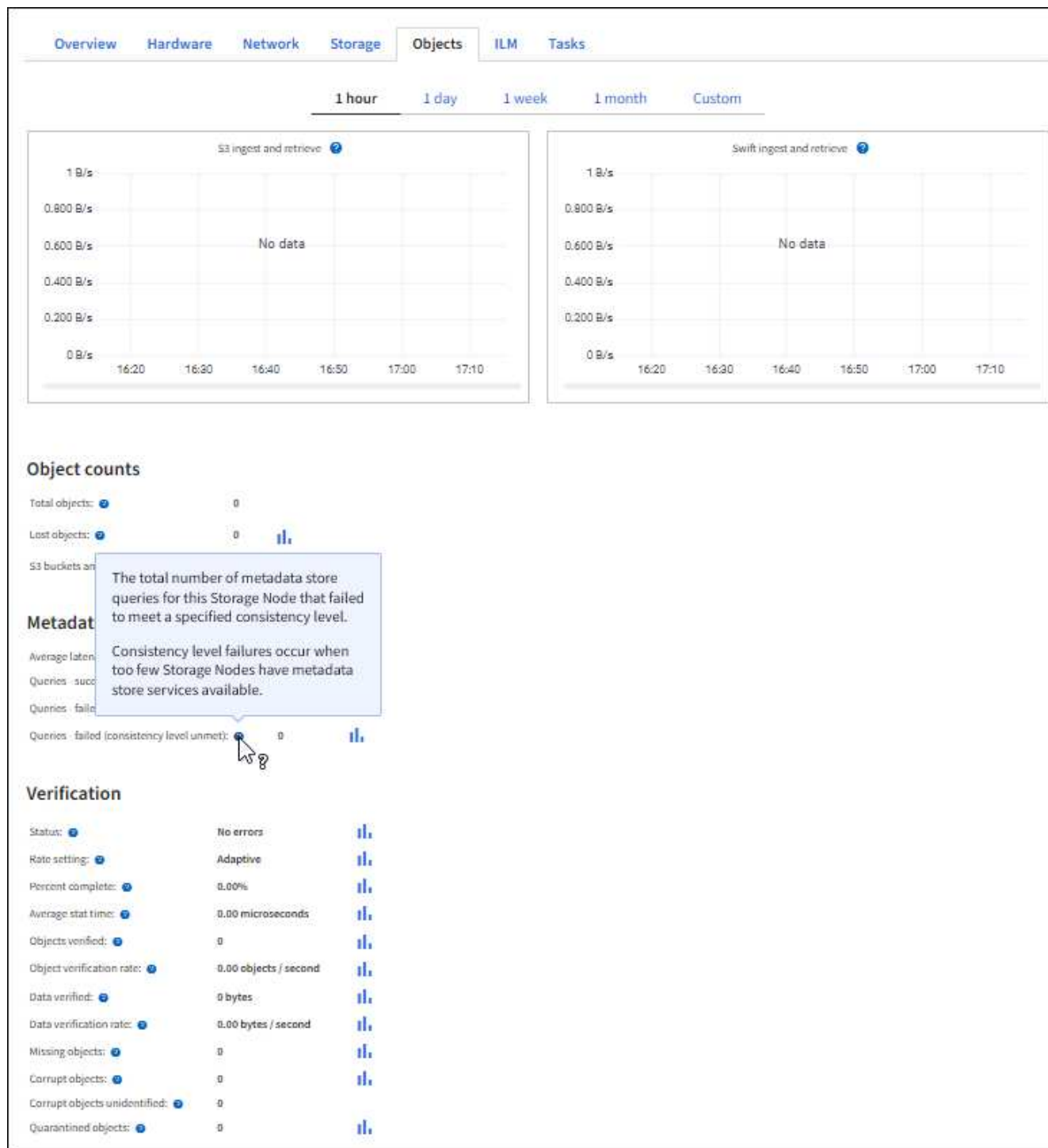
Passi

1. Dalla dashboard, seleziona la scheda **Prestazioni**.
2. Fare riferimento ai grafici S3, che riepilogano il numero di operazioni client eseguite dai nodi di archiviazione e il numero di richieste API ricevute dai nodi di archiviazione durante l'intervallo di tempo selezionato.
3. Selezionare **NODI** per accedere alla pagina Nodi.
4. Dalla home page dei Nodi (livello griglia), seleziona la scheda **Oggetti**.

Il grafico mostra le velocità di acquisizione e recupero S3 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 particolare nodo di archiviazione, seleziona il nodo dall'elenco a sinistra e seleziona la scheda **Oggetti**.

Il grafico mostra le velocità di acquisizione e recupero per il nodo. La scheda include anche metriche per il conteggio degli oggetti, le query sui metadati e le operazioni di verifica.



Monitorare le operazioni di bilanciamento del carico

Se si utilizza un bilanciatore del carico per gestire le connessioni client a StorageGRID, è necessario monitorare le operazioni di bilanciamento del carico dopo aver configurato inizialmente il sistema e dopo aver apportato modifiche alla configurazione o eseguito un'espansione.

Informazioni su questo compito

È possibile utilizzare il servizio Load Balancer sui nodi amministrativi o sui nodi gateway oppure un bilanciatore del carico esterno di terze parti per distribuire le richieste client su più nodi di archiviazione.

Dopo aver configurato il bilanciamento del carico, è necessario verificare che le operazioni di acquisizione e recupero degli oggetti siano distribuite uniformemente tra i nodi di archiviazione. Le richieste distribuite uniformemente garantiscono che StorageGRID rimanga reattivo alle richieste dei client sotto carico e possono contribuire a mantenere le prestazioni dei client.

Se è stato configurato un gruppo ad alta disponibilità (HA) di nodi gateway o nodi amministrativi in modalità di backup attivo, solo un nodo nel gruppo distribuisce attivamente le richieste client.

Per ulteriori informazioni, consultare ["Configurare le connessioni client S3"](#).

Passi

1. Se i client S3 si connettono tramite il servizio Load Balancer, verificare che i nodi amministrativi o i nodi gateway distribuiscono attivamente il traffico come previsto:

- a. Selezionare **NODES**.
- b. Selezionare un nodo gateway o un nodo amministrativo.
- c. Nella scheda **Panoramica**, verificare se un'interfaccia nodo si trova in un gruppo HA e se l'interfaccia 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 dovrebbe distribuire attivamente le richieste dei client, selezionare ["Scheda Bilanciatore del carico"](#).
- e. Esaminare il grafico del traffico delle richieste del Load Balancer dell'ultima settimana per assicurarsi che il nodo abbia distribuito attivamente le richieste.

I nodi in 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 della frequenza delle richieste in arrivo del Load Balancer dell'ultima settimana per esaminare la produttività degli oggetti del nodo.
 - g. Ripetere questi passaggi per ogni nodo amministrativo o nodo gateway nel sistema StorageGRID.
 - h. Facoltativamente, utilizzare i criteri di classificazione del traffico per visualizzare un'analisi più dettagliata del traffico servito dal servizio Load Balancer.
2. Verificare che queste richieste vengano distribuite uniformemente tra i nodi di archiviazione.
 - a. Selezionare **Nodo di archiviazione > LDR > HTTP**.
 - b. Esaminare il numero di **Sessioni in arrivo attualmente stabilite**.
 - c. Ripetere l'operazione per ogni nodo di archiviazione nella griglia.

Il numero di sessioni dovrebbe essere più o meno uguale su tutti i nodi di archiviazione.

Monitorare le connessioni della federazione di rete

È possibile monitorare le informazioni di base su tutti ["connessioni della federazione di rete"](#), informazioni dettagliate su una connessione specifica o metriche Prometheus sulle operazioni di replicazione tra griglie. È possibile monitorare una connessione da entrambe le griglie.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su entrambe le griglie utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) per la griglia a cui hai effettuato l'accesso.

Visualizza tutte le connessioni

La pagina Federazione di griglia mostra informazioni di base su tutte le connessioni di federazione di griglia e su tutti gli account tenant autorizzati a utilizzare le connessioni di federazione di griglia.

Passi

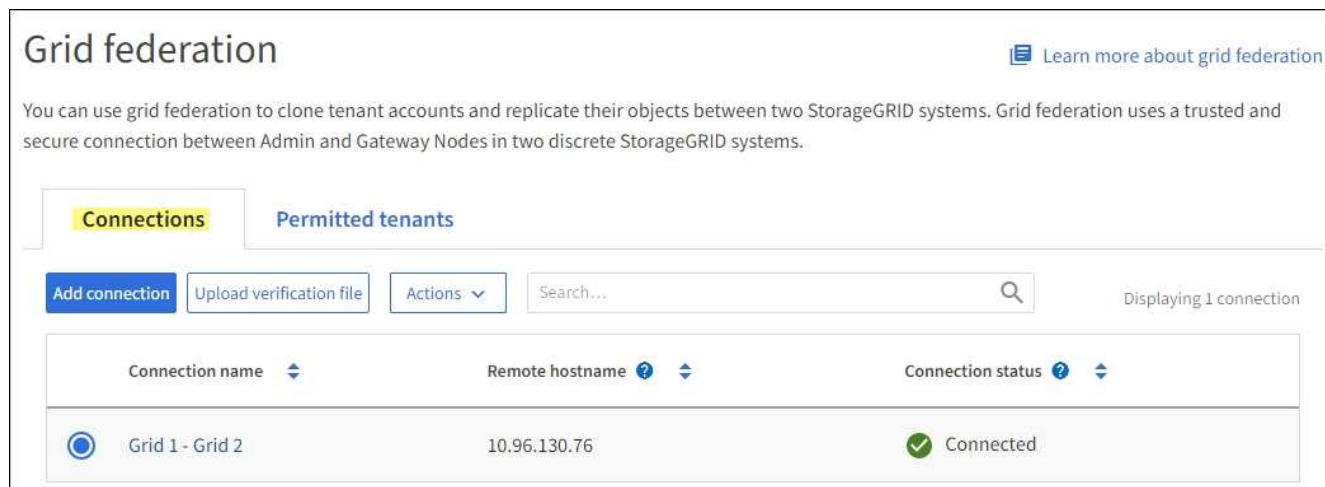
1. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.

Viene visualizzata la pagina Federazione Grid.

2. Per visualizzare le informazioni di base per tutte le connessioni su questa griglia, selezionare la scheda **Connessioni**.

Da questa scheda puoi:

- ["Crea una nuova connessione"](#) .
- Seleziona una connessione esistente a ["modificare o testare"](#) .



The screenshot shows the 'Grid federation' page with the 'Connections' tab selected. The page title is 'Grid federation' with a link to 'Learn more about grid federation'. Below the title is a descriptive paragraph: 'You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.' The 'Connections' tab is highlighted in yellow. Below the tabs are buttons for 'Add connection', 'Upload verification file', and 'Actions'. A search bar is also present. The table below shows one connection: 'Grid 1 - Grid 2' with remote hostname '10.96.130.76' and status 'Connected'.

Connection name	Remote hostname	Connection status
Grid 1 - Grid 2	10.96.130.76	Connected

3. Per visualizzare le informazioni di base per tutti gli account tenant su questa griglia che dispongono dell'autorizzazione **Usa connessione federata griglia**, selezionare la scheda **Tenant autorizzati**.

Da questa scheda puoi:

- ["Visualizza la pagina dei dettagli per ogni inquilino autorizzato"](#) .
- Visualizza la pagina dei dettagli per ogni connessione. Vedere [Visualizza una connessione specifica](#) .
- Selezionare un inquilino autorizzato e ["rimuovere il permesso"](#) .
- Verificare la presenza di errori di replicazione tra griglie e cancellare l'ultimo errore, se presente. Vedere ["Risolvere gli errori di federazione della griglia"](#) .

Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

[Connections](#)
[Permitted tenants](#)

[Remove permission](#)
[Clear error](#)

Displaying one result

Tenant name	Connection name	Connection status	Remote grid hostname	Last error
Tenant A	Grid 1 - Grid 2	Connected	10.96.130.76	Check for errors

Visualizza una connessione specifica

È possibile visualizzare i dettagli di una specifica connessione di federazione di rete.

Passi

1. Selezionare una delle schede dalla pagina Federazione della griglia, quindi selezionare il nome della connessione dalla tabella.

Dalla pagina dei dettagli della connessione, puoi:

- Visualizza le informazioni di base sullo stato della connessione, inclusi i nomi host locali e remoti, la porta e lo stato della connessione.
- Seleziona una connessione a ["modificare, testare o rimuovere"](#).

2. Quando si visualizza una connessione specifica, selezionare la scheda **Tenant consentiti** per visualizzare i dettagli sui tenant consentiti per la connessione.

Da questa scheda puoi:

- ["Visualizza la pagina dei dettagli per ogni inquilino autorizzato"](#).
- ["Rimuovere l'autorizzazione di un inquilino"](#) per utilizzare la connessione.
- Verificare la presenza di errori di replicazione tra griglie e cancellare l'ultimo errore. Vedere ["Risolvere gli errori di federazione della griglia"](#).

Grid 1 - Grid 2

Local hostname (this grid):

10.96.130.64

Port:

23000

Remote hostname (other grid):

10.96.130.76

Connection status:

✓

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Remove permission

Clear error

Search...

Displaying one result

Tenant name	Last error
Tenant A	Check for errors

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 puoi:

- ["Ruota i certificati di connessione"](#) .
- Selezionare **Server** o **Client** per visualizzare o scaricare il certificato associato o copiare il certificato PEM.

Grid A-Grid B

Local hostname (this grid):10.96.106.230

Port:23000

Remote hostname (other grid):10.96.104.230

Connection status:

✔ Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Rotate certificates

Server

Client

Download certificate

Copy certificate PEM

Metadata ?

Subject DN:/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230

Serial number:30:81:B8:DD:AE:B2:86:0A

Issuer DN:/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT

Issued on:2022-10-04T02:21:18.000Z

Expires on:2024-10-03T19:05:13.000Z

SHA-1 fingerprint:92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF

SHA-256 fingerprint:54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60

Alternative names:IP Address:10.96.106.230

Certificate PEM ?

-----BEGIN CERTIFICATE-----

MIIGdTCCBF2gAwIBAgIIMIG43a6yhgowDQYJKoZIhvcNAQENBQAwdzELMAkGA1UE

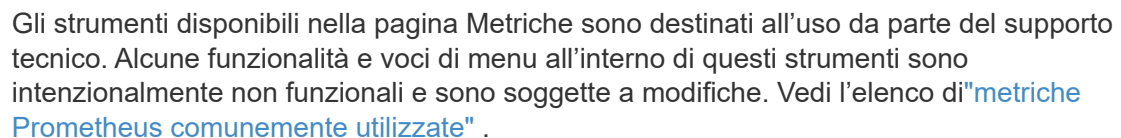
BhMCVVMxExZARBgNVBAGhNCKNhbg1mb3JuaWExEjAQBGNVBAcMCVN1bm55dmFsZTEU

NETAPPSUNNYVAZBGNVBAcMCVF1dEFjCRAQgggVwJIR3J1

-----END CERTIFICATE-----

È possibile utilizzare la dashboard Cross-Grid Replication in Grafana per visualizzare le metriche di Prometheus sulle operazioni di replica cross-grid sulla propria griglia.

1. Da Grid Manager, seleziona **SUPPORTO** > **Strumenti** > **Metriche**.



- Per istruzioni dettagliate, vedere ["Esaminare le metriche di supporto"](#).

3. Per riprovare la replica degli oggetti che non sono riusciti a replicare, vedere ["Identificare e riprovare le operazioni di replicazione non riuscite"](#) .

Gestisci gli avvisi

Gestisci gli avvisi

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

Gli avvisi vengono attivati a livelli di gravità specifici quando le condizioni delle regole di avviso vengono valutate come vere. Quando viene attivato un avviso, si verificano le seguenti azioni:

- Un'icona di gravità dell'avviso viene visualizzata sulla dashboard di Grid Manager e il conteggio degli avvisi correnti viene incrementato.
- L'avviso viene visualizzato nella pagina di riepilogo **NODES** e nella scheda **NODES > node > Panoramica**.
- Verrà inviata una notifica via e-mail, presupponendo che sia stato configurato un server SMTP e siano stati forniti gli indirizzi e-mail dei destinatari.
- Viene inviata una notifica SNMP (Simple Network Management Protocol), presupponendo che sia stato configurato l'agente SNMP StorageGRID .

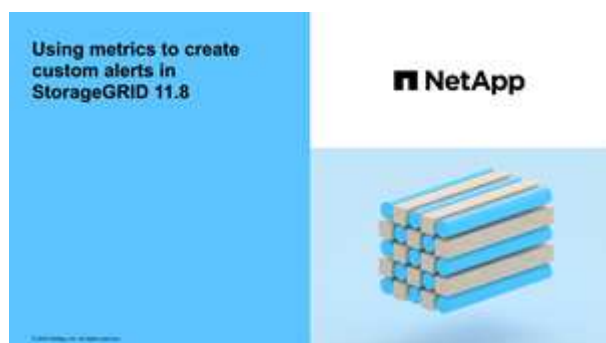
È possibile creare avvisi personalizzati, modificare o disattivare gli avvisi e gestire le notifiche degli avvisi.

Per saperne di più:

- Rivedi il video: ["Video: Panoramica degli avvisi"](#)



- Rivedi il video: ["Video: avvisi personalizzati"](#)



- Vedi il ["Riferimento avvisi"](#) .

Visualizza le regole di avviso

Le regole di avviso definiscono le condizioni che attivano "avvisi specifici" . StorageGRID include un set di regole di avviso predefinite, che è possibile utilizzare così come sono 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 alcuni avvisi sono disabilitati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Gestisci avvisi o autorizzazione di accesso root" .
- Facoltativamente, hai guardato il video: "Video: Panoramica degli avvisi"



Passi

1. Selezionare **AVVISI > Regole.**

Viene visualizzata la pagina Regole di avviso.

Alert Rules [Learn more](#)

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

+ Create custom rule Edit rule Remove custom rule

Name	Conditions	Type	Status
☐ Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0	Default	Enabled
☐ Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0	Default	Enabled
☐ Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0	Default	Enabled
☐ Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0	Default	Enabled
☐ Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0	Default	Enabled
☐ Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0	Default	Enabled
☐ Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0	Default	Enabled
☐ Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0	Default	Enabled
☐ Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0	Default	Enabled
☐ Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0	Default	Enabled

Displaying 62 alert rules.

2. Esaminare le informazioni nella tabella delle regole di avviso:

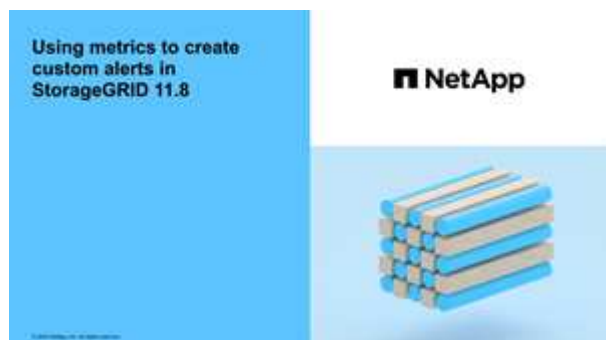
Intestazione di colonna	Descrizione
Nome	Nome e descrizione univoci della regola di avviso. Per prime vengono elencate le regole di avviso personalizzate, seguite dalle regole di avviso predefinite. Il nome della regola di avviso è l'oggetto delle notifiche e-mail.
Condizioni	Le espressioni di Prometheus che determinano quando viene attivato questo avviso. Un avviso può essere attivato a uno o più dei seguenti livelli di gravità, ma non è richiesta una condizione per ciascun livello di gravità. • *Critico*  : Si è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID . Bisogna affrontare immediatamente il problema di fondo. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati. • *Maggiore*  : Esiste una condizione anomala che sta influenzando le operazioni in corso o che si sta avvicinando alla soglia di un avviso critico. È necessario esaminare gli avvisi principali e risolvere eventuali problemi sottostanti per garantire che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID . • *Minore*  : Il sistema funziona normalmente, ma si verifica una condizione anomala che potrebbe compromettere la capacità del sistema di funzionare se continua così. È opportuno monitorare e risolvere gli avvisi minori che non si risolvono da soli, per evitare che diano origine a problemi più seri.
Tipo	Tipo di regola di avviso: • Predefinito: una regola di avviso fornita con il sistema. È possibile disattivare una regola di avviso predefinita o modificarne le condizioni e la durata. Non è possibile rimuovere una regola di avviso predefinita. • Predefinito*: una regola di avviso predefinita che include una condizione o una durata modificata. Se necessario, è possibile ripristinare facilmente una condizione modificata riportandola al valore predefinito originale. • Personalizzato: una regola di avviso creata da te. È possibile disattivare, modificare e rimuovere le regole di avviso personalizzate.
Stato	Indica se questa regola di avviso è attualmente abilitata o disabilitata. Le condizioni per le regole di avviso disabilitate non vengono valutate, quindi non vengono attivati avvisi.

Crea regole di avviso personalizzate

È possibile creare regole di avviso personalizzate per definire le condizioni di attivazione degli avvisi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Gestisci avvisi o autorizzazione di accesso root"](#) .
- Hai familiarità con il ["metriche Prometheus comunemente utilizzate"](#) .
- Tu capisci il ["sintassi delle query di Prometheus"](#) .
- Facoltativamente, hai guardato il video: ["Video: avvisi personalizzati"](#) .



Informazioni su questo compito

StorageGRID non convalida gli avvisi personalizzati. Se decidi di creare regole di avviso personalizzate, segui queste linee guida generali:

- Esamina le condizioni per le regole di avviso predefinite e usale come esempi per le tue 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 soglia per ogni condizione.
- Controllare attentamente ogni condizione per individuare eventuali errori di battitura e logici.
- Utilizzare solo le metriche elencate nell'API di gestione della griglia.
- Quando si testa un'espressione utilizzando l'API di gestione della griglia, tenere presente che una risposta "riuscita" potrebbe essere un corpo di risposta vuoto (nessun avviso attivato). Per verificare se l'avviso viene effettivamente attivato, puoi impostare temporaneamente una soglia su un valore che al momento ti aspetti sia vero.

Ad esempio, per testare l'espressione `node_memory_MemTotal_bytes < 24000000000` , prima esegui `node_memory_MemTotal_bytes >= 0` e assicurati di ottenere i risultati previsti (tutti i nodi restituiscono un valore). Quindi, riportare l'operatore e la soglia ai valori desiderati ed eseguire nuovamente. Nessun risultato indica che non ci sono avvisi correnti per questa espressione.

- Non dare per scontato che un avviso personalizzato funzioni, a meno che tu non abbia verificato che l'avviso venga attivato quando previsto.

Passi

1. Selezionare **AVVISI > Regole**.

Viene visualizzata la pagina Regole di avviso.

2. Seleziona **Crea regola personalizzata**.

Viene visualizzata la finestra di dialogo Crea regola personalizzata.

Create Custom Rule

Enabled ☒

Unique Name

Description

Recommended Actions
(optional)

Conditions

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

minutes

Cancel

Save

3. Selezionare o deselezionare la casella di controllo **Abilitato** per determinare se questa regola di avviso è attualmente abilitata.

Se una regola di avviso è disabilitata, le sue espressioni non vengono valutate e non viene attivato alcun avviso.

4. Inserisci le seguenti informazioni:

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi e costituisce anche l'oggetto delle notifiche e-mail. I nomi per le regole di avviso possono avere una lunghezza compresa tra 1 e 64 caratteri.

Campo	Descrizione
Descrizione	Una descrizione del problema che si sta verificando. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono contenere da 1 a 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Inserisci le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono avere una lunghezza compresa 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 solitamente della forma:

```
[metric] [operator] [value]
```

Le espressioni possono avere qualsiasi lunghezza, ma devono essere visualizzate su una singola riga nell'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 di byte (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

Per visualizzare le metriche disponibili e testare le espressioni di Prometheus, seleziona l'icona della guida  e seguire il collegamento alla sezione Metriche dell'API di gestione della griglia.

6. Nel campo **Durata**, immettere la quantità di tempo per cui una condizione deve rimanere in vigore ininterrottamente prima che venga attivato l'avviso e selezionare un'unità di tempo.

Per attivare immediatamente un avviso quando una condizione diventa vera, immettere **0**. Aumentare questo valore per evitare che condizioni temporanee attivino avvisi.

Il valore predefinito è 5 minuti.

7. Seleziona **Salva**.

La finestra di dialogo si chiude e la nuova regola di avviso personalizzata viene visualizzata nella tabella Regole di avviso.

Modifica le regole di avviso

È possibile modificare una regola di avviso per cambiare 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"](#).

- Tu hai il "[Gestisci avvisi o autorizzazione di accesso root](#)".

Informazioni su questo compito

Quando modifichi una regola di avviso predefinita, puoi cambiare le condizioni per gli avvisi minori, maggiori e critici, nonché la durata. Quando modifichi una regola di avviso personalizzata, puoi anche modificarne il nome, la descrizione e le azioni consigliate.



Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, è possibile che non venga rilevato un problema di fondo finché non si impedisce il completamento di un'operazione critica.

Passi

1. Selezionare **AVVISI > Regole**.

Viene visualizzata la pagina Regole di avviso.

2. Selezionare il pulsante di opzione per la regola di avviso che si desidera modificare.
3. Seleziona **Modifica regola**.

Viene visualizzata la finestra di dialogo Modifica regola. Questo esempio mostra una regola di avviso predefinita: i campi Nome univoco, Descrizione e Azioni consigliate sono disabilitati e non possono essere modificati.

Edit Rule - Low installed node memory

Enabled ☒

Unique Name

Description

Recommended Actions (optional)

Conditions 

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

4. Selezionare o deselezionare la casella di controllo **Abilitato** per determinare se questa regola di avviso è attualmente abilitata.

Se una regola di avviso è disabilitata, le sue espressioni non vengono valutate e non viene attivato alcun avviso.



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, non è consigliabile disabilitare una regola di avviso predefinita. Se una regola di avviso è disabilitata, potresti non rilevare un problema di fondo finché non impedisce il completamento di un'operazione critica.

5. Per le regole di avviso personalizzate, aggiornare le seguenti informazioni secondo necessità.



Non è possibile 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 e costituisce anche l'oggetto delle notifiche e-mail. I nomi per le regole di avviso possono avere una lunghezza compresa tra 1 e 64 caratteri.
Descrizione	Una descrizione del problema che si sta verificando. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono contenere da 1 a 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Inserisci le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono avere una lunghezza compresa 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 una condizione per una regola di avviso predefinita modificata al suo valore originale, selezionare i tre punti a destra della condizione modificata.

Conditions ⓘ

Minor	
Major	node_memory_MemTotal_bytes < 24000000000
Critical	node_memory_MemTotal_bytes <= 14000000000



Se si aggiornano le condizioni per un avviso corrente, le modifiche potrebbero non essere implementate finché non verrà risolta la condizione precedente. La prossima volta che verrà soddisfatta una delle condizioni della regola, l'avviso rifletterà i valori aggiornati.

Un'espressione di base è solitamente della forma:

```
[metric] [operator] [value]
```

Le espressioni possono avere qualsiasi lunghezza, ma devono essere visualizzate su una singola riga nell'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 di byte (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

7. Nel campo **Durata**, immettere la quantità di tempo per cui una condizione deve rimanere in vigore ininterrottamente prima che venga attivato l'avviso e selezionare l'unità di tempo.

Per attivare immediatamente un avviso quando una condizione diventa vera, immettere **0**. Aumentare questo valore per evitare che condizioni temporanee attivino avvisi.

Il valore predefinito è 5 minuti.

8. Seleziona **Salva**.

Se hai modificato una regola di avviso predefinita, nella colonna Tipo verrà visualizzato **Predefinito***. Se hai disabilitato una regola di avviso predefinita o personalizzata, nella colonna **Stato** apparirà **Disabilitato**.

Disabilita le regole di avviso

È possibile modificare lo stato abilitato/disabilitato per una regola di avviso predefinita o personalizzata.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Gestisci avvisi o autorizzazione di accesso root"](#).

Informazioni su questo compito

Quando una regola di avviso è disabilitata, le sue espressioni non vengono valutate e non viene attivato alcun avviso.



In generale, non è consigliabile disabilitare una regola di avviso predefinita. Se una regola di avviso è disabilitata, potresti non rilevare un problema di fondo finché non impedisce il completamento di un'operazione critica.

Passi

1. Selezionare **AVVISI > Regole**.

Viene visualizzata la pagina Regole di avviso.

2. Selezionare il pulsante di opzione per la regola di avviso che si desidera disabilitare o abilitare.

3. Seleziona **Modifica regola**.

Viene visualizzata la finestra di dialogo Modifica regola.

4. Selezionare o deselezionare la casella di controllo **Abilitato** per determinare se questa regola di avviso è attualmente abilitata.

Se una regola di avviso è disabilitata, le sue espressioni non vengono valutate e non viene attivato alcun avviso.



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. Seleziona **Salva**.

Nella colonna **Stato** appare **Disabilitato**.

Rimuovi 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"](#) .
- Tu hai il ["Gestisci avvisi o autorizzazione di accesso root"](#) .

Passi

1. Selezionare **AVVISI > Regole**.

Viene visualizzata la pagina Regole di avviso.

2. Seleziona il pulsante di opzione per la regola di avviso personalizzata che desideri rimuovere.

Non è possibile rimuovere una regola di avviso predefinita.

3. Seleziona **Rimuovi regola personalizzata**.

Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **OK** per rimuovere la regola di avviso.

Eventuali istanze attive dell'avviso verranno risolte entro 10 minuti.

Gestisci le notifiche di avviso

Imposta le notifiche SNMP per gli avvisi

Se si desidera che StorageGRID invii notifiche SNMP quando si verificano avvisi, è necessario abilitare l'agente SNMP StorageGRID e configurare una o più destinazioni trap.

È possibile utilizzare l'opzione **CONFIGURAZIONE > Monitoraggio > Agente SNMP** in Grid Manager o gli endpoint SNMP per l'API di gestione della griglia per abilitare e configurare l'agente SNMP StorageGRID . L'agente SNMP supporta tutte e tre le versioni del protocollo SNMP.

Per informazioni su come configurare l'agente SNMP, vedere ["Utilizzare il monitoraggio SNMP"](#) .

Dopo aver configurato l'agente SNMP StorageGRID , è possibile inviare due tipi di notifiche basate sugli eventi:

- Le trappole sono notifiche inviate dall'agente SNMP che non richiedono la conferma da parte del sistema di gestione. Le trappole servono a notificare al sistema di gestione che si è verificato un evento all'interno StorageGRID, ad esempio l'attivazione di un avviso. Le trappole sono supportate in tutte e tre le versioni di SNMP.
- Le informazioni sono simili alle trappole, ma richiedono il riconoscimento da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un certo lasso di tempo, invia nuovamente l'informazione finché non riceve una conferma o finché non viene raggiunto il valore massimo di tentativi. Le informazioni sono supportate in SNMPv2c e SNMPv3.

Le notifiche Trap and Inform vengono inviate quando viene attivato un avviso predefinito o personalizzato a

qualsiasi livello di gravità. Per sopprimere le notifiche SNMP per un avviso, è necessario configurare il silenzio per l'avviso. Vedere ["Disattiva 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 informazioni SNMP. Se il nodo di amministrazione primario non è disponibile, le notifiche vengono inviate temporaneamente da altri nodi di amministrazione. Vedere ["Che cos'è un nodo amministrativo?"](#) .

Imposta notifiche e-mail per gli avvisi

Se desideri che vengano inviate notifiche e-mail quando si verificano avvisi, devi fornire informazioni sul tuo server SMTP. È necessario immettere anche gli indirizzi e-mail dei destinatari delle notifiche di avviso.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Gestisci avvisi o autorizzazione di accesso root"](#) .

Informazioni su questo compito

La configurazione e-mail utilizzata per le notifiche di avviso non viene utilizzata per 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 informazioni SNMP. Se il nodo di amministrazione primario non è disponibile, le notifiche vengono inviate temporaneamente da altri nodi di amministrazione. Vedere ["Che cos'è un nodo amministrativo?"](#) .

Passi

1. Selezionare **AVVISI > Configurazione e-mail**.

Viene visualizzata la pagina Configurazione e-mail.

2. Selezionare la casella di controllo **Abilita notifiche e-mail** per indicare che si desidera che vengano inviate e-mail di notifica quando gli avvisi raggiungono le soglie configurate.

Vengono visualizzate le sezioni Server di posta elettronica (SMTP), Transport Layer Security (TLS), Indirizzi di posta elettronica e Filtri.

3. Nella sezione Server di posta elettronica (SMTP), immettere le informazioni necessarie a StorageGRID per accedere al server SMTP.

Se il tuo server SMTP richiede l'autenticazione, devi fornire sia un nome utente che una password.

Campo	Entra
Server di posta	Il nome di dominio completo (FQDN) o l'indirizzo IP del server SMTP.
Porta	La porta utilizzata per accedere al server SMTP. Deve essere compreso tra 1 e 65535.
Nome utente (facoltativo)	Se il server SMTP richiede l'autenticazione, inserisci il nome utente con cui effettuare l'autenticazione.

Campo	Entra
Password (facoltativa)	Se il server SMTP richiede l'autenticazione, immettere la password per l'autenticazione.

4. Nella sezione Indirizzi e-mail, inserisci gli indirizzi e-mail del mittente e di ciascun destinatario.
- a. Per **Indirizzo email del mittente**, specificare un indirizzo email valido da utilizzare come indirizzo del mittente per le notifiche di avviso.

Ad esempio: storagegrid-alerts@example.com

- b. Nella sezione Destinatari, inserisci un indirizzo email per ogni elenco email o persona che deve ricevere un'email quando si verifica un avviso.

Seleziona l'icona più+ per aggiungere destinatari.

5. Se per le comunicazioni con il server SMTP è richiesto Transport Layer Security (TLS), selezionare **Richiedi TLS** nella sezione Transport Layer Security (TLS).

- a. Nel campo **Certificato CA**, fornire il certificato CA che verrà utilizzato per verificare l'identità del server SMTP.

È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfogliare** e selezionare il file.

È necessario fornire un singolo file contenente i certificati di ciascuna autorità di certificazione (CA) emittente intermedia. Il file dovrebbe contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.

- b. Seleziona la casella di controllo **Invia certificato client** se il tuo server di posta elettronica SMTP richiede ai mittenti di posta elettronica di fornire certificati client per l'autenticazione.

- c. Nel campo **Certificato client**, fornire il certificato client codificato PEM da inviare al server SMTP.

È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfogliare** e selezionare il file.

- d. Nel campo **Chiave privata**, immettere la chiave privata per il certificato client nella codifica PEM non crittografata.

È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfogliare** e selezionare il file.



Se devi modificare la configurazione dell'email, seleziona l'icona della matita per aggiornare questo campo.

6. Nella sezione Filtri, seleziona i livelli di gravità degli avvisi che devono generare notifiche e-mail, a meno che la regola per un avviso specifico non sia stata disattivata.

Gravità	Descrizione
Minore, maggiore, critico	Una notifica via e-mail viene inviata quando viene soddisfatta la condizione minore, maggiore o critica per una regola di avviso.

Gravità	Descrizione
Maggiore, critico	Una notifica via e-mail viene inviata quando viene soddisfatta la condizione principale o critica per una regola di avviso. Le notifiche non vengono inviate per gli avvisi minori.
Solo critico	Una notifica via e-mail 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 sei pronto a testare le impostazioni della tua email, procedi come segue:

a. Seleziona **Invia email di prova**.

Viene visualizzato un messaggio di conferma che indica che è stata inviata un'e-mail di prova.

b. Controlla le caselle di posta di tutti i destinatari delle email e verifica che sia stata ricevuta un'email di prova.



Se l'e-mail non viene ricevuta entro pochi minuti o se viene attivato l'avviso **Errore di notifica e-mail**, controlla le impostazioni e riprova.

c. Sign in a qualsiasi altro nodo di amministrazione e invia un'e-mail di prova per verificare la connettività da tutti i siti.



Quando si testano le notifiche di avviso, è necessario accedere a ogni nodo di amministrazione per verificare la connettività. Ciò è in contrasto con i pacchetti di test AutoSupport , in cui tutti i nodi amministrativi inviano l'e-mail di prova.

8. Seleziona **Salva**.

L'invio di un'e-mail di prova non salva le impostazioni. Devi selezionare **Salva**.

Le impostazioni e-mail vengono salvate.

Informazioni incluse nelle notifiche e-mail di avviso

Dopo aver configurato il server di posta elettronica 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 "[Disattiva le notifiche di avviso](#)".

Le notifiche e-mail includono le seguenti informazioni:

Low object data storage (6 alerts) ¹

The space available for storing object data is low. ²

Recommended actions ³

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node DC1-S1-226 ⁴
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

DC1-S2-227

Node DC1-S2-227
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

Sent from: DC1-ADM1-225 ⁵

Chiamata	Descrizione
1	Il nome dell'avviso, seguito dal numero di istanze attive di questo avviso.
2	La descrizione dell'avviso.
3	Eventuali azioni consigliate per l'avviso.
4	Dettagli su ciascuna istanza attiva dell'avviso, inclusi il nodo e il sito interessati, la gravità dell'avviso, l'ora UTC in cui è stata attivata la regola di avviso e il nome del processo e del servizio interessati.
5	Il nome host del nodo di amministrazione che ha inviato la notifica.

Come vengono raggruppati gli avvisi

Per evitare che venga inviato 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 esempi di come StorageGRID raggruppa più avvisi nelle notifiche e-mail.

Comportamento	Esempio
Ogni notifica di avviso si applica solo agli avvisi che hanno lo stesso nome. Se vengono attivati contemporaneamente due avvisi con nomi diversi, vengono inviate due notifiche e-mail.	• L'avviso A viene attivato contemporaneamente su due nodi. Viene inviata una sola notifica. • L'avviso A viene attivato sul nodo 1 e contemporaneamente l'avviso B viene attivato sul nodo 2. Vengono inviate due notifiche: una per ogni avviso.
Per un avviso specifico su un nodo specifico, se vengono raggiunte le soglie per più di una gravità, viene inviata una notifica solo per l'avviso più grave.	• Viene attivato l'avviso A e vengono raggiunte le soglie di avviso minore, maggiore e critico. Per l'avviso critico viene inviata una notifica.
La prima volta che viene attivato un avviso, StorageGRID attende 2 minuti prima di inviare una notifica. Se durante tale periodo vengono attivati altri avvisi con lo stesso nome, StorageGRID raggruppa tutti gli avvisi nella notifica iniziale.	1. L'avviso A viene attivato sul nodo 1 alle 08:00. Non viene inviata alcuna notifica. 2. L'avviso 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 segnala tutti gli avvisi attivi (avvisi correnti che non sono stati disattivati), anche se segnalati in precedenza.	1. L'avviso A viene attivato sul nodo 1 alle 08:00. Una notifica viene inviata alle 08:02. 2. L'avviso A viene attivato sul nodo 2 alle 08:05. Una seconda notifica viene inviata alle 08:15 (10 minuti dopo). Entrambi i nodi sono segnalati.
Se sono presenti più avvisi correnti con lo stesso nome e uno di questi avvisi viene risolto, non verrà inviata una nuova notifica se l'avviso si ripresenta sul nodo per il quale è stato risolto.	1. L'avviso A viene attivato 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 e-mail una volta ogni 7 giorni finché tutte le istanze dell'avviso non vengono risolte o la regola di avviso non viene disattivata.	1. L'avviso A viene attivato per il nodo 1 l'8 marzo. Viene inviata una notifica. 2. L'avviso A non è stato risolto o silenziato. Ulteriori notifiche vengono inviate il 15 marzo, il 22 marzo, il 29 marzo e così via.

Risoluzione dei problemi relativi alle notifiche e-mail di avviso

Se viene attivato l'avviso **Errore di notifica e-mail** o non riesci a ricevere la notifica e-mail di avviso di prova, segui questi passaggi per risolvere il problema.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Gestisci avvisi o autorizzazione di accesso root"](#) .

Passi

1. Verifica le tue impostazioni.
 - a. Selezionare **AVVISI > Configurazione e-mail**.
 - b. Verificare che le impostazioni del server di posta elettronica (SMTP) siano corrette.
 - c. Verifica di aver specificato indirizzi email validi per i destinatari.
2. Controlla il filtro antispam e assicurati che l'e-mail non sia stata inviata nella cartella posta indesiderata.
3. Chiedi all'amministratore della tua posta elettronica di confermare che le email provenienti dall'indirizzo del mittente non siano bloccate.
4. Raccogli un file di registro per il nodo di amministrazione, quindi contatta l'assistenza tecnica.

L'assistenza tecnica può utilizzare le informazioni contenute nei registri per determinare cosa è andato storto. Ad esempio, il file prometheus.log potrebbe mostrare un errore durante la connessione al server specificato.

Vedere ["Raccogli file di registro e dati di sistema"](#) .

Disattiva le notifiche di avviso

Facoltativamente, è possibile configurare dei silenzi per sopprimere temporaneamente le notifiche di avviso.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Gestisci avvisi o autorizzazione di accesso root"](#) .

Informazioni su questo compito

È possibile disattivare le regole di avviso sull'intera griglia, su un singolo sito o su un singolo nodo e per una o più gravità. Ogni silenzio sopprime tutte le notifiche per una singola regola di avviso o per tutte le regole di avviso.

Se è stato abilitato l'agente SNMP, i silenziamenti sopprimono anche le trappole e le informazioni SNMP.



Prestare attenzione quando si decide di disattivare una regola di avviso. Se si disattiva un avviso, è possibile che non venga rilevato un problema di fondo finché non si impedisce il completamento di un'operazione critica.

Passi

1. Selezionare **AVVISI > Silenzi**.

Viene visualizzata la pagina Silenzi.

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

+ Create

Edit

Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
No results found.				

2. Seleziona **Crea**.

Viene visualizzata la finestra di dialogo Crea silenzio.

Create Silence

Alert Rule

Description (optional)

Duration

Minutes

Severity

☐ Minor only

☐ Minor, major

☐ Minor, major, critical

Nodes

☐ StorageGRID Deployment

☐ Data Center 1

☐ DC1-ADM1

☐ DC1-G1

☐ DC1-S1

☐ DC1-S2

☐ DC1-S3

Cancel

Save

3. Seleziona o inserisci le seguenti informazioni:

Campo	Descrizione
Regola di avviso	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 disabilitata. 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. Descrivi, ad esempio, lo scopo di questo silenzio.
Durata	Per quanto tempo desideri che questo silenzio rimanga in vigore, in minuti, ore o giorni. Il silenzio può avere una durata che va da 5 minuti a 1.825 giorni (5 anni). Nota: non dovresti disattivare una regola di avviso per un periodo di tempo prolungato. Se una regola di avviso viene disattivata, potresti non rilevare un problema di fondo finché non impedisce il completamento di un'operazione critica. Tuttavia, potrebbe essere necessario utilizzare un silenzio prolungato se un avviso viene attivato da una configurazione specifica e intenzionale, come potrebbe essere il caso degli avvisi Collegamento appliance servizi inattivo e degli avvisi Collegamento appliance di archiviazione inattivo.
Gravità	Quale livello di gravità dell'avviso deve essere silenziato. Se l'avviso viene attivato a uno dei livelli di gravità selezionati, non vengono inviate notifiche.
Nodi	A quale nodo o nodi vuoi che venga applicato questo silenzio. È possibile sopprimere una regola di avviso o tutte le regole sull'intera griglia, su un singolo sito o su un singolo nodo. Se si seleziona l'intera griglia, il silenzio si applica 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 di un sito per ogni silenzio. È necessario creare silenzi aggiuntivi se si desidera sopprimere la stessa regola di avviso su più nodi o più siti contemporaneamente.

4. Seleziona **Salva**.

5. Se vuoi modificare o terminare un silenzio prima che scada, puoi modificarlo o rimuoverlo.

Opzione	Descrizione
Modifica un silenzio	- Selezionare AVVISI > Silenzi. - Nella tabella, seleziona il pulsante di opzione relativo al silenzio che desideri modificare. - Selezionare Modifica. - Modifica la descrizione, il tempo rimanente, i livelli di gravità selezionati o il nodo interessato. - Seleziona Salva.

Opzione	Descrizione
Rimuovere un silenzio	a. Selezionare AVVISI > Silenzi. b. Nella tabella, seleziona il pulsante di opzione relativo al silenzio che desideri rimuovere. c. Seleziona 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 vengano sopprese da un altro silenzio). Se questo avviso è già attivato, potrebbero essere necessari alcuni minuti prima che le notifiche via e-mail o SNMP vengano inviate e che la pagina Avvisi venga aggiornata.

Informazioni correlate

["Configurare l'agente SNMP"](#)

Riferimento avvisi

In questo riferimento sono elencati gli avvisi predefiniti visualizzati in Grid Manager. Le azioni consigliate sono riportate nel messaggio di avviso ricevuto.

Se necessario, è possibile creare regole di avviso personalizzate per adattare al proprio approccio di gestione del sistema.

Alcuni degli avvisi predefiniti utilizzano ["Metriche di Prometeo"](#).

Avvisi sugli elettrodomestici

Nome dell'avviso	Descrizione
Batteria dell'apparecchio scaduta	La batteria nel controller di accumulo dell'apparecchio è scaduta.
Batteria dell'apparecchio guasta	La batteria nel controller di accumulo dell'apparecchio è guasta.
La batteria dell'apparecchio ha una capacità di apprendimento insufficiente	La batteria nel controller di accumulo dell'apparecchio non ha una capacità di apprendimento sufficiente.
Batteria dell'apparecchio prossima alla scadenza	La batteria nel controller di accumulo dell'apparecchio sta per esaurirsi.
Batteria dell'apparecchio rimossa	Manca la batteria nel controller di accumulo dell'apparecchio.
Batteria dell'apparecchio troppo calda	La batteria nel controller di accumulo dell'apparecchio è surriscaldata.

Nome dell'avviso	Descrizione
Errore di comunicazione BMC dell'apparecchio	La comunicazione con il controller di gestione della scheda madre (BMC) è stata interrotta.
Rilevato errore del dispositivo di avvio dell'appliance	È stato rilevato un problema con il dispositivo di avvio nell'appliance.
Errore del dispositivo di backup della cache dell'appliance	Un dispositivo di backup della cache persistente non è riuscito.
Capacità insufficiente del dispositivo di backup della cache dell'appliance	La capacità del dispositivo di backup della cache è insufficiente.
Dispositivo di backup della cache dell'appliance protetto da scrittura	Un dispositivo di backup della cache è protetto da scrittura.
Mancata corrispondenza delle dimensioni della memoria cache dell'appliance	I due controller nell'appliance hanno dimensioni di cache diverse.
Guasto della batteria CMOS dell'apparecchio	È stato rilevato un problema con la batteria CMOS dell'apparecchio.
Temperatura dello chassis del controller di elaborazione dell'appliance troppo alta	La temperatura del controller di elaborazione in un dispositivo StorageGRID ha superato una soglia nominale.
Temperatura della CPU del controller di elaborazione dell'appliance troppo alta	La temperatura della CPU nel controller di elaborazione di un dispositivo StorageGRID ha superato una soglia nominale.
Il controller di elaborazione dell'appliance necessita di attenzione	È stato rilevato un guasto hardware nel controller di elaborazione di un dispositivo StorageGRID .
L'alimentatore A del controller di elaborazione dell'apparecchio presenta un problema	L'alimentatore A nel controller di elaborazione presenta un problema.
L'alimentatore B del controller di elaborazione dell'apparecchio presenta un problema	L'alimentatore B nel controller di elaborazione presenta un problema.
Servizio di monitoraggio dell'hardware di elaborazione dell'appliance bloccato	Il servizio che monitora lo stato dell'hardware di archiviazione è bloccato.

Nome dell'avviso	Descrizione
L'unità DAS dell'appliance supera il limite di dati scritti al giorno	Ogni giorno viene scritta una quantità eccessiva di dati su un'unità, il che potrebbe invalidarne la garanzia.
Rilevato guasto dell'unità DAS dell'apparecchio	È stato rilevato un problema con un'unità di archiviazione collegata direttamente (DAS) nell'appliance.
Spia di localizzazione dell'unità DAS dell'apparecchio accesa	La spia di individuazione dell'unità per una o più unità di archiviazione collegate direttamente (DAS) in un nodo di archiviazione dell'appliance è accesa.
Ricostruzione dell'unità DAS dell'appliance	Un'unità di archiviazione collegata direttamente (DAS) è in fase di ricostruzione. Ciò è previsto se è stato sostituito o rimosso/reinserito di recente.
Rilevato guasto alla ventola dell'apparecchio	È stato rilevato un problema con un'unità ventola nell'apparecchio.
Rilevato guasto Fibre Channel dell'appliance	È stato rilevato un problema di collegamento Fibre Channel tra il controller di archiviazione dell'appliance e il controller di elaborazione
Errore della porta HBA Fibre Channel dell'appliance	Una porta HBA Fibre Channel è guasta o è guasta.
Unità cache flash dell'appliance non ottimali	Le unità utilizzate per la cache SSD non sono ottimali.
Interconnessione dell'apparecchio/contenitore della batteria rimosso	Manca il contenitore di interconnessione/batteria.
Porta LACP dell'appliance mancante	Una porta su un dispositivo StorageGRID non partecipa al bond LACP.
Rilevato guasto della scheda di rete dell'apparecchio	È stato rilevato un problema con una scheda di interfaccia di rete (NIC) nell'appliance.
Alimentazione elettrica complessiva dell'apparecchio degradata	La potenza di un dispositivo StorageGRID si è discostata dalla tensione operativa consigliata.
Avviso critico SSD dell'appliance	Un SSD dell'apparecchio segnala un avviso critico.
Errore del controller di archiviazione dell'apparecchio A	Il controller di archiviazione A in un dispositivo StorageGRID non funziona.

Nome dell'avviso	Descrizione
Guasto del controller di archiviazione dell'apparecchio B	Il controller di archiviazione B in un dispositivo StorageGRID non funziona.
Guasto dell'unità del controller di archiviazione dell'appliance	Una o più unità in un dispositivo StorageGRID sono guaste o non sono ottimali.
Problema hardware del controller di archiviazione dell'appliance	Il software SANtricity segnala "Richiede attenzione" per un componente in un dispositivo StorageGRID .
Guasto dell'alimentatore del controller di archiviazione dell'apparecchio A	L'alimentatore A in un dispositivo StorageGRID si è discostato dalla tensione di esercizio consigliata.
Guasto all'alimentatore B del controller di archiviazione dell'apparecchio	L'alimentatore B in un dispositivo StorageGRID si è discostato dalla tensione di esercizio consigliata.
Servizio di monitoraggio dell'hardware di archiviazione degli elettrodomestici bloccato	Il servizio che monitora lo stato dell'hardware di archiviazione è bloccato.
Ripiani di stoccaggio degli elettrodomestici degradati	Lo stato di uno dei componenti nello scaffale di archiviazione di un dispositivo di archiviazione è degradato.
Temperatura dell'apparecchio superata	È stata superata la temperatura nominale o massima del regolatore di accumulo dell'apparecchio.
Sensore di temperatura dell'apparecchio rimosso	È stato rimosso un sensore di temperatura.
Errore di avvio sicuro UEFI dell'appliance	Un dispositivo non è stato avviato in modo sicuro.
L'I/O del disco è molto lento	Un I/O del disco molto lento potrebbe influire sulle prestazioni della griglia.
Rilevato guasto della ventola dell'apparecchio di archiviazione	È stato rilevato un problema con un'unità ventola nel controller di archiviazione di un dispositivo.
Connettività di archiviazione dell'appliance di archiviazione degradata	Si è verificato un problema con una o più connessioni tra il controller di elaborazione e il controller di archiviazione.
Dispositivo di archiviazione inaccessibile	Non è possibile accedere a un dispositivo di archiviazione.

Avvisi di audit e syslog

Nome dell'avviso	Descrizione
I registri di controllo vengono aggiunti alla coda in memoria	Il nodo non riesce a inviare log al server syslog locale e la coda in memoria si sta riempiendo.
Errore di inoltro del server syslog esterno	Il nodo non può inoltrare i log al server syslog esterno.
Ampia coda di controllo	La coda del disco 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 riesce a 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 Available o Strong-site, che non è supportato.
Il bucket FabricPool ha un'impostazione di controllo delle versioni non supportata	Un bucket FabricPool ha abilitato il controllo delle versioni o il blocco degli oggetti S3, che non sono supportati.

Avvisi di Cassandra

Nome dell'avviso	Descrizione
Errore del compattatore automatico Cassandra	Si è verificato un errore nel compattatore automatico Cassandra.
Le metriche del compattatore automatico Cassandra non sono aggiornate	Le metriche che descrivono l'autocompattatore Cassandra non sono aggiornate.
Errore di comunicazione di Cassandra	I nodi che eseguono il servizio Cassandra hanno problemi di comunicazione tra loro.
Compattazioni di Cassandra sovraccariche	Il processo di compattazione di Cassandra è sovraccarico.
Errore di scrittura sovradimensionato di Cassandra	Un processo StorageGRID interno ha inviato a Cassandra una richiesta di scrittura troppo grande.

Nome dell'avviso	Descrizione
Le metriche di riparazione di Cassandra sono obsolete	Le metriche che descrivono i lavori di riparazione di Cassandra non sono aggiornate.
I progressi nella riparazione di Cassandra sono lenti	I progressi nelle riparazioni del database Cassandra sono lenti.
Servizio di riparazione Cassandra non disponibile	Il servizio di riparazione Cassandra non è disponibile.
Corruzione della tabella Cassandra	Cassandra ha rilevato un danneggiamento della tabella. Cassandra si riavvia automaticamente se rileva un danneggiamento della tabella.

Avvisi di Cloud Storage Pool

Nome dell'avviso	Descrizione
Errore di connettività del pool di archiviazione cloud	Il controllo dello stato di Cloud Storage Pool ha rilevato uno o più nuovi errori.
Scadenza della certificazione dell'entità finale di IAM Roles Anywhere	Il certificato dell'entità finale di IAM Roles Anywhere sta per scadere.

Avvisi di replicazione tra griglie

Nome dell'avviso	Descrizione
Errore permanente della replicazione tra griglie	Si è verificato un errore di replicazione tra griglie che richiede l'intervento dell'utente per essere risolto.
Risorse di replicazione cross-grid non disponibili	Le richieste di replicazione tra griglie sono in sospeso perché una risorsa non è disponibile.

Avvisi DHCP

Nome dell'avviso	Descrizione
Contratto di locazione DHCP scaduto	Il lease DHCP su un'interfaccia di rete è scaduto.
La scadenza del contratto di locazione DHCP è imminente	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 sulle prestazioni di debug	Quando la modalità debug è abilitata, le prestazioni del sistema potrebbero essere influenzate negativamente.
Configurazione della traccia abilitata	Quando la configurazione della traccia è abilitata, le prestazioni del sistema potrebbero subire un impatto negativo.

Avvisi via e-mail e AutoSupport

Nome dell'avviso	Descrizione
Impossibile inviare il messaggio AutoSupport	Il messaggio AutoSupport più recente non è stato inviato.
Errore nella risoluzione del nome di dominio	Il nodo StorageGRID non è riuscito a risolvere i nomi di dominio.
Errore di notifica e-mail	Non è stato possibile inviare la notifica via e-mail per un avviso.
Errori informativi SNMP	Errori durante l'invio di notifiche informative SNMP a una destinazione trap.
Rilevato accesso SSH o console	Nelle ultime 24 ore, un utente ha effettuato l'accesso tramite Web Console o SSH.

Avvisi di codifica di cancellazione (EC)

Nome dell'avviso	Descrizione
Errore di ribilanciamento della CE	La procedura di riequilibrio della CE è fallita o è stata interrotta.
Guasto alla riparazione della CE	Un processo di riparazione dei dati EC non è riuscito o è stato interrotto.
Riparazione EC bloccata	Un lavoro di riparazione dei dati EC è bloccato.
Errore di verifica del frammento codificato tramite cancellazione	I frammenti con codice di cancellazione non possono più essere verificati. I frammenti danneggiati potrebbero non essere riparati.

Avvisi di scadenza dei certificati

Nome dell'avviso	Descrizione
Scadenza del certificato CA del proxy di amministrazione	Uno o più certificati nel bundle CA del server proxy di amministrazione stanno per scadere.

Nome dell'avviso	Descrizione
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 dell'endpoint del bilanciatore del carico	Uno o più certificati dell'endpoint del bilanciatore 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 di rete

Nome dell'avviso	Descrizione
Mancata corrispondenza MTU della rete di griglia	L'impostazione MTU per l'interfaccia Grid Network (eth0) varia notevolmente tra i nodi della griglia.

Avvisi sulla federazione della griglia

Nome dell'avviso	Descrizione
Scadenza del certificato di federazione della rete	Uno o più certificati di federazione di griglia stanno per scadere.
Errore di connessione alla federazione di rete	La connessione di federazione della rete tra la rete locale e quella remota non funziona.

Avvisi di utilizzo elevato o di latenza elevata

Nome dell'avviso	Descrizione
Utilizzo elevato dell'heap Java	Viene utilizzata un'elevata percentuale di spazio heap Java.
Elevata latenza per le query sui metadati	Il tempo medio per le query sui metadati di Cassandra è troppo lungo.

Avvisi di federazione delle identità

Nome dell'avviso	Descrizione
Errore di sincronizzazione della federazione delle identità	Impossibile sincronizzare i gruppi e gli utenti federati dall'origine dell'identità.
Errore di sincronizzazione della federazione delle identità per un tenant	Impossibile sincronizzare gruppi e utenti federati dall'origine identità configurata da un tenant.

Avvisi sulla gestione del ciclo di vita delle informazioni (ILM)

Nome dell'avviso	Descrizione
Posizionamento ILM non realizzabile	Per determinati oggetti non è possibile ottenere un'istruzione di posizionamento in una regola ILM.
Bassa frequenza di scansione ILM	La velocità di scansione ILM è impostata su meno di 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 stata caricata.
Errore di connettività KMS	Un nodo appliance non è riuscito a connettersi al server di gestione delle chiavi per il proprio sito.
Nome della 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 decrittografati correttamente, ma uno o più volumi non sono riusciti a ruotare alla chiave più recente.
KMS non è configurato	Per questo sito non esiste alcun server di gestione delle chiavi.
La chiave KMS non è riuscita a decrittografare un volume dell'appliance	Uno o più volumi su un dispositivo con crittografia dei nodi abilitata non possono essere decrittografati con la chiave KMS corrente.

Nome dell'avviso	Descrizione
Scadenza del certificato del server KMS	Il certificato del server utilizzato dal server di gestione delle chiavi (KMS) sta per scadere.
Errore di connettività del server KMS	Un nodo appliance non è riuscito a connettersi a uno o più server nel cluster del server di gestione delle chiavi per il suo sito.

Avvisi del bilanciatore del carico

Nome dell'avviso	Descrizione
Connessioni di bilanciamento del carico con richiesta zero elevate	Una percentuale elevata di connessioni agli endpoint del bilanciatore del carico si è interrotta senza eseguire richieste.

Avvisi di scostamento dell'orologio locale

Nome dell'avviso	Descrizione
Grande offset orario dell'orologio locale	Lo scostamento tra l'orologio locale e l'ora del Network Time Protocol (NTP) è troppo grande.

Avvisi di memoria o spazio insufficienti

Nome dell'avviso	Descrizione
Bassa capacità del disco del registro di controllo	Lo spazio disponibile per i registri di controllo è limitato. Se questa condizione non viene risolta, le operazioni S3 o Swift potrebbero non riuscire.
Memoria del nodo disponibile insufficiente	La quantità di RAM disponibile su un nodo è bassa.
Spazio libero insufficiente per il pool di archiviazione	Lo spazio disponibile per l'archiviazione dei dati degli oggetti nel nodo di archiviazione è limitato.
Bassa memoria del nodo installata	La quantità di memoria installata su un nodo è bassa.
Basso spazio di archiviazione dei metadati	Lo spazio disponibile per l'archiviazione dei metadati degli oggetti è limitato.
Bassa capacità del disco metrico	Lo spazio disponibile per il database delle metriche è limitato.
Bassa capacità di archiviazione dei dati degli oggetti	Lo spazio disponibile per l'archiviazione dei dati degli oggetti è limitato.

Nome dell'avviso	Descrizione
Sovrascrittura della filigrana di sola lettura bassa	L'override della filigrana di sola lettura software del volume di archiviazione è inferiore alla filigrana minima ottimizzata per un nodo di archiviazione.
Bassa capacità del disco radice	Lo spazio disponibile sul disco radice è basso.
Bassa capacità di dati del 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 basso.

Avvisi di nodo o di rete di nodi

Nome dell'avviso	Descrizione
Utilizzo della rete di amministrazione ricevuto	L'utilizzo della ricezione sulla rete di amministrazione è elevato.
Utilizzo della trasmissione della rete amministrativa	L'utilizzo della trasmissione sulla rete di amministrazione è elevato.
Errore di configurazione del firewall	Impossibile applicare la configurazione del firewall.
Endpoint dell'interfaccia di gestione in modalità fallback	Per troppo tempo tutti gli endpoint dell'interfaccia di gestione sono tornati alle porte predefinite.
Errore di connettività della rete del nodo	Si sono verificati errori durante il trasferimento dei dati tra i nodi.
Errore di ricezione del frame della rete del nodo	Un'alta percentuale di frame di rete ricevuti da un nodo presentava errori.
Nodo non sincronizzato con il server NTP	Il nodo non è sincronizzato con il server NTP (Network Time Protocol).
Nodo non bloccato con il server NTP	Il nodo non è bloccato su un server NTP (Network Time Protocol).
Rete di nodi non elettrodomestici inattiva	Uno o più dispositivi di rete sono inattivi o disconnessi.
Collegamento dell'appliance dei servizi non attivo sulla rete di amministrazione	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.

Nome dell'avviso	Descrizione
Collegamento dell'appliance dei servizi non attivo sulla porta 1 della rete di amministrazione	La porta di rete amministrativa 1 sull'appliance è inattiva o disconnessa.
Collegamento dell'appliance dei servizi non attivo sulla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di servizi non attivo sulla porta di rete 1	La porta di rete 1 sull'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di servizi non attivo sulla porta di rete 2	La porta di rete 2 dell'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di servizi non attivo sulla porta di rete 3	La porta di rete 3 dell'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di servizi non attivo sulla porta di rete 4	La porta di rete 4 sull'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla rete di amministrazione	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla porta 1 della rete di amministrazione	La porta di rete amministrativa 1 sull'appliance è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non funzionante sulla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla porta di rete 1	La porta di rete 1 sull'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla porta di rete 2	La porta di rete 2 dell'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla porta di rete 3	La porta di rete 3 dell'apparecchio è inattiva o disconnessa.

Nome dell'avviso	Descrizione
Collegamento dell'appliance di archiviazione non attivo sulla porta di rete 4	La porta di rete 4 sull'apparecchio è inattiva o disconnessa.
Il nodo di archiviazione non si trova nello stato di archiviazione 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 sta avvicinando al numero massimo che può essere monitorato.
Impossibile comunicare con il nodo	Uno o più servizi non rispondono oppure il nodo non è raggiungibile.
Riavvio imprevisto del nodo	Un nodo si è riavviato inaspettatamente nelle ultime 24 ore.

Avvisi sugli oggetti

Nome dell'avviso	Descrizione
Controllo esistenza oggetto fallito	Il processo di controllo dell'esistenza dell'oggetto non è riuscito.
Controllo dell'esistenza dell'oggetto bloccato	Il processo di controllo dell'esistenza dell'oggetto si è bloccato.
Oggetti persi	Uno o più oggetti sono stati persi dalla griglia.
S3 PUT dimensione dell'oggetto troppo grande	Un client sta tentando un'operazione PUT Object che supera i limiti di dimensione S3.
Rilevato oggetto corrotto non identificato	È stato trovato un file nell'archivio oggetti replicati che non è stato possibile identificare come oggetto replicato.

Avvisi sui servizi della piattaforma

Nome dell'avviso	Descrizione
Capacità richiesta in sospeso dei servizi della piattaforma bassa	Il numero di richieste in sospeso dei Servizi della piattaforma sta per raggiungere la capacità massima.
Servizi della piattaforma non disponibili	In un sito sono in esecuzione o disponibili troppi nodi di archiviazione con il servizio RSM.

Avvisi sul volume di archiviazione

Nome dell'avviso	Descrizione
Il volume di archiviazione richiede attenzione	Un volume di archiviazione è offline e necessita di attenzione.
Il volume di archiviazione deve essere ripristinato	Un volume di archiviazione è stato recuperato e deve essere ripristinato.
Volume di archiviazione offline	Un volume di archiviazione è stato offline per più di 5 minuti.
Tentativo di rimontaggio del volume di archiviazione	Un volume di archiviazione era offline e ha attivato un rimontaggio automatico. Ciò potrebbe indicare un problema dell'unità o errori del file system.
Il ripristino del volume non è riuscito ad avviare la riparazione dei dati replicati	Non è stato possibile avviare automaticamente la riparazione dei dati replicati per un volume riparato.

Avvisi dei servizi StorageGRID

Nome dell'avviso	Descrizione
servizio nginx che utilizza la configurazione di backup	La configurazione del servizio nginx non è valida. Ora viene utilizzata la configurazione precedente.
servizio nginx-gw che utilizza la configurazione di backup	La configurazione del servizio nginx-gw non è valida. Ora viene utilizzata la configurazione precedente.
Riavvio richiesto per disabilitare FIPS	La policy di sicurezza non richiede la modalità FIPS, ma il modulo di sicurezza crittografica NetApp è abilitato.
Riavvio richiesto per abilitare FIPS	La policy di sicurezza richiede la modalità FIPS, ma il modulo di sicurezza crittografica NetApp è disabilitato.
Servizio SSH che utilizza la configurazione di backup	La configurazione del servizio SSH non è valida. Ora viene utilizzata la configurazione precedente.

Avvisi agli inquilini

Nome dell'avviso	Descrizione
Elevato utilizzo della quota degli inquilini	Viene utilizzata un'elevata percentuale di spazio quota. Questa regola è disabilitata per impostazione predefinita perché potrebbe causare troppe notifiche.

Metriche di 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 [ottenere un elenco completo di tutte le metriche](#) .

Per i dettagli sulla sintassi delle query di Prometheus, vedere "[Interrogando Prometeo](#)".

Cosa sono le metriche di Prometheus?

Le metriche di Prometheus sono misurazioni di serie temporali. Il servizio Prometheus sui nodi amministrativi raccoglie queste metriche dai servizi su tutti i nodi. Le metriche vengono memorizzate su ciascun nodo di amministrazione finché lo spazio riservato ai dati di Prometheus non è pieno. Quando il `/var/local/mysql_ibdata/` Quando il volume raggiunge la capacità massima, le metriche più vecchie vengono eliminate per prime.

Dove vengono utilizzate le metriche di Prometheus?

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

- **Pagina Nodi:** i grafici e i diagrammi nelle schede disponibili nella pagina Nodi utilizzano lo strumento di visualizzazione Grafana per mostrare le metriche delle serie temporali raccolte da Prometheus. Grafana visualizza i dati delle serie temporali in formato grafico e diagramma, mentre Prometheus funge da fonte di dati backend.



- **Avvisi:** gli avvisi vengono attivati a livelli di gravità specifici quando le condizioni delle regole di avviso che utilizzano le metriche Prometheus vengono valutate come vere.
- **API di gestione della griglia:** puoi utilizzare le metriche di Prometheus nelle regole di avviso personalizzate o con strumenti di automazione esterni per monitorare il tuo sistema StorageGRID . Un elenco completo delle metriche di Prometheus è disponibile nella Grid Management API. (Dalla parte superiore di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API > metriche**.) Sebbene siano disponibili più di mille metriche, per monitorare le operazioni StorageGRID più critiche ne basta un numero relativamente piccolo.



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

- La pagina **SUPPORTO > Strumenti > Diagnostica** e la pagina **SUPPORTO > Strumenti > Metriche:** queste pagine, destinate principalmente all'assistenza tecnica, forniscono diversi strumenti e grafici che utilizzano i valori delle metriche di Prometheus.



Alcune funzionalità e voci di menu nella pagina Metriche sono intenzionalmente non funzionali e sono soggette a modifiche.

Elenco delle metriche più comuni

L'elenco seguente contiene le metriche Prometheus più comunemente utilizzate.



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

alertmanager_notifiche_fallite_totale

Numero totale di notifiche di avviso non riuscite.

node_filesystem_disponibilità_byte

Quantità di spazio del file system disponibile per gli utenti non root, espressa in byte.

node_memory_MemAvailable_bytes

Campo informativo sulla memoria MemAvailable_bytes.

nodo_operatore_di_rete

Valore del vettore di `/sys/class/net/iface`.

node_network_receive_errs_total

Statistica del dispositivo di rete `receive_errs`.

errori_di_trasmissione_della_rete_del_nodo_totale

Statistica del dispositivo di rete `transmit_errs`.

storagegrid_amministrativamente_inattivo

Il nodo non è connesso alla rete per un motivo prevedibile. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando o il software è in fase di aggiornamento.

storagegrid_appliance_compute_controller_hardware_status

Lo stato dell'hardware del controller di elaborazione in un dispositivo.

storagegrid_appliance_failed_disks

Per il controller di archiviazione di un dispositivo, il numero di unità che non sono ottimali.

storagegrid_appliance_storage_controller_hardware_status

Stato generale dell'hardware del controller di archiviazione in un dispositivo.

storagegrid_content_buckets_and_containers

Numero totale di bucket S3 e container Swift noti a questo nodo di archiviazione.

oggetti_contenuto_di_archiviazione

Numero totale di oggetti dati S3 e Swift noti a questo nodo di archiviazione. Il conteggio è valido solo per gli oggetti dati creati dalle applicazioni client che interagiscono con il sistema tramite S3.

oggetti_contenuto_di_archiviazione_persi

Numero totale di oggetti che questo servizio rileva come mancanti dal sistema StorageGRID . È necessario

intervenire per determinare la causa della perdita e se è possibile un recupero.

["Risolvere i problemi relativi ai dati degli oggetti persi e mancanti"](#)

storagegrid_http_sessions_incoming_attempted

Numero totale di sessioni HTTP tentate su un nodo di archiviazione.

storagegrid_http_sessions_incoming_currently_established

Numero di sessioni HTTP attualmente attive (aperte) sul nodo di archiviazione.

storagegrid_http_sessions_incoming_failed

Numero totale di sessioni HTTP che non sono state completate correttamente, a causa di una richiesta HTTP non valida o di un errore durante l'elaborazione di un'operazione.

storagegrid_http_sessions_incoming_successful

Numero totale di sessioni HTTP completate correttamente.

storagegrid_ilm_in_attesa_di_oggetti_di_sfondo

Numero totale di oggetti su questo nodo in attesa della valutazione ILM dalla scansione.

storagegrid_ilm_in_attesa_di_oggetti_di_valutazione_client_al_secondo

La frequenza attuale con cui gli oggetti vengono valutati in base alla policy ILM su questo nodo.

storagegrid_ilm_in_attesa_di_oggetti_client

Numero totale di oggetti su questo nodo in attesa di valutazione ILM da parte delle operazioni client (ad esempio, acquisizione).

storagegrid_ilm_in_attesa_di_oggetti_totali

Numero totale di oggetti in attesa di valutazione ILM.

storagegrid_ilm_scan_oggetti_al_secondo

La velocità con cui gli oggetti di proprietà di questo nodo vengono scansionati e messi in coda per ILM.

storagegrid_ilm_scan_period_estimated_minutes

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_scadenza_tempo

Tempo di scadenza del certificato dell'endpoint del bilanciatore del carico in secondi dall'epoca.

storagegrid_metadata_queries_latenza_media_millisecondi

Tempo medio necessario per eseguire una query sull'archivio metadati tramite questo servizio.

storagegrid_network_bytes_ricevuti

Quantità totale di dati ricevuti dall'installazione.

storagegrid_network_bytes_trasmessi

Quantità totale di dati inviati dall'installazione.

percentuale_utilizzo_cpu_node_storagegrid

Percentuale di tempo CPU disponibile attualmente utilizzata da questo servizio. Indica il livello di attività del servizio. La quantità di tempo CPU disponibile dipende dal numero di CPU del server.

storagegrid_ntp_chosen_time_source_offset_millisecondi

Offset sistematico del tempo fornito da una sorgente temporale scelta. L'offset viene introdotto quando il ritardo per raggiungere una sorgente temporale non è uguale al tempo necessario alla sorgente temporale per raggiungere il client NTP.

storagegrid_ntp_bloccato

Il nodo non è bloccato su un server NTP (Network Time Protocol).

storagegrid_s3_data_transfers_bytes_ingested

Quantità totale di dati acquisiti dai client S3 in questo nodo di archiviazione dall'ultima reimpostazione dell'attributo.

storagegrid_s3_data_transfers_bytes_retrieved

Quantità totale di dati recuperati dai client S3 da questo nodo di archiviazione dall'ultima reimpostazione dell'attributo.

storagegrid_s3_operations_failed

Numero totale di operazioni S3 non riuscite (codici di stato HTTP 4xx e 5xx), escluse quelle causate da errori di autorizzazione S3.

storagegrid_s3_operations_successful

Numero totale di operazioni S3 riuscite (codice di stato HTTP 2xx).

storagegrid_s3_operations_unauthorized

Numero totale di operazioni S3 non riuscite dovute a un errore di autorizzazione.

giorni di scadenza del certificato dell'interfaccia di gestione del certificato del server di storagegrid

Numero di giorni prima della scadenza del certificato dell'interfaccia di gestione.

giorni di scadenza del certificato degli endpoint dell'api di archiviazione del certificato del server di storagegrid

Numero di giorni prima della scadenza del certificato Object Storage API.

storagegrid_service_cpu_seconds

Quantità cumulativa di tempo in cui la CPU è stata utilizzata da questo servizio dall'installazione.

storagegrid_service_memory_usage_bytes

La quantità di memoria (RAM) attualmente utilizzata da questo servizio. Questo valore è identico a quello visualizzato dall'utilità Linux top come RES.

storagegrid_service_network_bytes_ricevuti

Quantità totale di dati ricevuti da questo servizio dall'installazione.

storagegrid_service_network_bytes_trasmessi

La quantità totale di dati inviati da questo servizio.

storagegrid_service_restarts

Numero totale di volte in cui il servizio è stato riavviato.

secondi di esecuzione del servizio storagegrid

Tempo totale di esecuzione del servizio dall'installazione.

secondi di attività del servizio storagegrid

Tempo totale di esecuzione del servizio dall'ultimo riavvio.

storagegrid_stato_di_archiviazione_corrente

Lo stato attuale dei servizi di archiviazione. I valori degli attributi sono:

- 10 = Non in linea
- 15 = Manutenzione
- 20 = Sola lettura
- 30 = In linea

storagegrid_stato_archiviazione

Lo stato attuale dei servizi di archiviazione. I valori degli attributi sono:

- 0 = Nessun errore
- 10 = In transizione
- 20 = Spazio libero insufficiente
- 30 = Volume/i non disponibile/i
- 40 = Errore

storagegrid_byte_dati_di_utilizzo_archiviazione

Una stima della dimensione totale dei dati degli oggetti replicati e codificati per la cancellazione sul nodo di archiviazione.

storagegrid_metadati_utilizzo_archiviazione_byte_consentiti

Lo spazio totale sul volume 0 di ciascun nodo di archiviazione consentito per i metadati degli oggetti. Questo valore è sempre inferiore allo spazio effettivamente riservato ai metadati su un nodo, perché una parte dello spazio riservato è necessaria per operazioni essenziali del database (come compattazione e riparazione) e futuri aggiornamenti hardware e software. Lo spazio consentito per i metadati degli oggetti controlla la capacità complessiva degli oggetti.

storagegrid_metadati_utilizzo_archiviazione_byte

Quantità di metadati dell'oggetto sul volume di archiviazione 0, in byte.

storagegrid_utilizzo_archiviazione_spazio_totale_byte

Quantità totale di spazio di archiviazione assegnato a tutti gli archivi di oggetti.

storagegrid_storage_utilization_space_usable_bytes

Quantità totale di spazio di archiviazione degli oggetti rimanente. Calcolato sommando la quantità di spazio disponibile per tutti gli archivi di oggetti sul nodo di archiviazione.

storagegrid_swift_data_transfers_bytes_ingested

Quantità totale di dati acquisiti dai client Swift in questo nodo di archiviazione dall'ultima reimpostazione

dell'attributo.

storagegrid_swift_data_transfers_bytes_recuperati

Quantità totale di dati recuperati dai client Swift da questo nodo di archiviazione dall'ultima reimpostazione dell'attributo.

operazioni_swift_di_archiviazione_fallite

Numero totale di operazioni Swift non riuscite (codici di stato HTTP 4xx e 5xx), escluse quelle causate da errori di autorizzazione Swift.

operazioni_rapide_di_archiviazione_riuscite

Numero totale di operazioni Swift riuscite (codice di stato HTTP 2xx).

operazioni_rapide_di_archiviazione_non_autorizzate

Numero totale di operazioni Swift non riuscite dovute a 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.

conteggio_oggetti_utilizzo_tenant_storagegrid

Numero di oggetti per l'inquilino.

storagegrid_tenant_quota_utilizzo_byte

Quantità massima di spazio logico disponibile per gli oggetti del tenant. Se non viene specificata una metrica di quota, lo spazio disponibile è illimitato.

Ottieni un elenco di tutte le metriche

Per ottenere l'elenco completo delle metriche, utilizzare l'API Grid Management.

1. Nella parte superiore di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API**.
2. Individuare le operazioni **metriche**.
3. Eseguire il GET `/grid/metric-names` operazione.
4. Scarica i risultati.

Riferimento ai file di registro

Riferimento ai file di registro

StorageGRID fornisce registri utilizzati per acquisire eventi, messaggi diagnostici e condizioni di errore. Potrebbe esserti richiesto di raccogliere i file di registro e di inoltrarli al supporto tecnico per aiutarti a risolvere i problemi.

I registri sono classificati come segue:

- ["Registri del software StorageGRID"](#)
- ["Registri di distribuzione e manutenzione"](#)
- ["Informazioni su bycast.log"](#)



I dettagli forniti per ciascun tipo di registro sono solo a scopo di riferimento. I registri sono destinati alla risoluzione avanzata dei problemi da parte del supporto tecnico. Le tecniche avanzate che comportano la ricostruzione della cronologia dei problemi utilizzando i log di controllo e i file di log delle applicazioni esulano dallo scopo di queste istruzioni.

Accedi ai registri

Per accedere ai registri, puoi ["raccolgere file di registro e dati di sistema"](#) da uno o più nodi come un singolo archivio di file di registro. In alternativa, se il nodo di amministrazione primario non è disponibile o non riesce a 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. Inserisci la password elencata nel `Passwords.txt` file.
3. Immettere il seguente comando per passare alla root: `su -`
4. Inserisci la password elencata nel `Passwords.txt` file.

Esportare i registri sul server syslog

L'esportazione dei log sul server syslog offre le seguenti funzionalità:

- Ricevi un elenco di tutte le richieste di Grid Manager e Tenant Manager, oltre alle richieste S3 e Swift.
- Migliore visibilità sulle richieste S3 che restituiscono errori, senza l'impatto sulle prestazioni causato dai metodi di registrazione degli audit.
- Accesso alle richieste di livello HTTP e ai codici di errore facili da analizzare.
- Migliore visibilità sulle richieste bloccate dai classificatori del traffico nel bilanciatore del carico.

Per esportare i log, fare riferimento a ["Configurare i messaggi di controllo e le destinazioni dei registri"](#).

Categorie dei file di registro

L'archivio dei file di registro StorageGRID contiene i registri descritti per ciascuna categoria e file aggiuntivi che contengono metriche e output dei comandi di debug.

Posizione dell'archivio	Descrizione
revisione contabile	Messaggi di controllo generati durante il normale funzionamento del sistema.
base-os-logs	Informazioni di base sul sistema operativo, incluse le versioni delle immagini StorageGRID.
fasci	Informazioni di configurazione globali (bundle).
Cassandra	Informazioni sul database di Cassandra e registri di riparazione di Reaper.
ec	Informazioni VCS sul nodo corrente e informazioni sul gruppo EC in base all'ID del profilo.

Posizione dell'archivio	Descrizione
griglia	Registri generali della griglia, incluso il debug(<code>bycast.log</code>) E <code>servermanager</code> registri.
griglia.json	File di configurazione della griglia condiviso tra tutti i nodi. Inoltre, <code>node.json</code> è specifico del nodo corrente.
hagruppi	Metriche e log dei gruppi ad alta disponibilità.
installare	`Gdu-server` e installare i registri.
Lambda-arbitro	Registri relativi alla richiesta proxy S3 Select.
boscaiolo.log	Messaggi di debug relativi alla raccolta dei log.
Metrica	Registri di servizio per Grafana, Jaeger, node exporter e Prometheus.
miscd	Registri di accesso ed errori vari.
MySQL	Configurazione del database mariaDB e relativi log.
netto	Registri generati da script correlati alla rete e dal servizio Dynip.
nginx	File e registri di configurazione del bilanciatore del carico e della federazione della griglia. Include anche i registri del traffico di Grid Manager e Tenant Manager.

Posizione dell'archivio	Descrizione
nginx-gw	• <code>access.log</code>: Messaggi di registro delle richieste del Grid Manager e del Tenant Manager. ◦ Questi messaggi sono preceduti da <code>mgmt</code>: quando esportato tramite <code>syslog</code>. ◦ Il formato di questi messaggi di registro è <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$request" "\$http_host" "\$http_user_agent" "\$http_referer"</code> • <code>cgr-access.log.gz</code>: Richieste di replicazione cross-grid in entrata. ◦ Questi messaggi sono preceduti da <code>cgr</code>: quando esportato tramite <code>syslog</code>. ◦ Il formato di questi messaggi di registro è <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • <code>endpoint-access.log.gz</code>: Richieste S3 e Swift agli endpoint del bilanciatore del carico. ◦ Questi messaggi sono preceduti da <code>endpoint</code>: quando esportato tramite <code>syslog</code>. ◦ Il formato di questi messaggi di registro è <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • <code>nginx-gw-dns-check.log</code>: Correlato al nuovo avviso di controllo DNS.
ntp	File di configurazione e registri NTP.
Oggetti orfani	Registri relativi agli oggetti orfani.
sistema operativo	File di stato del nodo e della griglia, inclusi i servizi <code>pid</code> .
altro	File di registro sotto <code>/var/local/log</code> che non vengono raccolti in altre cartelle.
perf	Informazioni sulle prestazioni di CPU, rete e I/O del disco.
dati di Prometeo	Metriche Prometheus correnti, se la raccolta di log include dati Prometheus.
approvvigionamento	Registri relativi al processo di provisioning della rete.
zattera	Registri del cluster Raft utilizzati nei servizi della piattaforma.
ssh	Registri relativi alla configurazione e al servizio SSH.

Posizione dell'archivio	Descrizione
SNMP	Configurazione dell'agente SNMP utilizzata per l'invio di notifiche SNMP.
socket-dati	Dati socket per il debug di rete.
comandi-di-sistema.txt	Output dei comandi del contenitore StorageGRID . Contiene informazioni di sistema, come la rete e l'utilizzo del disco.
pacchetto di recupero sincronizzato	Correlato al mantenimento della coerenza dell'ultimo pacchetto di ripristino su tutti i nodi di amministrazione e di archiviazione che ospitano il servizio ADC.

Registri del software StorageGRID

È possibile utilizzare i log StorageGRID per risolvere i problemi.



Se si desidera inviare i log a un server syslog esterno o modificare la destinazione delle informazioni di controllo come `broadcast.log` e `names.log`, Vedere ["Configurare i messaggi di controllo e le destinazioni dei registri"](#) .

Registri generali di StorageGRID

Nome del file	Note	Trovato su
<code>/var/local/log/broadcast.log</code>	Il file principale per la risoluzione dei problemi StorageGRID . Selezionare SUPPORTO > Strumenti > Topologia griglia . Quindi seleziona Sito > Nodo > SSM > Eventi .	Tutti i nodi
<code>/var/local/log/broadcast-err.log</code>	Contiene un sottoinsieme di <code>broadcast.log</code> (messaggi con gravità ERROR e CRITICAL). Nel sistema vengono visualizzati anche i messaggi CRITICI. Selezionare SUPPORTO > Strumenti > Topologia griglia . Quindi seleziona Sito > Nodo > SSM > Eventi .	Tutti i nodi
<code>/var/local/core/</code>	Contiene tutti i file core dump creati se il programma termina in modo anomalo. Le possibili cause includono errori di asserzione, violazioni o timeout dei thread. Nota: Il file <code>/var/local/core/kexec_cmd</code> di solito è presente sui nodi dell'appliance e non indica un errore.	Tutti i nodi

Registri relativi alla cifratura

Nome del file	Note	Trovato su
/var/local/log/ssh-config-generation.log	Contiene i registri relativi alla generazione delle configurazioni SSH e al ricaricamento dei servizi SSH.	Tutti i nodi
/var/local/log/nginx/config-generation.log	Contiene i registri relativi alla generazione delle configurazioni nginx e al ricaricamento dei servizi nginx.	Tutti i nodi
/var/local/log/nginx-gw/config-generation.log	Contiene i registri relativi alla generazione delle configurazioni nginx-gw (e al ricaricamento dei servizi nginx-gw).	Nodi di amministrazione e gateway
/var/local/log/update-cipher-configurations.log	Contiene i registri relativi alla configurazione dei criteri TLS e SSH.	Tutti i nodi

Registri della federazione della griglia

Nome del file	Note	Trovato su
/var/local/log/update_grid_federation_config.log	Contiene i registri relativi alla generazione delle configurazioni nginx e nginx-gw per le connessioni di federazione della griglia.	Tutti i nodi

Registri NMS

Nome del file	Note	Trovato su
/var/local/log/nms.log	• Acquisisce notifiche dal Grid Manager e dal Tenant Manager. • Cattura gli eventi relativi al funzionamento del servizio NMS. Ad esempio, notifiche e-mail e modifiche alla configurazione. • Contiene gli aggiornamenti del bundle XML derivanti dalle modifiche di configurazione apportate al 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 della pagina ed errori HTTP Status 500.	Nodi amministrativi
/var/local/log/nms.errlog	Contiene messaggi di errore relativi agli aggiornamenti del database MySQL. Contiene il flusso di errore standard (stderr) dei servizi corrispondenti. Esiste un file di registro per servizio. Questi file sono generalmente vuoti, a meno che non ci siano problemi con il servizio.	Nodi amministrativi
/var/local/log/nms.requestlog	Contiene informazioni sulle connessioni in uscita dall'API di gestione ai servizi StorageGRID interni.	Nodi amministrativi

Registri di Server Manager

Nome del file	Note	Trovato su
/var/local/log/servermanager.log	File di registro per l'applicazione Server Manager in esecuzione sul server.	Tutti i nodi
/var/local/log/GridstatBackend.errlog	File di registro per l'applicazione backend GUI di Server Manager.	Tutti i nodi
/var/local/log/gridstat.errlog	File di registro per l'interfaccia utente grafica di Server Manager.	Tutti i nodi

Registri dei servizi StorageGRID

Nome del file	Note	Trovato su
/var/local/log/acct.errlog		Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/adc.errlog	Contiene il flusso di errore standard (stderr) dei servizi corrispondenti. Esiste un file di registro per servizio. Questi file sono generalmente vuoti, a meno che non ci siano problemi con il servizio.	Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/ams.errlog		Nodi amministrativi
/var/local/log/cassandra/system.log	Informazioni per l'archivio metadati (database Cassandra) che possono essere utilizzate se si verificano problemi durante l'aggiunta di nuovi nodi di archiviazione o se l'attività di riparazione di nodetool si blocca.	Nodi di archiviazione
/var/local/log/cassandra-reaper.log	Informazioni per il servizio Cassandra Reaper, che esegue riparazioni dei dati nel database Cassandra.	Nodi di archiviazione
/var/local/log/cassandra-reaper.errlog	Informazioni di errore per il servizio Cassandra Reaper.	Nodi di archiviazione
/var/local/log/chunk.errlog		Nodi di archiviazione
/var/local/log/cmn.errlog		Nodi amministrativi
/var/local/log/cms.errlog	Questo file di registro potrebbe essere presente nei sistemi che sono stati aggiornati da una versione precedente di StorageGRID. Contiene informazioni legacy.	Nodi di archiviazione
/var/local/log/dds.errlog		Nodi di archiviazione
/var/local/log/dmv.errlog		Nodi di archiviazione
/var/local/log/dynip*	Contiene i registri relativi al servizio dynip, che monitora la griglia per rilevare modifiche IP dinamiche e aggiorna la configurazione locale.	Tutti i nodi
/var/local/log/grafana.log	Il registro associato al servizio Grafana, utilizzato per la visualizzazione delle metriche in Grid Manager.	Nodi amministrativi

Nome del file	Note	Trovato su
/var/local/log/hagroups.log	Il registro associato ai gruppi ad alta disponibilità.	Nodi amministrativi e nodi gateway
/var/local/log/hagroups_events.log	Tiene traccia dei cambiamenti di stato, come la transizione da BACKUP a MASTER o FAULT.	Nodi amministrativi e nodi gateway
/var/local/log/idnt.errlog		Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/jaeger.log	Il registro associato al servizio Jaeger, utilizzato per la raccolta delle tracce.	Tutti i nodi
/var/local/log/kstn.errlog		Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/lambda*	Contiene i registri per il servizio S3 Select.	Nodi di amministrazione e gateway Solo alcuni nodi Admin e Gateway contengono questo registro. Vedi il "Requisiti e limitazioni di S3 Select per i nodi Admin e Gateway" .
/var/local/log/ldr.errlog		Nodi di archiviazione
/var/local/log/miscd/*.log	Contiene i registri per il servizio MISCD (Information Service Control Daemon), che fornisce un'interfaccia per interrogare e gestire i servizi su altri nodi e per gestire le configurazioni ambientali sul nodo, ad esempio interrogando lo stato dei servizi in esecuzione su altri nodi.	Tutti i nodi
/var/local/log/nginx/*.log	Contiene i log per il servizio nginx, che funge da meccanismo di autenticazione e comunicazione sicura per vari servizi di griglia (come Prometheus e Dynip) per poter comunicare con i servizi su altri nodi tramite API HTTPS.	Tutti i nodi

Nome del file	Note	Trovato su
/var/local/log/nginx-gw/*.log	Contiene registri generali relativi al servizio nginx-gw, inclusi i registri degli errori e i registri per le porte amministrative riservate sui nodi amministrativi.	Nodi amministrativi e nodi gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contiene i registri di accesso relativi al traffico di replicazione tra griglie.	Nodi amministrativi, nodi gateway o entrambi, in base alla configurazione della federazione della griglia. Presente solo sulla griglia di destinazione per la replica tra griglie.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contiene i registri di accesso per il servizio Load Balancer, che fornisce il bilanciamento del carico del traffico S3 dai client ai nodi di archiviazione.	Nodi amministrativi e nodi gateway
/var/local/log/persistence*	Contiene i registri per il servizio di persistenza, che gestisce i file sul disco radice che devono essere mantenuti anche dopo un riavvio.	Tutti i nodi
/var/local/log/prometheus.log	Per tutti i nodi, contiene il registro del servizio di esportazione dei nodi e il registro del servizio delle metriche di esportazione ade. Per i nodi amministrativi, 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 di archiviazione con servizio RSM
/var/local/log/rms.errlog	Contiene i registri per il servizio Replicated State Machine Service (RSM), utilizzato per i servizi della piattaforma S3.	Nodi di archiviazione con servizio RSM
/var/local/log/ssm.errlog		Tutti i nodi

Nome del file	Note	Trovato su
/var/local/log/update-s3vs-domains.log	Contiene i registri relativi all'elaborazione degli aggiornamenti per la configurazione dei nomi di dominio ospitati virtuali S3. Consultare le istruzioni per l'implementazione delle applicazioni client S3.	Nodi di amministrazione e gateway
/var/local/log/update-snmp-firewall.*	Contiene i registri relativi alle porte del 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 di amministrazione 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

- ["Informazioni su bycast.log"](#)
- ["Utilizzare l'API REST S3"](#)

Registri di distribuzione e manutenzione

È possibile utilizzare i registri di distribuzione e manutenzione per risolvere i problemi.

Nome del file	Note	Trovato su
/var/local/log/install.log	Creato durante l'installazione del software. Contiene una registrazione degli eventi di installazione.	Tutti i nodi
/var/local/log/expansion-progress.log	Creato durante le operazioni di espansione. Contiene una registrazione degli eventi di espansione.	Nodi di archiviazione
/var/local/log/pa-move.log	Creato durante l'esecuzione del <code>pa-move.sh</code> sceneggiatura.	Nodo di amministrazione primario
/var/local/log/pa-move-new_pa.log	Creato durante l'esecuzione del <code>pa-move.sh</code> sceneggiatura.	Nodo di amministrazione primario

Nome del file	Note	Trovato su
/var/local/log/pa-move-old_pa.log	Creato durante l'esecuzione del <code>pa-move.sh</code> sceneggiatura.	Nodo di amministrazione 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 di amministrazione 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

Informazioni su `broadcast.log`

Il file `/var/local/log/broadcast.log` è il file principale per la risoluzione dei problemi del software StorageGRID. C'è un `broadcast.log` file per ogni nodo della griglia. Il file contiene messaggi specifici per quel nodo della griglia.

Il file `/var/local/log/broadcast-err.log` è un sottoinsieme di `broadcast.log`. Contiene messaggi di gravità ERRORE e CRITICO.

Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati quando viene configurato un server syslog esterno. Vedere ["Configurare i messaggi di controllo e le destinazioni dei registri"](#).

Rotazione dei file per `broadcast.log`

Quando il `broadcast.log` file raggiunge 1 GB, il file esistente viene salvato e viene avviato un nuovo file di registro.

Il file salvato viene rinominato `broadcast.log.1` e il nuovo file è denominato `broadcast.log`. Quando il nuovo `broadcast.log` raggiunge 1 GB, `broadcast.log.1` viene rinominato e compresso per diventare `broadcast.log.2.gz`, e `broadcast.log` è rinominato `broadcast.log.1`.

Il limite di rotazione per `broadcast.log` è di 21 file. Quando la 22a versione del `broadcast.log` viene creato un file, il file più vecchio viene eliminato.

Il limite di rotazione per `broadcast-err.log` è composto da sette file.



Se un file di registro è stato compresso, non è possibile decomprimerlo nella stessa posizione in cui è stato scritto. La decompressione del file nella stessa posizione può interferire con gli script di rotazione del registro.

Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati

quando viene configurato un server syslog esterno. Vedere ["Configurare i messaggi di controllo e le destinazioni dei registri"](#).

Informazioni correlate

["Raccogli file di registro e dati di sistema"](#)

Messaggi in bycast.log

Messaggi in `bycast.log` sono scritti dall'ADE (Asynchronous Distributed Environment). ADE è l'ambiente di runtime utilizzato dai servizi di ciascun nodo della griglia.

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 del messaggio	Valore nell'esempio
Nodo ID	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-GGTHH:MM:SS.uuuuuu)
Livello di gravità	ERRORE
Numero di tracciamento interno	0906
Messaggio	SVMR: Il controllo dello stato di salute del volume 3 è fallito con il motivo 'TOUT'

Gravità dei messaggi in bycast.log

I messaggi in `bycast.log` vengono assegnati livelli di gravità.

Per esempio:

- **AVVISO** — Si è verificato un evento che dovrebbe essere registrato. La maggior parte dei messaggi di registro si trova a questo livello.
- **ATTENZIONE** — Si è verificata una condizione imprevista.
- **ERRORE** — Si è verificato un errore grave che avrà ripercussioni sulle operazioni.

- **CRITICO** — Si è verificata una condizione anomala che ha interrotto le normali operazioni. È necessario intervenire immediatamente sulla condizione di base.

Codici di errore in `broadcast.log`

La maggior parte dei messaggi di errore in `broadcast.log` contengono codici di errore.

La tabella seguente elenca i codici non numerici comuni in `broadcast.log`. Il significato esatto di un codice non numerico dipende dal contesto in cui viene riportato.

Codice di errore	Senso
SUCS	Nessun errore
GERR	Sconosciuto
CANC	Annullato
ABRT	Abortito
TUTTO	Tempo scaduto
INVL	Non valido
NFND	Non trovato
VERSO	Versione
CONF	Configurazione
FALLIRE	Fallito
ICPL	Incompleto
FATTO	Fatto
SUNV	Servizio non disponibile

La tabella seguente elenca i codici di errore numerici in `broadcast.log`.

Numero di errore	Codice di errore	Senso
001	EPERM	Operazione non consentita
002	ENOENT	Nessun file o directory con questo nome

Numero di errore	Codice di errore	Senso
003	ESRCH	Nessun processo del genere
004	EINTR	Chiamata di sistema interrotta
005	EIO	errore di I/O
006	ENXIO	Nessun dispositivo o indirizzo del genere
007	E2BIG	Elenco argomenti troppo lungo
008	ENOEXEC	Errore di formato Exec
009	EBADF	Numero di file errato
010	BAMBINO	Nessun processo figlio
011	DI NUOVO	Riprova
012	ENOMEM	Memoria esaurita
013	EACCES	Permesso negato
014	ERRORE	Indirizzo errato
015	ENOTBLK	Dispositivo di blocco richiesto
016	EBUSY	Dispositivo o risorsa occupati
017	EESI	Il file esiste
018	EXDEV	Collegamento tra dispositivi
019	ENODEV	Nessun dispositivo del genere
020	ENOTDIR	Non una directory
021	EISDIR	È una directory
022	EINVAL	Argomento non valido
023	ENFILE	Overflow della tabella dei file

Numero di errore	Codice di errore	Senso
024	EMFILE	Troppi file aperti
025	ENOTTY	Non una macchina da scrivere
026	ETXTBSY	File di testo occupato
027	EFBIG	File troppo grande
028	ENOSPC	Nessuno spazio rimasto sul dispositivo
029	ESPIPE	Ricerca illegale
030	EROFS	File system di sola lettura
031	EMLINK	Troppi link
032	EPIPE	Tubo rotto
033	EDOM	Argomento matematico fuori dal dominio della funzione
034	GAMMA	Risultato matematico non rappresentabile
035	EDEADLK	Si verificherebbe un blocco delle risorse
036	Smaltolungo	Nome del file troppo lungo
037	ENOLCK	Nessun blocco record disponibile
038	ENOSYS	Funzione non implementata
039	ENOTEMPTY	Directory non vuota
040	ELOOP	Sono stati riscontrati troppi link simbolici
041		
042	ENOMSG	Nessun messaggio del tipo desiderato
043	EIDRM	Identificatore rimosso
044	ECHRNG	Numero di canale fuori intervallo

Numero di errore	Codice di errore	Senso
045	EL2NSYNC	Livello 2 non sincronizzato
046	EL3HLT	Livello 3 interrotto
047	EL3RST	Ripristino di livello 3
048	ELNRNG	Numero di collegamento fuori intervallo
049	EUNATCH	Driver del protocollo non collegato
050	ENOCSE	Nessuna struttura CSI disponibile
051	EL2HLT	Livello 2 interrotto
052	EBADE	Scambio non valido
053	EBADR	Descrittore di richiesta non valido
054	EXFULL	Scambio completo
055	ENOANO	Nessun anodo
056	EBADRQC	Codice di richiesta non valido
057	EBADSLT	Slot non valido
058		
059	EBFONT	Formato file font non valido
060	ENOSTR	Dispositivo non in streaming
061	ENODATI	Nessun dato disponibile
062	ETIME	Timer scaduto
063	ENOSR	Risorse fuori flusso
064	ENONET	La macchina non è in rete
065	ENOPKG	Pacchetto non installato

Numero di errore	Codice di errore	Senso
066	EREMOTE	L'oggetto è remoto
067	ENOLINK	Il collegamento è stato interrotto
068	EADV	Errore di pubblicità
069	ESRMNT	Errore di srmount
070	ECOMM	Errore di comunicazione durante l'invio
071	EPROTO	Errore di protocollo
072	EMULTIHOP	Tentativo multihop
073	EDOTDOT	Errore specifico RFS
074	EBADMSG	Non è un messaggio di dati
075	Eoverflow	Valore troppo grande per il tipo di dati definito
076	ENOTUNIQ	Nome non univoco sulla rete
077	EBADFD	Descrittore di 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 collegare troppe librerie condivise
083	ELIBEXEC	Impossibile eseguire direttamente una libreria condivisa
084	EILSEQ	Sequenza di byte non valida
085	RIAVVIARE	La chiamata di sistema interrotta deve essere riavviata

Numero di errore	Codice di errore	Senso
086	ESTRPIPE	Errore del tubo di flusso
087	EUSERS	Troppi utenti
088	ENOTSOCK	Funzionamento della presa su non presa
089	EDESTADDRREQ	Indirizzo di destinazione richiesto
090	EMSGSIZE	Messaggio troppo lungo
091	EPROTOTIPO	Tipo di protocollo errato per il socket
092	ENOPROTOOPT	Protocollo non disponibile
093	EPROTONOSUPPORT	Protocollo non supportato
094	ESOCKTNOSUPPORT	Tipo di socket non supportato
095	EOPNOTSUPP	Operazione non supportata sull'endpoint di trasporto
096	EPFNOSUPPORT	Famiglia di protocolli non supportata
097	EAFNOSUPPORT	Indirizzo famiglia non supportato dal protocollo
098	EADDRINUSE	Indirizzo già in uso
099	EADDRNOTAVAIL	Impossibile assegnare l'indirizzo richiesto
100	ENETDOWN	La rete è inattiva
101	ENETUNREACH	La rete non è raggiungibile
102	ENETRESET	Connessione di rete interrotta a causa del ripristino
103	ECONNABORTED	Il software ha causato la terminazione della connessione
104	ECONNRESET	Connessione ripristinata dal peer
105	ENOBUFS	Nessuno spazio buffer disponibile
106	EISCONN	L'endpoint di trasporto è già connesso

Numero di errore	Codice di errore	Senso
107	ENOTCONN	L'endpoint di trasporto non è connesso
108	SPEGNIMENTO	Impossibile inviare dopo l'arresto dell'endpoint di trasporto
109	ETOOMANYREFS	Troppi riferimenti: impossibile unire
110	ETIMEDOUT	Connessione scaduta
111	ECONNRIFIUTATO	Connessione rifiutata
112	EHOSTDOWN	L'host è inattivo
113	EHOSTUNREACH	Nessun percorso per l'host
114	GIÀ	Operazione già in corso
115	EINPROGRESS	Operazione in corso
116		
117	EUCLEAN	La struttura necessita di pulizia
118	ENOTNAM	Non è un file di tipo denominato XENIX
119	DISPONIBILE	Nessun semaforo XENIX disponibile
120	EISNAM	È un file di tipo denominato
121	EREMOTEIO	Errore di I/O remoto
122	EDQUOT	Quota superata
123	ENOMEDIO	Nessun mezzo trovato
124	TIPOMEDIO	Tipo di mezzo sbagliato
125	ECANCELED	Operazione annullata
126	ENOKEY	Chiave richiesta non disponibile
127	EKEYEXPIRED	La chiave è scaduta

Numero di errore	Codice di errore	Senso
128	EKEYREVOKED	La chiave è stata revocata
129	EKEYREJECTED	La chiave è stata rifiutata dal servizio
130	PROPRIETARIOMORTO	Per mutex robusti: il proprietario è morto
131	NON RECUPERABILI	Per mutex robusti: Stato non recuperabile

Configurare le destinazioni dei messaggi di controllo e dei registri

Considerazioni sull'utilizzo di un server syslog esterno

Un server syslog esterno è un server esterno a StorageGRID che puoi utilizzare per raccogliere informazioni di controllo del sistema in un'unica posizione. Utilizzando un server syslog esterno è possibile ridurre il traffico di rete sui nodi amministrativi e gestire le informazioni in modo più efficiente. Per StorageGRID, il formato del pacchetto dei messaggi syslog in uscita è conforme a RFC 3164.

I tipi di informazioni di controllo che è possibile inviare al server syslog esterno includono:

- Registri di controllo contenenti i messaggi di controllo generati durante il normale funzionamento del sistema
- Eventi relativi alla sicurezza come accessi ed escalation alla radice
- Registri 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 una griglia di grandi dimensioni, si utilizzano più tipi di applicazioni S3 o si desidera conservare tutti i dati di audit. L'invio di informazioni di audit a un server syslog esterno consente di:

- Raccogli e gestisci 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 tuoi nodi amministrativi poiché le informazioni di controllo vengono trasferite direttamente dai vari nodi di archiviazione al server syslog esterno, senza dover passare attraverso un nodo amministrativo.



Quando i log vengono inviati a un server syslog esterno, i singoli log superiori a 8.192 byte vengono troncati alla fine del messaggio per conformarsi alle limitazioni comuni nelle implementazioni dei server syslog esterni.



Per massimizzare le opzioni di recupero completo dei dati in caso di guasto del server syslog esterno, fino a 20 GB di registri locali di record di controllo(`localaudit.log`) vengono 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 prevede di 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:** il 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. Non vi è alcun vantaggio significativo in termini di sicurezza nell'utilizzare una chiave privata crittografata, poiché sia la chiave che la passphrase devono essere memorizzate; per semplicità, si consiglia di utilizzare una chiave privata non crittografata, se disponibile.

Come stimare la dimensione del server syslog esterno

Normalmente, la griglia viene dimensionata per raggiungere la produttività richiesta, definita in termini di operazioni S3 al secondo o byte al secondo. Ad esempio, potresti avere il requisito che la tua griglia gestisca 1.000 operazioni S3 al secondo, o 2.000 MB al secondo, di inserimenti e recuperi di oggetti. Dovresti dimensionare il tuo server syslog esterno in base ai requisiti di dati della tua griglia.

Questa sezione fornisce alcune formule euristiche che aiutano a stimare la velocità e la dimensione media dei messaggi di log di vario tipo che il server syslog esterno deve essere in grado di gestire, espresse in termini di caratteristiche prestazionali note o desiderate della griglia (operazioni S3 al secondo).

Utilizzare S3 operazioni al secondo nelle formule di stima

Se la griglia è stata dimensionata per una velocità espressa in byte al secondo, è necessario convertire questa dimensione in operazioni S3 al secondo per utilizzare le formule di stima. Per convertire la velocità effettiva della griglia, è necessario innanzitutto determinare la dimensione media dell'oggetto, operazione che è possibile effettuare utilizzando le informazioni presenti nei registri di controllo e nelle metriche esistenti (se presenti) oppure sfruttando la conoscenza delle applicazioni che utilizzeranno StorageGRID. Ad esempio, se la griglia è stata dimensionata per raggiungere una velocità di elaborazione di 2.000 MB/secondo e la dimensione media degli oggetti è di 2 MB, la griglia è stata dimensionata per 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 del caso comune (piuttosto che stime del caso peggiore). A seconda della configurazione e del carico di lavoro, potresti riscontrare una frequenza di messaggi syslog o un volume di dati syslog maggiore o minore rispetto a quanto previsto dalle formule. Le formule sono da intendersi solo come linee guida.

Formule di stima per i registri di controllo

Se non si hanno informazioni sul carico di lavoro S3, a parte il numero di operazioni S3 al secondo che la griglia dovrebbe supportare, è possibile stimare il volume di log di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule, partendo dal presupposto che i Livelli di controllo vengano lasciati impostati sui valori predefiniti (tutte le categorie impostate su Normale, eccetto Archiviazione, che è impostata

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 dovrebbe essere dimensionato per supportare 2.000 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere archiviare) i dati del registro di controllo a una velocità di 1,6 MB al secondo.

Se si conoscono meglio i propri carichi di lavoro, è possibile ottenere stime più precise. Per i registri di controllo, le variabili aggiuntive più importanti sono la percentuale di operazioni S3 che sono PUT (rispetto a GETS) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni di 4 caratteri utilizzate nella tabella sono nomi di campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Tasto S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Utilizziamo P per rappresentare la percentuale di operazioni S3 che sono PUT, dove $0 \leq P \leq 1$ (quindi per un carico di lavoro PUT del 100%, $P = 1$ e per un carico di lavoro GET del 100%, $P = 0$).

Utilizziamo K per rappresentare la dimensione media della somma dei nomi degli account S3, del bucket S3 e della chiave S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi di lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi di 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 log di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule, partendo dal presupposto che i Livelli di controllo vengano lasciati impostati sui valori predefiniti (tutte le categorie impostate su Normale, tranne Archiviazione, che è impostata su Errore):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate  
Audit Log Average Size = (570 + K) bytes
```


Ad esempio, se la griglia è dimensionata per 1.000 operazioni S3 al secondo, il carico di lavoro è costituito al 50% da PUT e i nomi degli account S3, dei bucket e degli oggetti sono in media pari a 90 byte, il server syslog esterno dovrebbe essere dimensionato per supportare 1.500 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere archiviare) 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 impostate su Normale, tranne Archiviazione, che è impostata su Errore). Non sono disponibili formule dettagliate per stimare la frequenza e la dimensione media dei messaggi di controllo per impostazioni di livello di controllo non predefinite. Tuttavia, la tabella seguente può essere utilizzata per effettuare una stima approssimativa della frequenza; è possibile utilizzare la formula per la dimensione media fornita per i registri di controllo, ma è importante tenere presente che è probabile che si ottenga 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 impostati su Debug o Normale	Tasso di controllo log = 8 x tasso di operazioni S3
Codifica di cancellazione: livelli di controllo tutti impostati su Debug o Normale	Utilizzare la stessa formula delle impostazioni predefinite

Formule di stima per eventi di sicurezza

Gli eventi di sicurezza non sono correlati alle operazioni S3 e in genere producono un volume trascurabile di registri e dati. Per questi motivi non vengono fornite formule di stima.

Formule di stima per i registri delle applicazioni

Se non si hanno informazioni sul carico di lavoro S3, a parte il numero di operazioni S3 al secondo che la griglia dovrebbe supportare, è possibile stimare il volume dei registri 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 la griglia è dimensionata per 1.000 operazioni S3 al secondo, il server syslog esterno dovrebbe essere dimensionato per supportare 3.300 log delle applicazioni al secondo ed essere in grado di ricevere (e archiviare) i dati dei log delle applicazioni a una velocità di circa 1,2 MB al secondo.

Se si conoscono meglio i propri carichi di lavoro, è possibile ottenere stime più precise. Per i registri delle applicazioni, le variabili aggiuntive più importanti sono la strategia di protezione dei dati (replicazione vs. codifica di cancellazione), la percentuale di operazioni S3 che sono PUT (vs. GET/altro) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni di 4 caratteri utilizzate nella tabella sono nomi di campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Tasto S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Esempi di stime dimensionali

In questa sezione vengono illustrati alcuni casi esemplificativi su come utilizzare le formule di stima per le griglie con i seguenti metodi di protezione dei dati:

- Replicazione
- Codifica di cancellazione

Se si utilizza la replica per la protezione dei dati

Sia P la percentuale di operazioni S3 che sono PUT, dove $0 \leq P \leq 1$ (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 nomi degli account S3, del bucket S3 e della chiave S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi di lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi di lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Allora K ha un valore di 90 (13+13+28+36).

Se riesci a determinare i valori per P e K , puoi stimare il volume dei log delle applicazioni che il tuo server syslog esterno dovrà essere in grado di 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
```

Quindi, ad esempio, se la griglia è dimensionata per 1.000 operazioni S3 al secondo, il carico di lavoro è costituito al 50% da PUT e i nomi degli account S3, dei bucket e degli oggetti sono in media pari a 90 byte, il server syslog esterno dovrebbe essere dimensionato per supportare 1.800 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 la codifica di cancellazione per la protezione dei dati

Sia P la percentuale di operazioni S3 che sono PUT, dove $0 \leq P \leq 1$ (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 nomi degli account S3, del bucket S3 e della chiave S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi di lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi di lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Allora K ha un valore di 90 (13+13+28+36).

Se riesci a determinare i valori per P e K , puoi stimare il volume dei log delle applicazioni che il tuo server syslog esterno dovrà essere in grado di 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
```

Quindi, ad esempio, se la griglia è dimensionata per 1.000 operazioni S3 al secondo, il carico di lavoro è costituito al 50% da PUT e i nomi degli account S3, dei bucket e degli oggetti sono in media pari a 90 byte, il server syslog esterno dovrebbe essere dimensionato per supportare 2.250 log delle applicazioni al secondo e dovrebbe essere in grado di ricevere (e in genere archiviare) i 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 le intestazioni delle richieste HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client, configurare un server syslog esterno e specificare dove inviare i registri di controllo, i registri degli eventi di sicurezza e i registri del software StorageGRID .

I messaggi e i registri di controllo 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 controllo e registri per monitorare l'attività e gli eventi del sistema.

Facoltativamente, è possibile configurare un server syslog esterno per salvare le informazioni di audit in remoto. L'utilizzo di un server esterno riduce al minimo l'impatto sulle 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 una griglia di grandi dimensioni, si utilizzano più tipi di applicazioni S3 o si desidera conservare tutti i dati di audit. Vedere ["Configurare i messaggi di controllo e il server syslog esterno"](#) per i dettagli.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#) .
- Se si prevede di configurare un server syslog esterno, è necessario aver esaminato il ["considerazioni sull'utilizzo di un server syslog esterno"](#) e ha garantito che il server avesse capacità sufficiente per ricevere e archiviare i file di registro.
- Se si prevede di configurare un server syslog esterno utilizzando il protocollo TLS o RELP/TLS, è necessario disporre dei certificati CA e client del server richiesti e della chiave privata del client.

Modifica i livelli dei messaggi di controllo

È possibile impostare un livello di controllo diverso per ciascuna delle seguenti categorie di messaggi nel registro di controllo:

Categoria di revisione	Impostazione predefinita	Ulteriori informazioni
Sistema	Normale	"Messaggi di controllo del sistema"
Magazzinaggio	Errore	"Messaggi di controllo dell'archiviazione degli oggetti"
Gestione	Normale	"Messaggio di controllo di gestione"
Il cliente legge	Normale	"Il cliente ha letto i messaggi di controllo"
Il cliente scrive	Normale	"Il cliente scrive messaggi di audit"
ILM	Normale	"Messaggi di controllo ILM"
Replicazione cross-grid	Errore	"CGRR: richiesta di replicazione tra griglie"



Queste impostazioni predefinite si applicano se StorageGRID è stato inizialmente installato utilizzando la versione 10.3 o successiva. Se inizialmente hai utilizzato 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 immediatamente effettive.

Passi

1. Selezionare **CONFIGURAZIONE > Monitoraggio > Server di audit e syslog**.
2. Per ogni categoria di messaggio di controllo, selezionare un livello di controllo dall'elenco a discesa:

Livello di audit	Descrizione
Spento	Nessun messaggio di controllo della categoria viene registrato.
Errore	Vengono registrati solo i messaggi di errore, ovvero i messaggi di controllo 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.
Debug	Obsoleto. Questo livello si comporta come il livello di controllo Normale.

I messaggi inclusi per ogni livello specifico includono quelli che verrebbero registrati ai livelli superiori. Ad

esempio, il livello Normale include tutti i messaggi di errore.



Se non è necessario un registro dettagliato delle operazioni di lettura client per le applicazioni S3, è possibile modificare facoltativamente l'impostazione **Lettture client** in **Errore** per ridurre il numero di messaggi di controllo registrati nel registro di controllo.

3. Seleziona **Salva**.

Un banner verde indica che la configurazione è stata salvata.

Definisci 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.

Passi

1. Nella sezione **Intestazioni protocollo di controllo**, definisci le intestazioni delle richieste HTTP che desideri includere nei messaggi di controllo di lettura e scrittura del client.

Utilizzare un asterisco (*) come carattere jolly per trovare la corrispondenza con zero o più caratteri.
Utilizzare la sequenza di escape (*) per trovare la corrispondenza con un asterisco letterale.

2. Seleziona **Aggiungi un'altra intestazione** per creare intestazioni aggiuntive, se necessario.

Quando in una richiesta vengono trovate intestazioni HTTP, queste vengono incluse nel messaggio di controllo nel campo HTRH.



Le intestazioni delle richieste del protocollo di controllo vengono registrate solo se il livello di controllo per **Lettture client** o **Scritture client** non è **Disattivato**.

3. Seleziona **Salva**

Un banner verde indica che la configurazione è stata salvata.

Utilizza un server syslog esterno

Facoltativamente, è possibile configurare un server syslog esterno per salvare i log di controllo, i log delle applicazioni e i log degli eventi di sicurezza in una posizione esterna alla griglia.



Se non si desidera utilizzare un server syslog esterno, saltare questo passaggio e andare a [Seleziona le destinazioni delle informazioni di audit](#).



Se le opzioni di configurazione disponibili in questa procedura non sono sufficientemente flessibili per soddisfare le vostre esigenze, è possibile applicare opzioni di configurazione aggiuntive utilizzando `audit-destinations` endpoint, che si trovano nella sezione API privata del ["API di gestione della griglia"](#). Ad esempio, è possibile utilizzare l'API se si desidera utilizzare server syslog diversi per gruppi diversi di nodi.

Inserisci le informazioni syslog

Accedere alla procedura guidata Configura server syslog esterno e fornire le informazioni necessarie a StorageGRID per accedere al server syslog esterno.

Passi

1. Dalla pagina Server di controllo e syslog, selezionare **Configura server syslog esterno**. Oppure, se in precedenza hai configurato un server syslog esterno, seleziona **Modifica server syslog esterno**.

Viene visualizzata la procedura guidata Configura server syslog esterno.

2. Per il passaggio **Inserisci 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. Immettere 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 aiuta a proteggere le connessioni tra la griglia e il server syslog esterno. Per ulteriori informazioni, consultare ["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 la funzionalità del protocollo syslog per garantire una consegna affidabile dei messaggi di evento. L'utilizzo di RELP può aiutare a prevenire la perdita di informazioni di audit se il server syslog esterno deve essere riavviato.

5. Selezionare **Continua**.
6. Se hai selezionato **TLS** o **RELP/TLS**, carica 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 chiave.
 - c. Selezionare **Apri** per caricare il file.

Accanto al nome del certificato o del file chiave viene visualizzato un segno di spunta verde, che indica che il caricamento è stato eseguito correttamente.

7. Selezionare **Continua**.

Gestisci il contenuto syslog

È possibile selezionare quali informazioni inviare al server syslog esterno.

Passi

1. Per il passaggio **Gestisci contenuto syslog** della procedura guidata, seleziona ogni tipo di informazione di controllo che desideri inviare al server syslog esterno.
 - **Invia registri di controllo**: invia eventi StorageGRID e attività di sistema
 - **Invia eventi di sicurezza**: invia eventi di sicurezza, ad esempio quando un utente non autorizzato

tenta di accedere o un utente accede come root

- **Invia registri applicazione:** Invia ["File di registro del software StorageGRID"](#) utile per la risoluzione dei problemi, tra cui:

- `bycast-err.log`
- `bycast.log`
- `jaeger.log`
- `nms.log` (Solo nodi amministrativi)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

- **Invia registri di accesso:** invia registri di accesso HTTP per richieste esterne a Grid Manager, Tenant Manager, endpoint del bilanciamento del carico configurati e richieste di federazione della griglia da sistemi remoti.

2. Utilizzare i menu a discesa per selezionare la gravità e la facilità (tipo di messaggio) per ciascuna categoria di informazioni di audit che si desidera inviare.

Impostando i valori di gravità e di funzionalità è possibile aggregare i registri in modi personalizzabili per un'analisi più semplice.

- a. Per **Gravità**, seleziona **Passthrough** oppure seleziona un valore di gravità compreso tra 0 e 7.

Se selezioni un valore, il valore selezionato verrà applicato a tutti i messaggi di questo tipo. Se si sovrascrive la gravità con un valore fisso, le informazioni sui diversi livelli di gravità andranno perse.

Gravità	Descrizione
Passaggio	Ogni messaggio inviato al syslog esterno deve 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 vengono generati dalla distribuzione Linux sui nodi. • Per i registri delle applicazioni, la gravità varia tra "info" e "notice", a seconda del problema. Ad esempio, l'aggiunta di un server NTP e la configurazione di un gruppo HA forniscono il valore "info", mentre l'arresto intenzionale del servizio SSM o RSM fornisce il valore "notice". • Per i registri di accesso, la gravità è "info".
0	Emergenza: il sistema è inutilizzabile
1	Attenzione: è necessario intervenire immediatamente
2	Critico: Condizioni critiche
3	Errore: Condizioni di errore

Gravità	Descrizione
4	Attenzione: Condizioni di avviso
5	Avviso: condizione normale ma significativa
6	Informativo: Messaggi informativi
7	Debug: messaggi a livello di debug

- b. Per **Struttura**, selezionare **Passthrough** oppure selezionare un valore di struttura compreso tra 0 e 23.

Se selezioni un valore, questo verrà applicato a tutti i messaggi di questo tipo. Se si sovrascrive una struttura con un valore fisso, le informazioni sulle diverse strutture andranno perse.

Facilità	Descrizione
Passaggio	Ogni messaggio inviato al syslog esterno deve avere lo stesso valore di funzionalità di quando è stato registrato localmente sul nodo: • Per i registri di controllo, la funzione 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 hanno i seguenti valori di funzionalità: ◦ <code>broadcast.log</code>: utente o demone ◦ <code>broadcast-err.log</code>: utente, demone, local3 o local4 ◦ <code>jaeger.log</code>: locale2 ◦ <code>nms.log</code>: locale3 ◦ <code>prometheus.log</code>: locale4 ◦ <code>raft.log</code>: locale5 ◦ <code>hagroups.log</code>: locale6 • Per i registri di accesso, la funzione inviata al server syslog esterno è "local0".
0	kern (messaggi del kernel)
1	utente (messaggi a livello utente)
2	posta
3	demone (demoni di sistema)

Facilità	Descrizione
4	auth (messaggi di sicurezza/autorizzazione)
5	syslog (messaggi generati internamente da syslogd)
6	lpr (sottosistema della stampante di linea)
7	notizie (sottosistema di notizie di rete)
8	UUCP
9	cron (demone dell'orologio)
10	sicurezza (messaggi di sicurezza/autorizzazione)
11	FTP
12	NTP
13	logaudit (revisione dei registri)
14	logalert (avviso di registro)
15	orologio (demone dell'orologio)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Selezionare **Continua**.

Invia messaggi di prova

Prima di iniziare a utilizzare un server syslog esterno, è necessario richiedere a tutti i nodi della griglia di inviare messaggi di prova al server syslog esterno. Dovresti utilizzare questi messaggi di prova per convalidare l'intera infrastruttura di raccolta dei log prima di impegnarti a inviare dati al server syslog esterno.



Non utilizzare la configurazione del server syslog esterno finché non hai verificato che il server syslog esterno ha ricevuto un messaggio di prova da ciascun nodo della griglia e che il messaggio è stato elaborato come previsto.

Passi

1. Se non si desidera inviare messaggi di prova perché si è certi che il server syslog esterno sia configurato correttamente e possa ricevere informazioni di audit da tutti i nodi della griglia, selezionare **Salta e termina**.

Un banner verde indica che la configurazione è stata salvata.

2. Altrimenti, seleziona **Invia messaggi di prova** (consigliato).

I risultati del test vengono visualizzati continuamente sulla pagina finché non si interrompe il test. Mentre il test è in corso, i messaggi di controllo continuano a essere inviati alle destinazioni configurate in precedenza.

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 aiutarti a risolvere eventuali errori.

4. Attendi finché non vedi un banner verde che indica che tutti i nodi hanno superato il test.
5. Controllare il server syslog per verificare se i messaggi di prova 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 altrettanto rigoroso come gli altri protocolli.

6. Seleziona **Interrompi e termina**.

Verrai reindirizzato alla pagina **Server di audit e syslog**. Un banner verde indica che la configurazione del server syslog è stata salvata.



Le informazioni di controllo StorageGRID non vengono inviate al server syslog esterno finché non si seleziona una destinazione che includa il server syslog esterno.

Seleziona le destinazioni delle informazioni di audit

È possibile specificare dove salvare i registri di controllo, i registri degli eventi di sicurezza e "[Registri 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 trovare quale nodo ha le voci più recenti utilizzando `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.

Passi

1. Nella pagina Server di controllo e syslog, selezionare la destinazione per le informazioni di controllo.



Solo nodi locali e server syslog esterno in genere offrono prestazioni migliori.

Opzione	Descrizione
Solo nodi locali (predefinito)	I messaggi di controllo, i registri degli eventi di sicurezza e i registri delle applicazioni non vengono inviati ai nodi di amministrazione. Vengono invece salvati solo sui nodi che li hanno generati ("nodo locale"). Le informazioni di audit generate su ogni nodo locale vengono memorizzate in <code>/var/local/log/localaudit.log</code>. Nota: StorageGRID rimuove periodicamente i registri locali a rotazione per liberare spazio. Quando il file di registro di un nodo raggiunge 1 GB, il file esistente viene salvato e ne viene avviato uno nuovo. Il limite di rotazione per il registro è di 21 file. Quando viene creata la 22a versione del file di registro, il file di registro più vecchio viene eliminato. In media, su ogni nodo vengono archiviati circa 20 GB di dati di registro.
Nodi amministrativi/nodi locali	I messaggi di controllo vengono inviati al registro di controllo sui nodi di amministrazione, mentre i registri degli eventi di sicurezza e i registri delle applicazioni vengono archiviati sui nodi che li hanno generati. Le informazioni di audit sono archiviate nei seguenti file: • Nodi amministrativi (primari e non primari): <code>/var/local/audit/export/audit.log</code> • Tutti i nodi: Il <code>/var/local/log/localaudit.log</code> il file è solitamente vuoto o mancante. Potrebbe contenere informazioni secondarie, come una copia aggiuntiva di alcuni messaggi.
Server syslog esterno	Le informazioni di audit vengono inviate a un server syslog esterno e salvate sui nodi locali(<code>/var/local/log/localaudit.log</code>). Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione è abilitata 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 di amministrazione 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 è abilitata solo dopo aver configurato un server syslog esterno.

2. Seleziona **Salva**.

Viene visualizzato un messaggio di avviso.

3. Selezionare **OK** per confermare che si desidera modificare la destinazione delle informazioni di controllo.

Un banner verde indica che la configurazione di audit è stata salvata.

I nuovi registri vengono inviati alle destinazioni selezionate. I registri esistenti rimangono nella loro posizione attuale.

Utilizzare il monitoraggio SNMP

Utilizzare il monitoraggio SNMP

Se si desidera monitorare StorageGRID tramite il protocollo SNMP (Simple Network Management Protocol), è necessario configurare l'agente SNMP incluso in StorageGRID.

- ["Configurare l'agente SNMP"](#)
- ["Aggiorna l'agente SNMP"](#)

Capacità

Ogni nodo StorageGRID esegue un agente SNMP, o demone, che fornisce un MIB. StorageGRID MIB contiene definizioni di tabelle e notifiche per gli avvisi. Il MIB contiene anche informazioni descrittive del sistema, come la piattaforma e il numero di modello per ciascun nodo. Ogni nodo StorageGRID supporta anche un sottoinsieme di oggetti MIB-II.



Vedere ["Accedi ai file MIB"](#) se vuoi scaricare i file MIB sui nodi della tua griglia.

Inizialmente, SNMP è disabilitato 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 in sola lettura per le query e può inviare due tipi di notifiche basate su eventi a un sistema di gestione:

Trappole

Le trappole sono notifiche inviate dall'agente SNMP che non richiedono la conferma da parte del sistema di gestione. Le trappole servono a notificare al sistema di gestione che si è verificato un evento all'interno StorageGRID, ad esempio l'attivazione di un avviso.

Le trappole sono supportate in tutte e tre le versioni di SNMP.

Informa

Le informazioni sono simili alle trappole, ma richiedono il riconoscimento da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un certo lasso di tempo, invia nuovamente l'informazione finché non riceve una conferma o finché 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:

- A qualsiasi livello di gravità viene attivato un avviso predefinito o personalizzato. Per sopprimere le notifiche SNMP per un avviso, è necessario ["configurare un silenzio"](#) per l'avviso. Le notifiche di avviso vengono inviate da ["mittente preferito Nodo amministratore"](#).

Ogni avviso viene mappato su 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 queste trappole, vedere ["Riferimento avvisi"](#).

Supporto della versione SNMP

La tabella fornisce un riepilogo di alto livello di ciò che è supportato 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 e delle query	Stringa della comunità	Stringa della comunità	Modello di sicurezza basato sull'utente (USM) utente
Notifiche (TRAPPOLA e INFORMA)	Solo trappole	Intrappola e informa	Intrappola e informa
Autenticazione e delle notifiche	Comunità trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Comunità trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Utente USM per ogni destinazione trap

Limitazioni

- StorageGRID supporta l'accesso MIB in 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 del trasporto (TSM).
- SNMPv3: l'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).
- SNMPv3: l'unico protocollo di 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 in sola lettura e le notifiche.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .

Informazioni su questo compito

L'agente SNMP StorageGRID supporta SNMPv1, SNMPv2c e SNMPv3. È possibile configurare l'agente per una o più versioni. Per SNMPv3 è supportata solo l'autenticazione USM (User Security Model).

Tutti i nodi della griglia utilizzano la stessa configurazione SNMP.

Specificare la configurazione di base

Come primo passo, abilitare l'agente SNMP StorageGRID e fornire informazioni di base.

Passi

1. Selezionare **CONFIGURAZIONE > Monitoraggio > Agente SNMP**.

Viene visualizzata la pagina dell'agente SNMP.

2. Per abilitare l'agente SNMP su tutti i nodi della griglia, selezionare la casella di controllo **Abilita SNMP**.
3. Inserire le seguenti informazioni nella sezione Configurazione di base.

Campo	Descrizione
Contatto di sistema	Opzionale. Contatto primario per il sistema StorageGRID , restituito nei messaggi SNMP come sysContact. Il contatto di sistema è in genere un indirizzo e-mail. Questo valore si applica a tutti i nodi nel sistema StorageGRID . Contatto di sistema può contenere al massimo 255 caratteri.
Posizione del sistema	Opzionale. Posizione del sistema StorageGRID , restituita nei messaggi SNMP come sysLocation. La posizione del sistema può essere qualsiasi informazione utile per identificare dove si trova il sistema StorageGRID . Ad esempio, potresti utilizzare l'indirizzo di una struttura. Questo valore si applica a tutti i nodi nel sistema StorageGRID . Posizione del sistema può contenere al massimo 255 caratteri.
Abilita le notifiche dell'agente SNMP	• Se selezionato, l'agente SNMP StorageGRID invia notifiche trap e inform. • Se non selezionato, l'agente SNMP supporta l'accesso MIB in sola lettura, ma non invia alcuna notifica SNMP.

Campo	Descrizione
Abilita trappole di autenticazione	Se selezionata, l'agente SNMP StorageGRID invia trap di autenticazione se riceve messaggi di protocollo autenticati in modo non corretto.

Inserisci stringhe di comunità

Se si utilizza SNMPv1 o SNMPv2c, compilare la sezione Stringhe della community.

Quando il sistema di gestione interroga il MIB StorageGRID , invia una stringa di community. Se la stringa della community corrisponde a uno dei valori specificati qui, l'agente SNMP invia una risposta al sistema di gestione.

Passi

1. Per **Community di sola lettura**, immettere facoltativamente una stringa di community per consentire l'accesso MIB di sola lettura sugli indirizzi agente IPv4 e IPv6.



Per garantire la sicurezza del tuo sistema StorageGRID , non utilizzare "public" come stringa della community. Se si lascia vuoto questo campo, l'agente SNMP utilizza l'ID griglia del sistema StorageGRID come stringa della community.

Ogni stringa di comunità può contenere al massimo 32 caratteri e non può contenere spazi.

2. Seleziona **Aggiungi un'altra stringa della community** per aggiungere altre stringhe.

Sono consentite fino a cinque stringhe.

Crea destinazioni trappola

Utilizzare la scheda Destinazioni trap nella sezione Altre configurazioni per definire una o più destinazioni per le notifiche trap o informative StorageGRID . Quando si abilita l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Le notifiche standard vengono inviate anche per le entità MIB-II supportate (ad esempio, ifDown e coldStart).

Passi

1. Nel campo **Community trap predefinita**, immettere facoltativamente la stringa della community predefinita che si desidera utilizzare per le destinazioni trap SNMPv1 o SNMPv2.

Se necessario, è possibile fornire una stringa di community diversa ("personalizzata") quando si definisce una destinazione trap specifica.

La comunità trap predefinita può contenere al massimo 32 caratteri e non può contenere spazi.

2. Per aggiungere una destinazione trap, selezionare **Crea**.
3. Selezionare la versione SNMP che verrà utilizzata per questa destinazione trap.
4. Compila il modulo Crea destinazione trappola per la versione selezionata.

SNMPv1

Se hai selezionato SNMPv1 come versione, compila questi campi.

Campo	Descrizione
Tipo	Deve essere Trap per SNMPv1.
Ospite	Un indirizzo IPv4 o IPv6 oppure un nome di dominio completo (FQDN) per ricevere la trap.
Porta	Utilizzare 162, che è la porta standard per le 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 della comunità	Utilizzare la community trap predefinita, se ne è stata specificata una, oppure immettere una stringa community personalizzata per questa destinazione trap. La stringa community personalizzata può contenere al massimo 32 caratteri e non può contenere spazi.

SNMPv2c

Se hai selezionato SNMPv2c come versione, compila questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trappole o informazioni.
Ospite	Un indirizzo IPv4 o IPv6 o FQDN per ricevere la trap.
Porta	Utilizzare 162, che è la porta standard per le 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 della comunità	Utilizzare la community trap predefinita, se ne è stata specificata una, oppure immettere una stringa community personalizzata per questa destinazione trap. La stringa community personalizzata può contenere al massimo 32 caratteri e non può contenere spazi.

SNMPv3

Se hai selezionato SNMPv3 come versione, compila questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trappole o informazioni.
Ospite	Un indirizzo IPv4 o IPv6 o FQDN per ricevere la trap.
Porta	Utilizzare 162, che è la porta standard per le 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 hai selezionato Trappola, verranno visualizzati solo gli utenti USM senza ID motore autorevoli. • Se hai selezionato Informa, verranno visualizzati solo gli utenti USM con ID motore autorevoli. • Se non vengono visualizzati utenti: i. Creare e salvare la destinazione della trappola. ii. Vai a Crea 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. Seleziona **Crea**.

La destinazione della trappola viene creata e aggiunta alla tabella.

Crea indirizzi di agenti

Facoltativamente, utilizzare la scheda Indirizzi agente nella sezione Altre configurazioni per specificare uno o più "indirizzi di ascolto". Questi sono gli indirizzi StorageGRID sui quali l'agente SNMP può ricevere query.

Se non si configura un indirizzo agente, l'indirizzo di ascolto predefinito è la porta UDP 161 su tutte le reti StorageGRID .

Passi

1. Seleziona **Crea**.
2. Inserisci 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 utilizzerà UDP o TCP. Per impostazione predefinita, SNMP utilizza UDP.
Rete StorageGRID	Su quale rete StorageGRID l'agente ascolterà. • Reti Grid, Admin e Client: l'agente SNMP ascolterà le query su tutte e tre le reti. • Rete a griglia • Rete di amministrazione • Rete clienti Nota: se si utilizza la rete client per dati non sicuri 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 ascolto. La porta UDP predefinita per un agente SNMP è 161, ma è possibile immettere qualsiasi numero di porta non utilizzato. Nota: quando si salva l'agente SNMP, StorageGRID apre automaticamente le porte degli indirizzi dell'agente sul firewall interno. È necessario assicurarsi che eventuali firewall esterni consentano l'accesso a queste porte.

3. Seleziona **Crea**.

L'indirizzo dell'agente viene creato e aggiunto alla tabella.

Crea 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.



Le destinazioni SNMPv3 *inform* devono avere utenti con ID motore. La destinazione SNMPv3 *trap* non può avere utenti con ID motore.

Questi passaggi non sono validi se si utilizza solo SNMPv1 o SNMPv2c.

Passi

1. Seleziona **Crea**.
2. Inserisci le seguenti informazioni.

Campo	Descrizione
Nome utente	Un nome univoco per questo utente USM. I nomi utente possono contenere un massimo di 32 caratteri e non possono contenere spazi. Dopo la creazione dell'utente, non è possibile modificare il nome utente.
Accesso MIB di sola lettura	Se selezionata, l'utente avrà accesso in sola lettura al MIB.
ID motore autorevole	Se questo utente verrà utilizzato in una destinazione informata, l'ID motore autorevole per questo utente. Inserire da 10 a 64 caratteri esadecimali (da 5 a 32 byte) senza spazi. Questo valore è obbligatorio per gli utenti USM che verranno selezionati nelle destinazioni trap per le informazioni. Questo valore non è consentito per gli utenti USM che verranno selezionati nelle destinazioni delle trappole. Nota: questo campo non viene visualizzato se è stato selezionato Accesso MIB di sola lettura perché gli utenti USM con accesso MIB di sola lettura non possono avere ID motore.
Livello di sicurezza	Livello di sicurezza per l'utente USM: • authPriv: Questo utente comunica con autenticazione e privacy (crittografia). È necessario specificare un protocollo di autenticazione e una password, nonché un protocollo di privacy e una password. • authNoPriv: Questo utente comunica con autenticazione e senza privacy (nessuna crittografia). È necessario 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 questo utente utilizzerà per l'autenticazione.
Protocollo sulla privacy	Visualizzato solo se hai selezionato authPriv e impostato sempre su AES, che è l'unico protocollo di privacy supportato.
Password	Visualizzato solo se hai selezionato authPriv . La password che questo utente utilizzerà per la privacy.

3. Seleziona **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.

Aggiorna l'agente SNMP

È possibile disattivare le notifiche SNMP, aggiornare le stringhe della community oppure aggiungere o rimuovere indirizzi degli agenti, utenti USM e destinazioni trap.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .

Informazioni su questo compito

Vedere ["Configurare l'agente SNMP"](#) per i dettagli su ciascun campo nella pagina dell'agente SNMP. Per salvare le modifiche apportate in ogni scheda, è necessario selezionare **Salva** in fondo alla pagina.

Passi

1. Selezionare **CONFIGURAZIONE > Monitoraggio > Agente SNMP**.

Viene visualizzata la pagina dell'agente SNMP.

2. Per disabilitare l'agente SNMP su tutti i nodi della griglia, deselezionare la casella di controllo **Abilita SNMP** e selezionare **Salva**.

Se si riabilita l'agente SNMP, tutte le impostazioni di configurazione SNMP precedenti verranno mantenute.

3. Facoltativamente, aggiorna le informazioni nella sezione Configurazione di base:

- a. Se necessario, aggiornare **Contatto di sistema** e **Posizione di sistema**.
- b. Facoltativamente, selezionare o deselezionare la casella di controllo **Abilita notifiche agente SNMP** per controllare se l'agente SNMP StorageGRID invia notifiche trap e inform.

Se questa casella di controllo è deselezionata, l'agente SNMP supporta l'accesso MIB in 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 StorageGRID invia trap di autenticazione quando riceve messaggi di protocollo autenticati in modo non corretto.

4. Se si utilizza SNMPv1 o SNMPv2c, è possibile aggiornare o aggiungere una **community di sola lettura** nella sezione Stringhe della community.

5. Per aggiornare le destinazioni delle trappole, selezionare la scheda Destinazioni delle trappole nella sezione Altre configurazioni.

Utilizzare questa scheda per definire una o più destinazioni per le notifiche trap o informative StorageGRID . Quando si abilita l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Le notifiche standard vengono inviate anche per le entità MIB-II supportate (ad esempio, ifDown e coldStart).

Per i dettagli su cosa inserire, vedere ["Creare destinazioni trappola"](#) .

- Facoltativamente, aggiorna o rimuovi la community trap predefinita.

Se si rimuove la community trap predefinita, è necessario innanzitutto assicurarsi che tutte le destinazioni trap esistenti utilizzino una stringa community personalizzata.

- Per aggiungere una destinazione trap, selezionare **Crea**.

- Per modificare la destinazione di una trappola, selezionare il pulsante di opzione e selezionare **Modifica**.
- Per rimuovere una destinazione trap, selezionare il pulsante di opzione e scegliere **Rimuovi**.
- Per salvare le modifiche, seleziona **Salva** in fondo alla pagina.

6. Per aggiornare gli indirizzi degli agenti, selezionare la scheda Indirizzi degli agenti nella sezione Altre configurazioni.

Utilizzare questa scheda per specificare uno o più "indirizzi di ascolto". Questi sono gli indirizzi StorageGRID sui quali l'agente SNMP può ricevere query.

Per i dettagli su cosa inserire, vedere "[Crea indirizzi di agenti](#)".

- Per aggiungere l'indirizzo di un agente, seleziona **Crea**.
- Per modificare l'indirizzo di un agente, seleziona il pulsante di opzione e seleziona **Modifica**.
- Per rimuovere l'indirizzo di un agente, seleziona il pulsante di opzione e seleziona **Rimuovi**.
- Per salvare le modifiche, seleziona **Salva** in fondo alla 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 i dettagli su cosa inserire, vedere "[Crea utenti USM](#)".

- Per aggiungere un utente USM, seleziona **Crea**.
- Per modificare un utente USM, selezionare il pulsante di opzione e scegliere **Modifica**.

Il nome utente di un utente USM esistente non può essere modificato. Se devi cambiare un nome utente, devi rimuovere l'utente e crearne uno nuovo.



Se aggiungi o rimuovi l'ID motore autorevole di un utente e quell'utente è attualmente selezionato per una destinazione, devi 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 scegliere **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 salvare le modifiche, seleziona **Salva** in fondo alla pagina.

8. Dopo aver aggiornato la configurazione dell'agente SNMP, selezionare **Salva**.

Accedi 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 monitorare la tua rete.

Vedere ["Utilizzare il monitoraggio SNMP"](#) per ulteriori informazioni sui file SNMP e MIB.

Accedi ai file MIB

Per accedere ai file MIB, seguire questi passaggi.

Passi

- 1. Selezionare **CONFIGURAZIONE > Monitoraggio > Agente SNMP**.
- 2. Nella pagina dell'agente SNMP, seleziona il file che desideri 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 oggetti e notifiche per appliance basate su E-Series.
 - **MIB_1_10.zip**: definisce oggetti e notifiche per appliance con 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. Ottieni l'OID della radice 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 StorageGRID nell'intero albero (utilizzando `paste` per unire le linee):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



IL `snmptranslate` Il comando ha molte opzioni utili per esplorare il MIB. Questo comando è disponibile su qualsiasi nodo StorageGRID .

Contenuto del file MIB

Tutti gli oggetti sono sotto l'OID StorageGRID .

Nome dell'oggetto	ID oggetto (OID)	Descrizione
		Modulo MIB per entità NetApp StorageGRID .

oggetti MIB

Nome dell'oggetto	ID oggetto (OID)	Descrizione
activeAlertCount		Numero di avvisi attivi in activeAlertTable.
TabellaAvvisiAttivi		Una tabella degli avvisi attivi in StorageGRID.

Nome dell'oggetto	ID oggetto (OID)	Descrizione
activeAlertId		L'ID dell'avviso. Unico nel set attuale di avvisi attivi.
NomeAvvisoAttivo		Il nome dell'avviso.
activeAlertInstance		Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
activeAlertSeverity		La gravità dell'allerta.
activeAlertStartTime		Data e ora in cui è stato attivato l'avviso.

Tipi di notifica (Trappole)

Tutte le notifiche includono le seguenti variabili come varbind:

- activeAlertId
- NomeAvvisoAttivo
- activeAlertInstance
- activeAlertSeverity
- activeAlertStartTime

Tipo di notifica	ID oggetto (OID)	Descrizione
activeMinorAlert		Un avviso di gravità minore
activeMajorAlert		Un avviso di grave gravità
Avviso critico attivo		Un avviso con gravità critica

Raccogli dati StorageGRID aggiuntivi

Utilizzare diagrammi e grafici

È possibile utilizzare grafici e report per monitorare lo stato del sistema StorageGRID e risolvere i problemi.

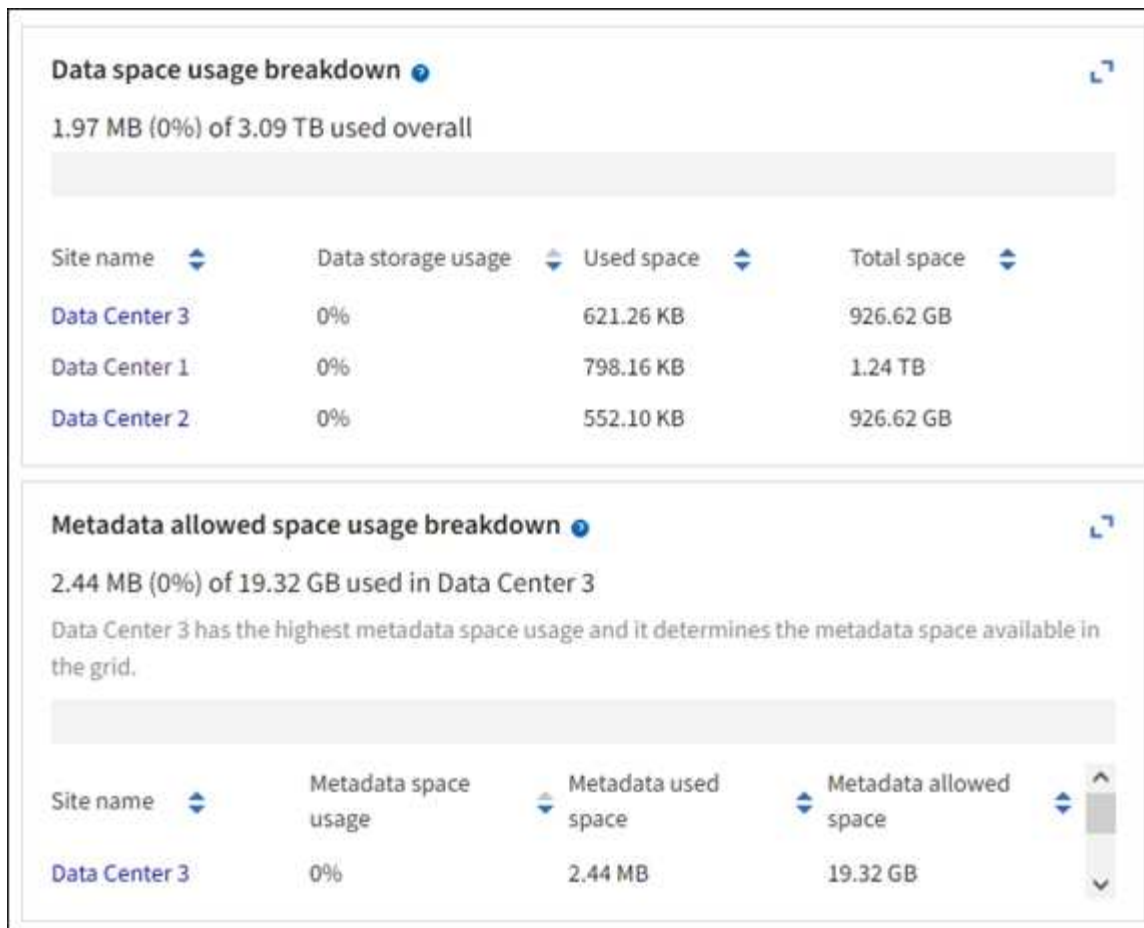


Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere agli screenshot di esempio presenti in questa pagina.

Tipi di grafici

I grafici e i diagrammi riepilogano i valori di specifiche metriche e attributi StorageGRID .

La dashboard di Grid Manager include schede che riepilogano lo spazio di archiviazione disponibile per la griglia e per ciascun sito.



Il pannello Utilizzo dello storage nella dashboard di Tenant Manager mostra quanto segue:

- Un elenco dei bucket (S3) o dei contenitori (Swift) più grandi per il tenant
- Un grafico a barre che rappresenta le dimensioni relative dei contenitori o dei bucket più grandi
- La quantità totale di spazio utilizzato e, se è impostata una quota, la quantità e la percentuale di spazio rimanente

Dashboard

16 Buckets
[View buckets](#)

2 Platform services
endpoints
[View endpoints](#)

0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage ?

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage ?

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details ?

Name: Tenant02

ID: 3341 1240 0546 8283 2208

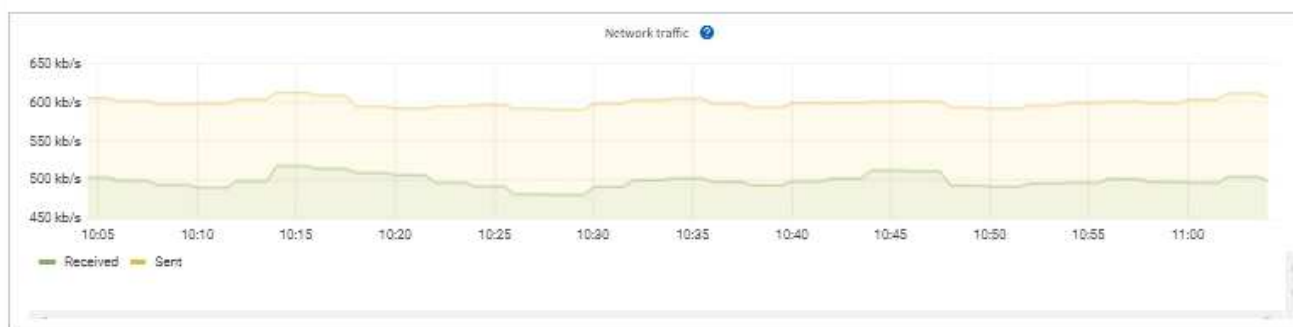
- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Inoltre, nella pagina Nodi e nella pagina **SUPPORTO > Strumenti > Topologia griglia** sono disponibili grafici che mostrano come le metriche e gli attributi StorageGRID cambiano nel tempo.

Esistono quattro tipi di grafici:

- **Grafici Grafana:** mostrati nella pagina Nodi, i grafici Grafana vengono utilizzati per tracciare i valori delle metriche di Prometheus nel tempo. Ad esempio, la scheda **NODI > Rete** per un nodo di archiviazione include un grafico Grafana per il traffico di rete.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

Name ⓘ ↕	Hardware address ⓘ ↕	Speed ⓘ	Duplex ⓘ ↕	Auto-negotiation ⓘ ↕	Link status ⓘ ↕
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface ⓘ ↕	Data ⓘ ↕	Packets ⓘ ↕	Errors ⓘ ↕	Dropped ⓘ ↕	Frame overruns ⓘ ↕	Frames ⓘ ↕
eth0	3.04 GB ⓘ	20,403,428 ⓘ	0 ⓘ	24,899 ⓘ	0 ⓘ	0 ⓘ

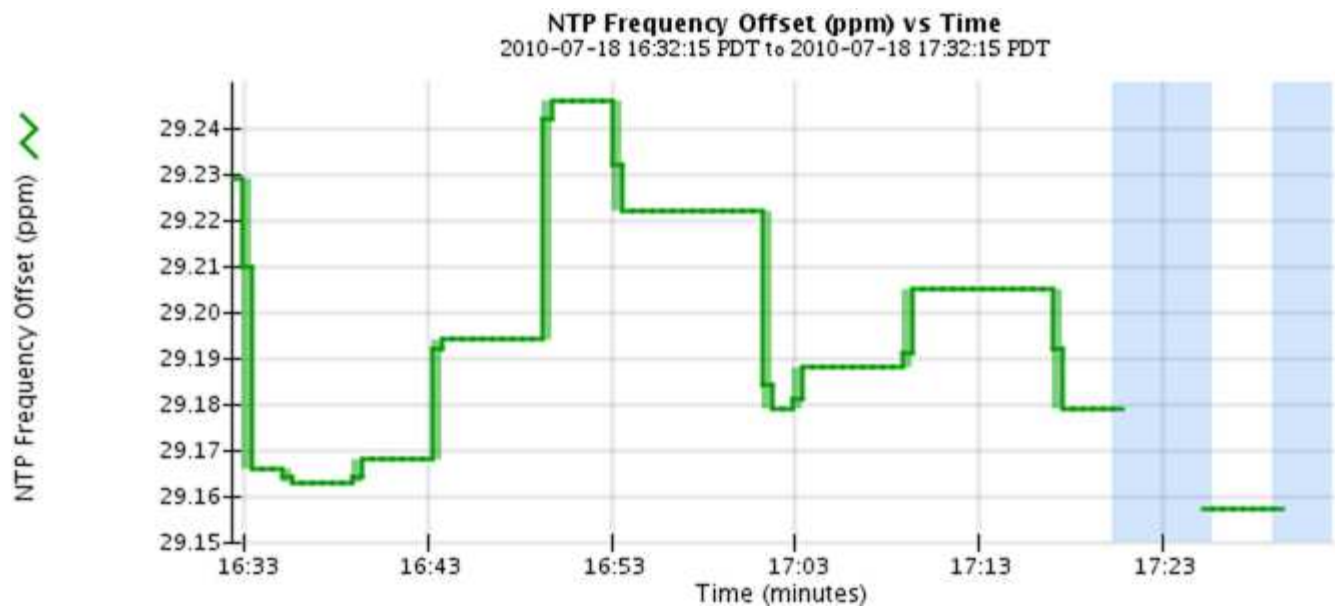
Transmit

Interface ⓘ ↕	Data ⓘ ↕	Packets ⓘ ↕	Errors ⓘ ↕	Dropped ⓘ ↕	Collisions ⓘ ↕	Carrier ⓘ ↕
eth0	3.65 GB ⓘ	19,061,947 ⓘ	0 ⓘ	0 ⓘ	0 ⓘ	0 ⓘ

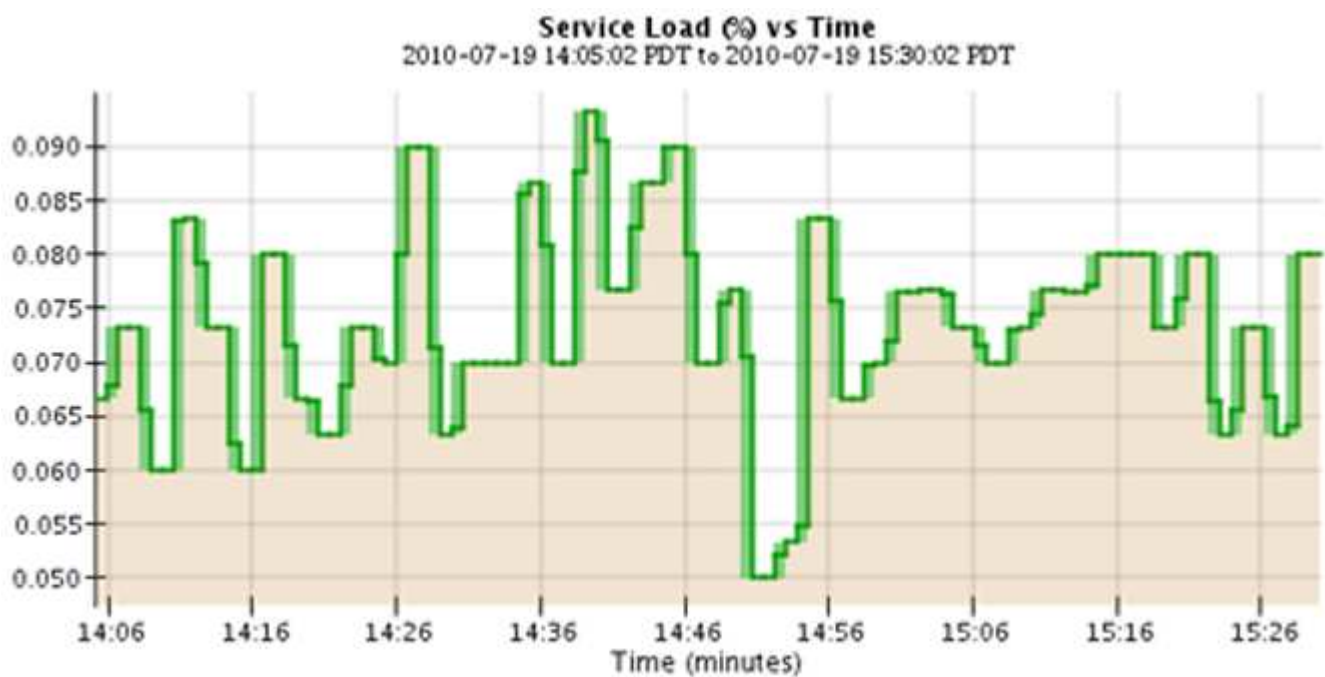


I grafici Grafana sono inclusi anche nei dashboard predefiniti disponibili nella pagina **SUPPORTO > Strumenti > Metriche**.

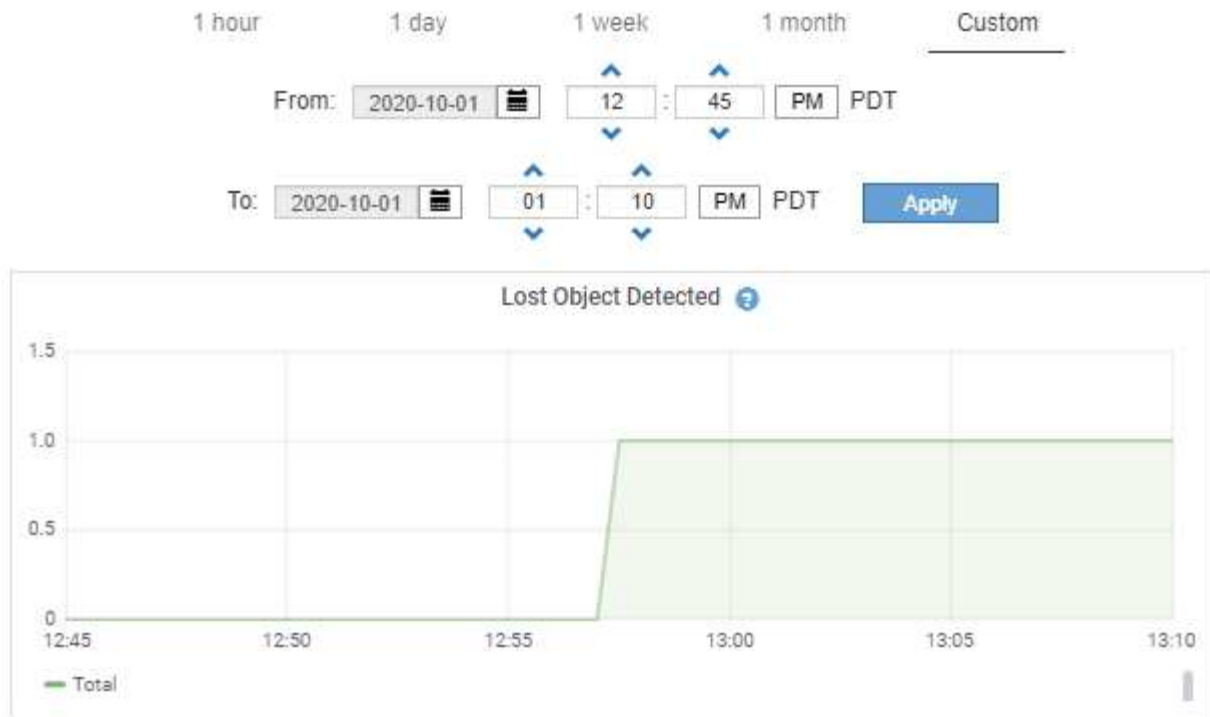
- **Grafici lineari:** disponibili dalla pagina Nodi e dalla pagina **SUPPORTO > Strumenti > Topologia griglia** (selezionare l'icona del grafico ⓘ dopo un valore di dati), i grafici lineari vengono utilizzati per tracciare i valori degli attributi StorageGRID che hanno un valore unitario (ad esempio l'offset di frequenza NTP, in ppm). Le variazioni del valore vengono rappresentate graficamente in intervalli di dati regolari (bin) nel tempo.



- **Grafici ad area:** disponibili dalla pagina Nodi e dalla pagina **SUPPORTO > Strumenti > Topologia griglia** (selezionare l'icona del grafico  dopo un valore di dati), i grafici ad area vengono utilizzati per tracciare quantità di attributi volumetrici, come conteggi di oggetti o valori di carico del servizio. I grafici ad area sono simili ai grafici a linee, ma presentano una leggera ombreggiatura marrone sotto la linea. Le variazioni del valore vengono rappresentate graficamente in intervalli di dati regolari (bin) nel tempo.

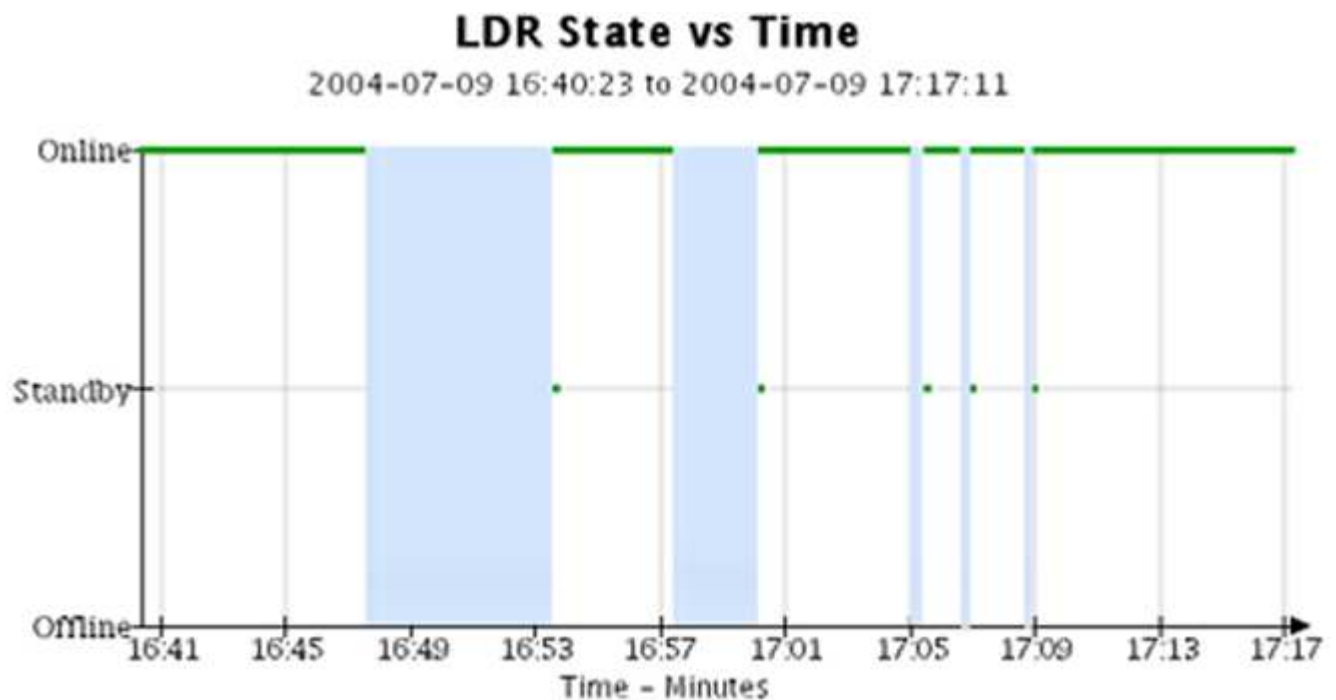


- Alcuni grafici sono contrassegnati da un diverso tipo di icona del grafico  e hanno un formato diverso:



[Close](#)

- **Grafico di stato:** disponibile dalla pagina **SUPPORTO > Strumenti > Topologia griglia** (selezionare l'icona del grafico  dopo un valore di dati), i grafici di stato vengono utilizzati per tracciare i valori degli attributi che rappresentano stati distinti, ad esempio uno stato di servizio che può essere online, in standby o offline. I grafici di stato sono simili ai grafici lineari, ma la transizione è discontinua, ovvero il valore salta da un valore di stato a un altro.



Informazioni correlate

- ["Visualizza la pagina Nodi"](#)
- ["Visualizza l'albero della topologia della griglia"](#)
- ["Esaminare le metriche di supporto"](#)

Legenda del grafico

Le linee e i colori utilizzati per disegnare i grafici hanno un significato specifico.

Esempio	Senso
	I valori degli attributi segnalati vengono tracciati utilizzando linee verde scuro.
	L'ombreggiatura verde chiaro attorno alle linee verde scuro indica che i valori effettivi in quell'intervallo di tempo variano e sono stati "classificati" per una rappresentazione grafica più rapida. La linea scura rappresenta la media ponderata. L'intervallo in verde chiaro indica i valori massimo e minimo all'interno del contenitore. Nei grafici ad area viene utilizzata l'ombreggiatura marrone chiaro per indicare i dati volumetrici.
	Le aree vuote (nessun dato tracciato) 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 azzurra chiara indica che alcuni o tutti i valori degli attributi in quel momento erano indeterminati; l'attributo non segnalava valori perché il servizio era in uno stato sconosciuto.
	L'ombreggiatura grigia indica che alcuni o tutti i valori degli attributi in quel momento non erano noti perché il servizio che segnalava gli attributi era amministrativamente inattivo.
	Una combinazione di ombreggiature grigie e blu indica che alcuni valori degli attributi in quel momento erano indeterminati (perché il servizio era in uno stato sconosciuto), mentre altri non erano noti perché il servizio che segnalava gli attributi era amministrativamente inattivo.

Visualizzare grafici e diagrammi

La pagina Nodi contiene i grafici e i diagrammi a cui dovresti accedere regolarmente per monitorare attributi quali capacità di archiviazione e produttività. In alcuni casi, soprattutto quando si lavora con l'assistenza tecnica, è possibile utilizzare la pagina **SUPPORTO > Strumenti > Topologia griglia** per accedere a grafici aggiuntivi.

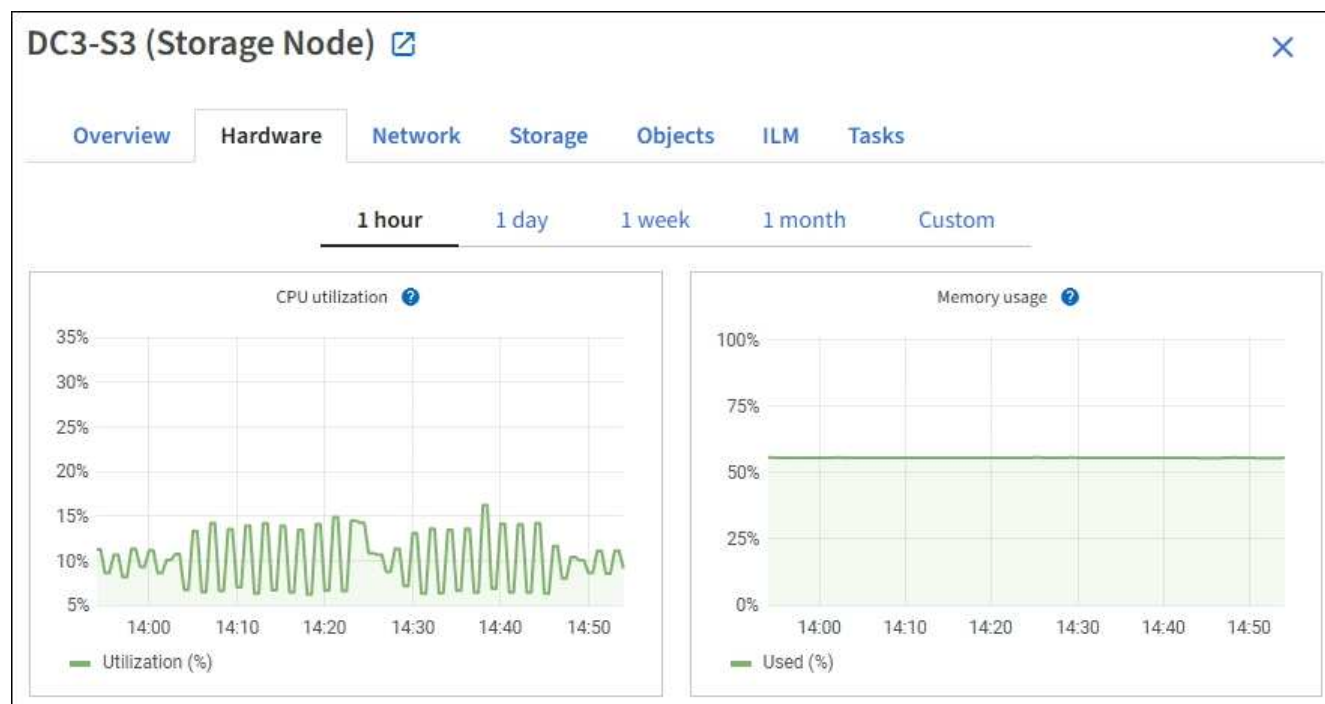
Prima di iniziare

Devi aver effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

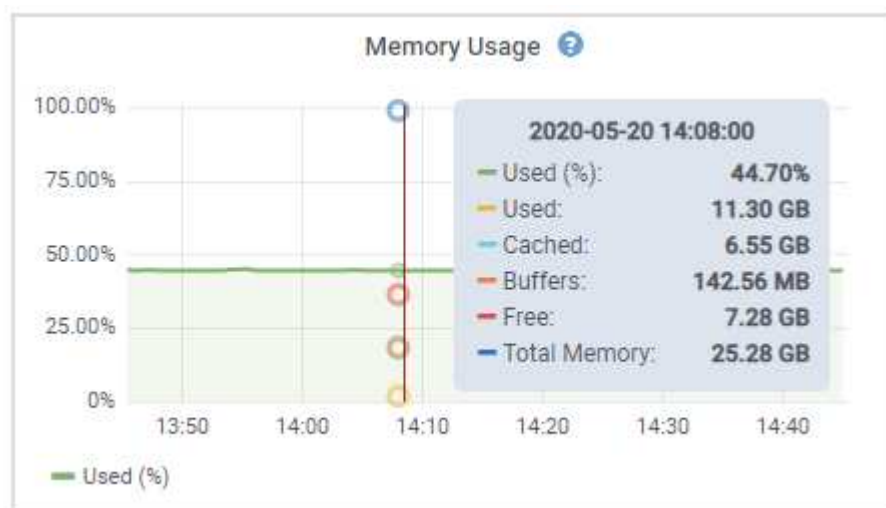
Passi

1. Selezionare **NODES**. Quindi, seleziona un nodo, un sito o l'intera griglia.
2. Seleziona la scheda di cui desideri visualizzare le informazioni.

Alcune schede includono uno o più grafici Grafana, utilizzati per tracciare i valori delle metriche di Prometheus nel tempo. Ad esempio, la scheda **NODI > Hardware** per un nodo include due grafici Grafana.



3. Facoltativamente, posiziona il cursore sul grafico per visualizzare valori più dettagliati per un determinato momento.



4. A seconda delle necessità, spesso è possibile visualizzare un grafico per un attributo o una metrica specifici. Dalla tabella nella pagina Nodi, seleziona l'icona del grafico  a destra del nome dell'attributo.

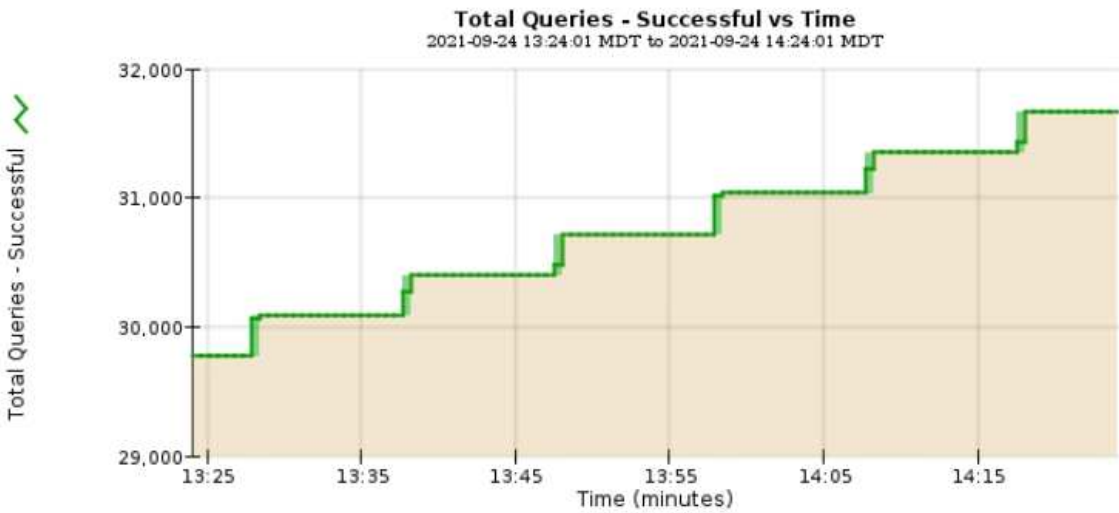


I grafici non sono disponibili per tutte le metriche e tutti gli attributi.

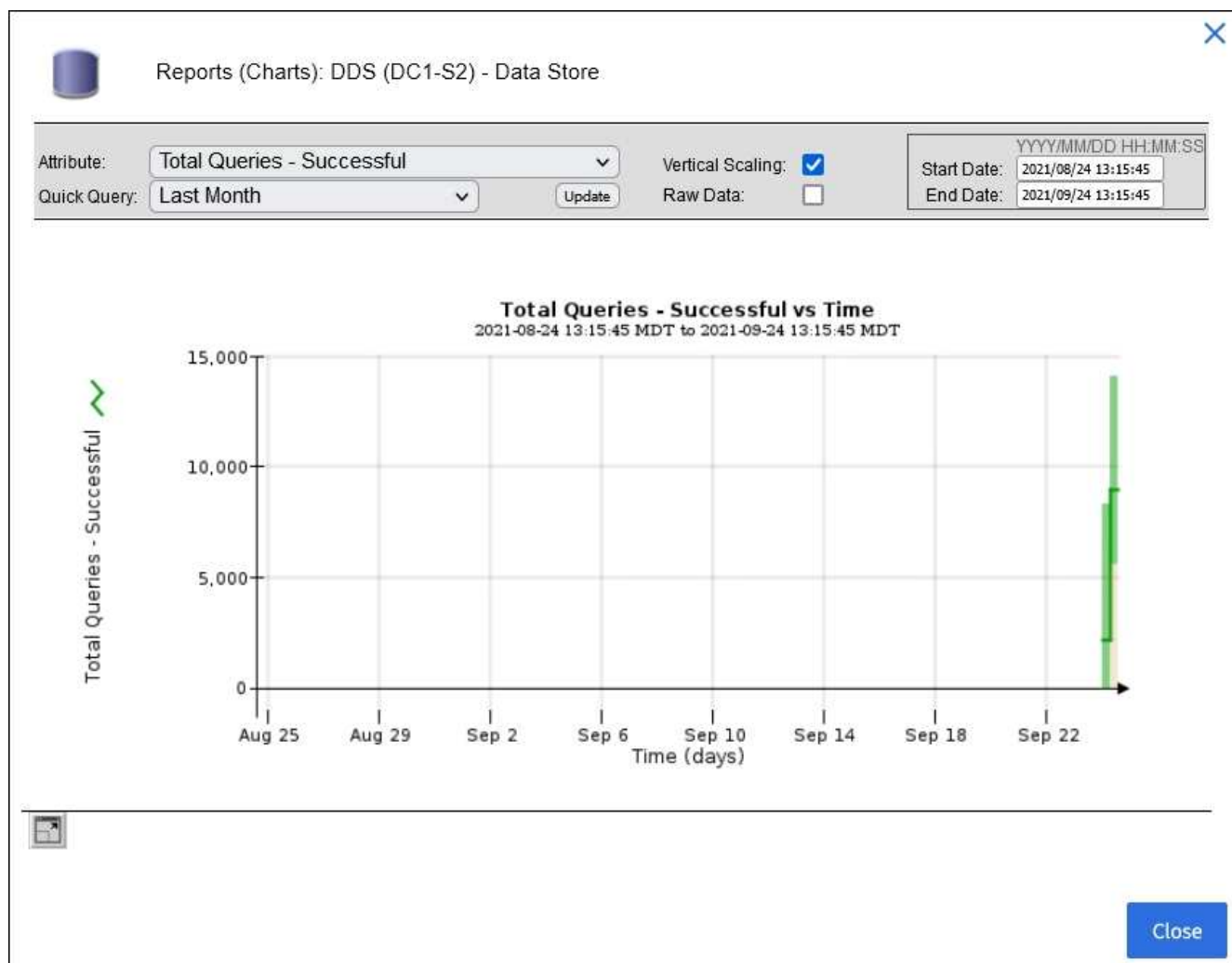
Esempio 1: dalla scheda Oggetti per un nodo di archiviazione, è possibile selezionare l'icona del grafico  per visualizzare il numero totale di query di archiviazione metadati riuscite per il nodo di archiviazione.



Attribute:	Total Queries - Successful	Vertical Scaling:	☒	Start Date:	2021/09/24 13:24:01
Quick Query:	Last Hour	Raw Data:	☐	End Date:	2021/09/24 14:24:01



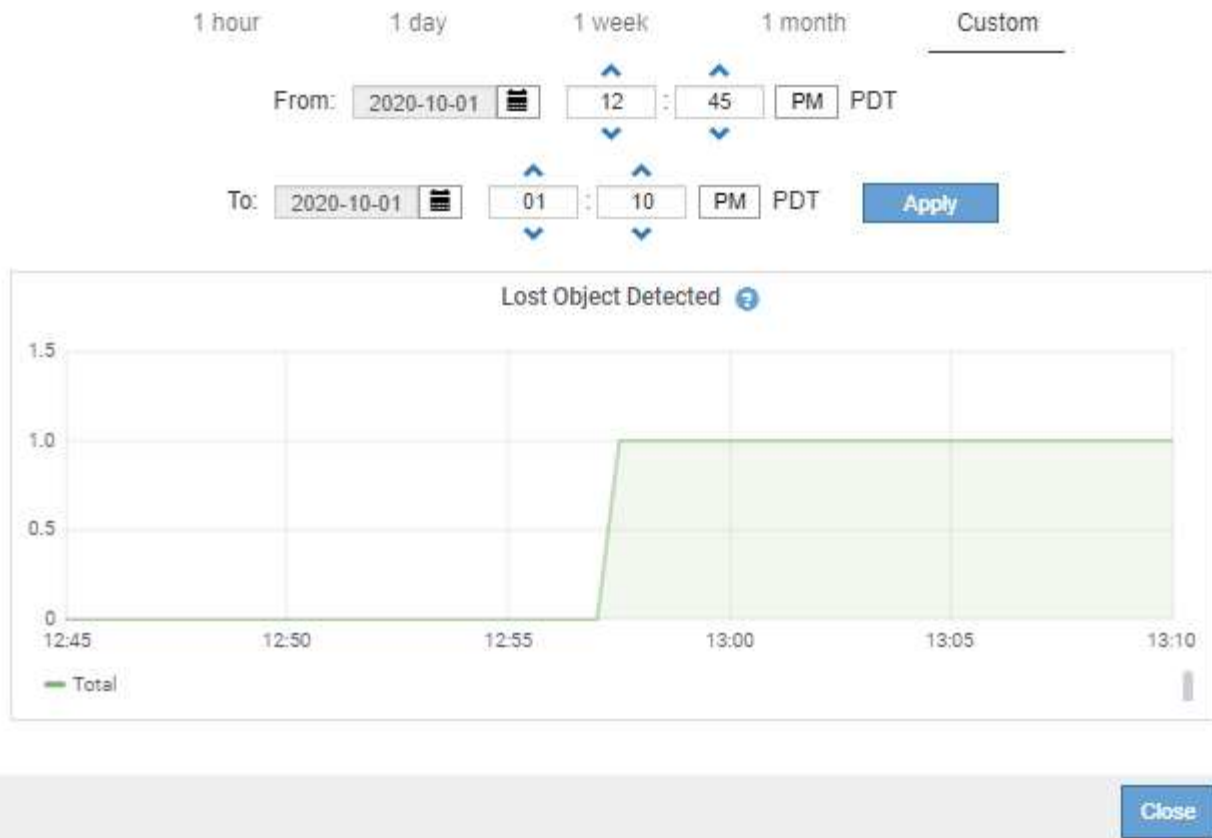
Close



Esempio 2: Dalla scheda Oggetti per un nodo di archiviazione, è possibile selezionare l'icona del grafico  per vedere il grafico Grafana del conteggio degli oggetti persi rilevati nel tempo.

Object Counts	
Total Objects	1
Lost Objects	1
S3 Buckets and Swift Containers	1





5. Per visualizzare i grafici per gli attributi non mostrati nella pagina Nodo, selezionare **SUPPORTO > Strumenti > Topologia griglia**.
6. Selezionare **nodo griglia > componente o servizio > Panoramica > Principale**.

Overview

Alarms

Reports

Configuration

Main



Overview: SSM (DC1-ADM1) - Resources

Updated: 2018-05-07 16:29:52 MDT

Computational Resources

Service Restarts:	1	
Service Runtime:	6 days	
Service Uptime:	6 days	
Service CPU Seconds:	10666 s	
Service Load:	0.266 %	

Memory

Installed Memory:	8.38 GB	
Available Memory:	2.9 GB	

Processors

Processor Number	Vendor	Type	Cache
1	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
2	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
3	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
4	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
5	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
6	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
7	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
8	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB

7. Seleziona l'icona del grafico  accanto all'attributo.

La visualizzazione passa automaticamente alla pagina **Report > Grafici**. Il grafico mostra i dati dell'attributo nel giorno precedente.

Genera grafici

I grafici mostrano una rappresentazione grafica dei valori dei dati degli attributi. È possibile creare report su un sito di data center, un nodo di griglia, un componente o un servizio.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai "[autorizzazioni di accesso specifiche](#)".

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **nodo griglia > componente o servizio > Report > Grafici**.
3. Selezionare l'attributo da segnalare dall'elenco a discesa **Attributo**.
4. Per forzare l'asse Y a partire da zero, deselezionare la casella di controllo **Scala verticale**.
5. Per visualizzare i valori con la massima precisione, selezionare la casella di controllo **Dati grezzi** 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 grezzi**.

6. Selezionare il periodo di tempo su cui effettuare il report dall'elenco a discesa **Query rapida**.

Selezionare l'opzione Query personalizzata per selezionare un intervallo di tempo specifico.

Il grafico appare dopo qualche istante. Per la tabulazione di intervalli di tempo lunghi, attendere alcuni minuti.

7. Se hai selezionato Query personalizzata, personalizza il periodo di tempo per il grafico inserendo **Data di inizio** e **Data di fine**.

Utilizzare il formato `YYYY/MM/DDHH:MM:SS` nell'ora locale. Per rispettare il formato è necessario utilizzare gli zeri iniziali. 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 pochi secondi viene generato un grafico. Per la tabulazione di intervalli di tempo lunghi, attendere alcuni minuti. A seconda della durata impostata per la query, viene visualizzato un report di testo grezzo o un report di testo aggregato.

Utilizzare report di testo

I report di testo mostrano una rappresentazione testuale dei valori dei dati degli attributi elaborati dal servizio NMS. A seconda del periodo di tempo su cui si sta effettuando il report, vengono generati due tipi di report: report di testo grezzo per periodi inferiori a una settimana e report di testo aggregato per periodi superiori a una settimana.

Rapporti di testo grezzo

Un report di testo grezzo visualizza i dettagli sull'attributo selezionato:

- Ora di ricezione: data e ora locali in cui un valore campione dei dati di un attributo è stato elaborato dal servizio NMS.
- Ora di campionamento: data e ora locali in cui un valore di attributo è stato campionato o modificato all'origine.
- 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 %

Rapporti di testo aggregati

Un report di testo aggregato visualizza i dati per un periodo di tempo più lungo (solitamente una settimana) rispetto a un report di testo grezzo. Ogni voce è il risultato della sintesi di più valori di attributi (un aggregato di valori di attributi) da parte del servizio NMS nel tempo in un'unica voce con valori medi, massimi e minimi derivati dall'aggregazione.

Ogni voce visualizza le seguenti informazioni:

- Ora aggregata: ultima data e ora locale in cui il servizio NMS ha aggregato (raccolto) un set di valori di attributi modificati.
- Valore medio: la media del valore dell'attributo nel periodo di tempo aggregato.
- Valore minimo: il valore minimo nel periodo di tempo aggregato.
- 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

Genera report di testo

I report di testo mostrano una rappresentazione testuale dei valori dei dati degli attributi elaborati dal servizio NMS. È possibile creare report su un sito di data center, un nodo di griglia, un componente o un servizio.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai "[autorizzazioni di accesso specifiche](#)".

Informazioni su questo compito

Per i dati degli attributi che si prevede cambino continuamente, questi dati vengono campionati dal servizio NMS (alla fonte) a intervalli regolari. Per i dati degli attributi che cambiano raramente (ad esempio, dati basati su eventi quali cambiamenti di stato o di stato), un valore dell'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 era amministrativamente inattivo durante il periodo in cui è stato effettuato il campionamento. Il testo blu indica che il servizio era in uno stato sconosciuto.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **nodo griglia > componente o servizio > 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 grezzi**.
6. Selezionare il periodo di tempo su cui effettuare il report dall'elenco a discesa **Query rapida**.

Selezionare l'opzione Query personalizzata per selezionare un intervallo di tempo specifico.

Il rapporto appare dopo qualche istante. Per la tabulazione di intervalli di tempo lunghi, attendere alcuni

minuti.

- Se hai selezionato Query personalizzata, devi personalizzare il periodo di tempo su cui effettuare il report inserendo la **Data di inizio** e la **Data di fine**.

Utilizzare il formato YYYY/MM/DDHH:MM:SS nell'ora locale. Per rispettare il formato è necessario utilizzare gli zeri iniziali. Ad esempio, 2017/4/6 7:30:00 non supera la convalida. Il formato corretto è: 2017/04/06 07:30:00.

- Fare clic su **Aggiorna**.

Dopo qualche istante viene generato un report di testo. Per la tabulazione di intervalli di tempo lunghi, attendere alcuni minuti. A seconda della durata impostata per la query, viene visualizzato un report di testo grezzo o un report di testo aggregato.

Esporta report di testo

I report di testo esportati aprono una nuova scheda del browser, che consente di selezionare e copiare i dati.

Informazioni su questo compito

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 .

Passi

- Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
- Crea un report di testo.
- Fare clic su *Esporta*.

OverviewAlarmsReportsConfiguration

ChartsText

 **Reports (Text): SSM (170-176) - Events**

Attribute: Attribute Send to Relay RateQuick Query: Custom QueryUpdate

Results Per Page: 5Raw Data: ☒

YYYY/MM/DD HH:MM:SSStart Date: 2010/07/19 08:42:09End Date: 2010/07/20 08:42:09

Text Results for Attribute Send to Relay Rate
2010-07-19 08:42:09 PDT To 2010-07-20 08:42:09 PDT

1 - 5 of 254

Time Received	Sample Time	Value
2010-07-20 08:40:46	2010-07-20 08:40:46	0.274981485 Messages/s
2010-07-20 08:38:46	2010-07-20 08:38:46	0.274989 Messages/s
2010-07-20 08:36:46	2010-07-20 08:36:46	0.283317543 Messages/s
2010-07-20 08:34:46	2010-07-20 08:34:46	0.274982493 Messages/s
2010-07-20 08:32:46	2010-07-20 08:32:46	0.291646426 Messages/s

Previous « 1 2 3 4 5 » Next

Si apre la finestra Esporta report di testo che visualizza il report.

Grid ID: 000 000
 OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
 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 le prestazioni PUT e GET

È possibile monitorare le prestazioni di determinate operazioni, come l'archiviazione e il recupero di oggetti, per identificare modifiche che potrebbero richiedere ulteriori indagini.

Informazioni su questo compito

Per monitorare le prestazioni PUT e GET, è possibile eseguire i comandi S3 direttamente da una workstation oppure utilizzando l'applicazione open source S3tester. Utilizzando questi metodi è possibile valutare le prestazioni indipendentemente da fattori esterni a StorageGRID, come problemi con un'applicazione client o problemi con una rete esterna.

Quando si eseguono test sulle operazioni PUT e GET, attenersi alle seguenti linee guida:

- Utilizza dimensioni degli oggetti paragonabili a quelle degli oggetti che solitamente inserisci nella tua griglia.
- Eseguire operazioni sia su siti locali che remoti.

Messaggi nel "[registro di controllo](#)" indicano 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 controllo SGET. È inoltre possibile trovare l'attributo TIME nei messaggi di controllo per le seguenti operazioni S3: DELETE, GET, HEAD, Metadati aggiornati, POST, PUT

Quando si analizzano i risultati, bisogna considerare il tempo medio necessario per soddisfare una richiesta, nonché la produttività complessiva che è possibile ottenere. Ripeti regolarmente gli stessi test e registra i risultati, in modo da poter identificare le tendenze che potrebbero richiedere indagini.

- Puoi "[scarica S3tester da github](#)".

Monitorare le operazioni di verifica degli oggetti

Il sistema StorageGRID può verificare l'integrità dei dati degli oggetti sui nodi di archiviazione, controllando sia gli oggetti danneggiati che quelli mancanti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#) .

Informazioni su questo compito

Due ["processi di verifica"](#) collaborare per garantire l'integrità dei dati:

- **La verifica degli sfondi** viene eseguita automaticamente, verificando costantemente la correttezza dei dati dell'oggetto.

La verifica in background controlla automaticamente e costantemente tutti i nodi di archiviazione per determinare se sono presenti copie danneggiate di dati di oggetti replicati e codificati per la cancellazione. Se vengono rilevati problemi, il sistema StorageGRID tenta automaticamente di sostituire i dati degli oggetti danneggiati dalle copie archiviate altrove nel sistema. La verifica in background non viene eseguita sugli oggetti in un Cloud Storage Pool.



L'avviso **Oggetto danneggiato non identificato rilevato** viene attivato se il sistema rileva un oggetto danneggiato che non può essere corretto automaticamente.

- **Il controllo dell'esistenza dell'oggetto** 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 dell'oggetto verifica se tutte le copie replicate previste degli oggetti e dei frammenti con codice di cancellazione sono presenti su un nodo di archiviazione. Il controllo dell'esistenza degli oggetti consente di verificare l'integrità dei dispositivi di archiviazione, soprattutto se un recente problema hardware potrebbe aver influito sull'integrità dei dati.

Dovresti rivedere regolarmente i risultati delle verifiche dei precedenti e dei controlli dell'esistenza degli oggetti. Indagare immediatamente su eventuali casi di dati di oggetti danneggiati o mancanti per determinarne la causa principale.

Passi

1. Esaminare i risultati delle verifiche dei precedenti:
 - a. Selezionare **NODI > Nodo di archiviazione > Oggetti**.
 - b. Controlla i risultati della verifica:
 - Per verificare la verifica dei dati degli oggetti replicati, consultare gli attributi nella sezione Verifica.

Verification		
Status: ?	No errors	
Percent complete: ?	0.00%	
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	

- Per verificare la verifica dei frammenti con codice di cancellazione, selezionare **Storage Node > ILM** e osservare gli attributi nella sezione Verifica del codice di cancellazione.

Erasure coding verification		
Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Seleziona il punto interrogativo ? accanto al nome di un attributo per visualizzare il testo della guida.

- Esaminare i risultati dei processi di controllo dell'esistenza degli oggetti:
 - Selezionare **MANUTENZIONE > Controllo esistenza oggetto > Cronologia lavori**.
 - Esaminare la colonna Copie di oggetti mancanti rilevate. Se durante un processo mancano 100 o più copie di oggetti e viene attivato l'avviso **Oggetti persi**, contattare l'assistenza tecnica.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job

Job history

Delete

Search...

☐

Job ID ?

Status ?

Nodes (volumes) ?

Missing object copies detected ?

☐

15816859223101303015

Completed

DC2-S1 (3 volumes)

0

☐

12538643155010477372

Completed

DC1-S3 (1 volume)

0

☐

5490044849774982476

Completed

DC1-S2 (1 volume)

0

☐

3395284277055907678

Completed

DC1-S1 (3 volumes)
DC1-S2 (3 volumes)
DC1-S3 (3 volumes)
and 7 more

0

Monitorare gli eventi

È possibile monitorare gli eventi rilevati da un nodo della griglia, inclusi gli eventi personalizzati creati per tenere traccia degli eventi registrati sul server syslog. Il messaggio Ultimo evento visualizzato in Grid Manager fornisce maggiori informazioni sull'evento più recente.

I messaggi di evento sono elencati anche in `/var/local/log/bycast-err.log` file di registro. Vedi [il "Riferimento ai file di registro"](#).

L'allarme SMTT (eventi totali) può essere attivato ripetutamente da problemi quali problemi di rete, interruzioni di corrente o aggiornamenti. Questa sezione contiene informazioni su come indagare sugli 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 reimpostare i contatori degli eventi.

Passi

- Esaminare gli eventi di sistema per ciascun nodo della griglia:
 - Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - Seleziona **site > grid node > SSM > Eventi > Panoramica > Principale**.
- Genera un elenco di messaggi di eventi precedenti per aiutare a isolare i problemi verificatisi in passato:

- Selezionare **SUPPORTO > Strumenti > Topologia griglia.**
- Selezionare **site > grid node > SSM > Eventi > Report.**
- Seleziona **Testo.**

L'attributo **Ultimo evento** non viene visualizzato in "visualizzazione dei grafici". Per visualizzarlo:

- Cambia **Attributo** in **Ultimo evento.**
- Facoltativamente, seleziona un periodo di tempo per **Query rapida.**
- Selezionare **Aggiorna.**

Reports (Text): SSM (170-41) - Events

Attribute: Results Per Page: Start Date: End Date:

Quick Query: Raw Data: ☒

Text Results for Last Event
2009-04-15 15:19:53 PDT To 2009-04-15 15:24:53 PDT

1 - 2 of 2

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

Crea eventi syslog personalizzati

Gli eventi personalizzati consentono di tenere traccia di tutti gli eventi utente di livello kernel, daemon, errore e critico registrati sul server syslog. Un evento personalizzato può essere utile per monitorare il verificarsi di messaggi di registro di sistema (e quindi eventi di sicurezza di rete e guasti hardware).

Informazioni su questo compito

Prendi in considerazione la creazione di eventi personalizzati per monitorare i problemi ricorrenti. Le seguenti considerazioni si applicano agli eventi personalizzati.

- Dopo aver creato un evento personalizzato, ogni sua occorrenza viene monitorata.
- Per creare un evento personalizzato basato sulle parole chiave nel `/var/local/log/messages` file, i registri in quei file devono essere:
 - Generato dal kernel
 - Generato dal demone o dal programma utente a livello di errore o critico

Nota: Non tutte le voci nel `/var/local/log/messages` i file verranno abbinati a meno che non soddisfino i requisiti sopra indicati.

Passi

- Selezionare **SUPPORTO > Allarmi (legacy) > Eventi personalizzati.**
- Fai clic su ***Modifica*** (o ***Inserisci*** se questo non è il primo evento).

3. Inserisci una stringa di evento personalizzata, ad esempio, arresto

Events
Updated: 2021-10-22 11:15:34 MDT

Custom Events (1 - 1 of 1)

Event	Actions
shutdown	

Show 10 Records Per Page Refresh Previous 1 Next

Apply Changes

4. Selezionare **Applica modifiche**.

5. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.

6. Selezionare **nodo griglia > SSM > Eventi**.

7. Individuare la voce Eventi personalizzati nella tabella Eventi e monitorare il valore per **Conteggio**.

Se il conteggio aumenta, significa che su quel nodo della griglia viene attivato un evento personalizzato che stai monitorando.

Overview
Alarms
Reports
Configuration

Main



Overview: SSM (DC1-ADM1) - Events
Updated: 2021-10-22 11:19:18 MDT

System Events

Log Monitor State: Connected
Total Events: 0
Last Event: No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Errors	0
Cassandra Heap Out Of Memory Errors	0
Chunk Service Events	0
Custom Events	0
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	0
Grid Node Errors	0
Hotfix Installation Failure Events	0
I/O Errors	0
IDE Errors	0
Identity Service Events	0
Kernel Errors	0
Kernel Memory Allocation Failure	0
Keystone Service Events	0
Network Receive Errors	0
Network Transmit Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0

Reimposta a zero il conteggio degli eventi personalizzati

Se si desidera reimpostare il contatore solo per gli eventi personalizzati, è necessario utilizzare la pagina Topologia griglia nel menu Supporto.

L'azzeramento di un contatore fa sì che l'allarme venga attivato dall'evento successivo. Al contrario, quando si riconosce un allarme, l'allarme viene riattivato solo se viene raggiunto il livello di soglia successivo.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **grid node > SSM > Eventi > Configurazione > Principale**.
3. Selezionare la casella di controllo **Reimposta** per Eventi personalizzati.

Overview

Alarms

Reports

Configuration

Main

Alarms



Configuration: SSM (DC2-ADM1) - Events

Updated: 2018-04-11 10:35:44 MDT

Description	Count	Reset
Abnormal Software Events	0	☐
Account Service Events	0	☐
Cassandra Errors	0	☐
Cassandra Heap Out Of Memory Errors	0	☐
Custom Events	0	☒
File System Errors	0	☐
Forced Termination Events	0	☐

4. Selezionare **Applica modifiche**.

Rivedi i messaggi di audit

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

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

- I messaggi di controllo del sistema sono correlati al sistema di controllo 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 controllo dell'archiviazione degli oggetti sono correlati all'archiviazione e alla gestione degli oggetti all'interno StorageGRID, inclusi l'archiviazione e il recupero degli oggetti, i trasferimenti da un nodo della griglia all'altro e le verifiche.
- I messaggi di controllo di lettura e scrittura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per creare, modificare o recuperare un oggetto.
- I messaggi di controllo di gestione registrano le richieste degli utenti nell'API di gestione.

Ogni nodo amministrativo memorizza i messaggi di audit in file di testo. La condivisione di controllo contiene il file attivo (audit.log) e i registri di controllo compressi dei giorni precedenti. Ogni nodo della griglia memorizza anche una copia delle informazioni di audit generate sul nodo.

È possibile accedere ai file di registro di controllo direttamente dalla riga di comando del nodo di amministrazione.

StorageGRID può inviare informazioni di audit per impostazione predefinita, ma è possibile modificare la destinazione:

- StorageGRID utilizza per impostazione predefinita le destinazioni di controllo dei nodi locali.

- Le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di archiviazione.
- Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati quando viene configurato un server syslog esterno.
- ["Scopri come configurare i messaggi di controllo e le destinazioni dei log"](#) .

Per i dettagli sul file di registro di controllo, il formato dei messaggi di controllo, i tipi di messaggi di controllo e gli strumenti disponibili per analizzare i messaggi di controllo, vedere ["Esaminare i registri di controllo"](#) .

Raccogli file di registro e dati di sistema

È possibile utilizzare Grid Manager per recuperare file di registro e dati di sistema (inclusi i dati di configurazione) per il sistema StorageGRID .

Prima di iniziare

- È necessario aver effettuato l'accesso a Grid Manager sul nodo di amministrazione primario utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- È necessario disporre della passphrase di provisioning.

Informazioni su questo compito

Puoi usare Grid Manager per raccogliere ["file di registro"](#) , 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 puoi poi scaricare sul tuo computer locale.

Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati quando viene configurato un server syslog esterno. Vedere ["Configurare i messaggi di controllo e le destinazioni dei registri"](#) .

Passi

1. Selezionare **SUPPORTO > Strumenti > Registri**.

2. Selezionare i nodi della griglia per i quali si desidera raccogliere i file di registro.

A seconda delle necessità, è possibile raccogliere file di registro per l'intera griglia o per un intero sito di data center.

3. Selezionare un'**Ora di inizio** e un'**Ora di fine** per impostare l'intervallo di tempo dei dati da includere nei file di registro.

Se si seleziona un periodo di tempo molto lungo o si raccolgono i log da tutti i nodi in una griglia di grandi dimensioni, l'archivio dei log potrebbe diventare troppo grande per essere archiviato su un nodo o troppo grande per essere raccolto nel nodo di amministrazione primario per il download. In tal caso, è necessario riavviare la raccolta dei registri con un set di dati più piccolo.

4. Seleziona i tipi di log che vuoi 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 delle applicazioni disponibili.
- **Registri di controllo:** registri contenenti i messaggi di controllo generati durante il normale funzionamento del sistema.
- **Traccia di rete:** registri utilizzati per il debug di rete.
- **Database Prometheus:** Metriche delle serie temporali dai servizi su tutti i nodi.

5. Facoltativamente, inserisci delle note sui file di registro che stai raccogliendo nella casella di testo **Note**.

È possibile utilizzare queste note per fornire al supporto tecnico informazioni sul problema che ha spinto a raccogliere i file di registro. Le tue note vengono aggiunte a un file denominato `info.txt`, insieme ad

altre informazioni sulla raccolta dei file di registro. IL `info.txt` il file viene salvato nel pacchetto di archivio dei file di registro.

6. Immettere la passphrase di provisioning per il sistema StorageGRID nella casella di testo **Passphrase di provisioning**.

7. Seleziona **Raccogli registri**.

Quando si invia una nuova richiesta, la precedente raccolta di file di registro viene eliminata.

È possibile utilizzare la pagina Registri per monitorare l'avanzamento della raccolta dei file di registro per ciascun nodo della griglia.

Se ricevi un messaggio di errore relativo alle dimensioni del registro, prova a raccogliere i registri per un periodo di tempo più breve o per un numero inferiore di nodi.

8. Selezionare **Scarica** una volta completata la raccolta dei file di registro.

Il file `.tar.gz` contiene tutti i file di registro di tutti i nodi della griglia in cui la raccolta dei registri è riuscita. All'interno del file `.tar.gz` combinato, è presente un archivio di file di registro per ciascun nodo della griglia.

Dopo aver finito

Se necessario, puoi scaricare nuovamente il pacchetto di archiviazione del file di registro in un secondo momento.

Facoltativamente, è possibile selezionare **Elimina** per rimuovere il pacchetto di archivio del file di registro e liberare spazio su disco. Il pacchetto di archivio dei file di registro corrente verrà rimosso automaticamente la prossima volta che si raccolgono i file di registro.

Attivare manualmente un pacchetto AutoSupport

Per aiutare il supporto tecnico a risolvere i problemi del sistema StorageGRID , è possibile attivare manualmente l'invio di un pacchetto AutoSupport .

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- È necessario disporre dell'autorizzazione di accesso Root o di un'altra configurazione della griglia.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport***.
2. Nella scheda **Azioni**, seleziona **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 **Ultima volta riuscita** nella scheda **Risultati** vengono aggiornati. Se si verifica un problema, il valore **Risultato più recente** viene aggiornato in "Non riuscito" e StorageGRID non tenta più di inviare il pacchetto AutoSupport .

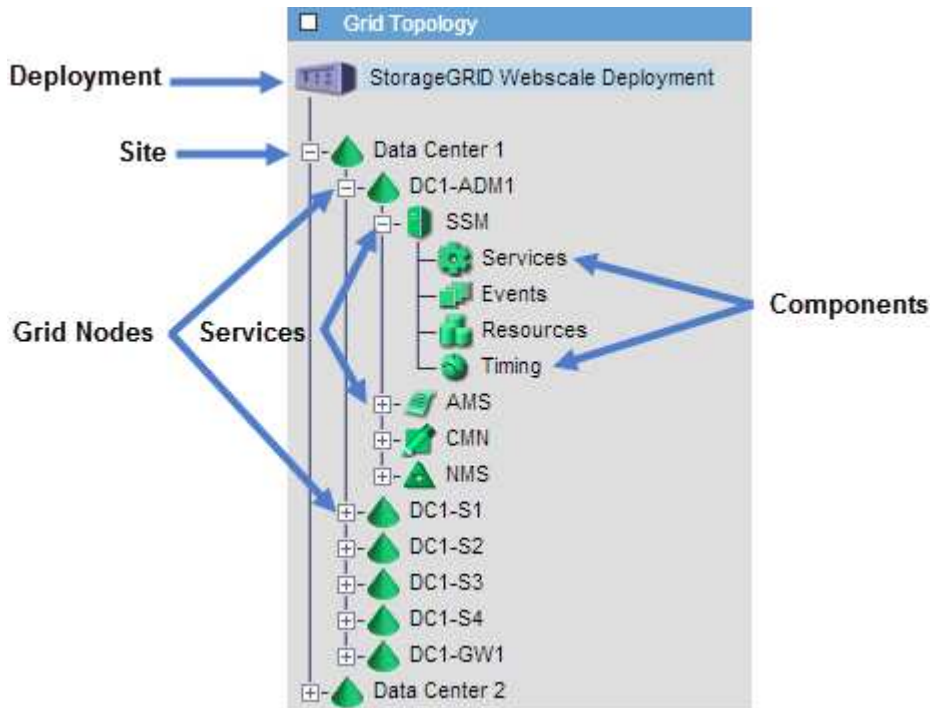


Dopo aver inviato un pacchetto AutoSupport attivato dall'utente, aggiorna la pagina AutoSupport nel browser dopo 1 minuto per accedere ai risultati più recenti.

Visualizza l'albero della topologia della griglia

L'albero della topologia della griglia fornisce accesso a informazioni dettagliate sugli elementi del sistema StorageGRID , inclusi siti, nodi della griglia, servizi e componenti. Nella maggior parte dei casi, è necessario accedere all'albero della topologia della griglia solo quando indicato nella documentazione o quando si lavora con il supporto tecnico.

Per accedere all'albero della topologia della griglia, selezionare **SUPPORTO > Strumenti > Topologia della griglia**.



Per espandere o comprimere l'albero della topologia della griglia, fare clic su **+** o **-** a livello di sito, nodo o servizio. Per espandere o comprimere tutti gli elementi nell'intero sito o in ciascun nodo, tenere premuto il tasto **<Ctrl>** e fare clic.

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, ciascun sito e l'intera griglia.

Gli attributi StorageGRID vengono utilizzati in diversi punti di Grid Manager:

- **Pagina Nodi:** molti dei valori mostrati nella pagina Nodi sono attributi StorageGRID . (Le metriche di Prometheus sono mostrate anche nelle pagine Nodi.)
- **Albero della topologia della griglia:** i valori degli attributi vengono visualizzati nell'albero della topologia della griglia (**SUPPORTO > Strumenti > Topologia della griglia**).
- **Eventi:** gli eventi di sistema si verificano quando determinati attributi registrano un errore o una condizione di guasto per un nodo, inclusi errori quali errori di rete.

Valori degli attributi

Gli attributi vengono riportati con la massima cura e sono approssimativamente corretti. In alcune circostanze, gli aggiornamenti degli attributi possono andare persi, ad esempio in caso di crash di un servizio o di errore e

ricostruzione di un nodo della griglia.

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

Esaminare le metriche di supporto

Durante la risoluzione di un problema, puoi collaborare con il supporto tecnico per esaminare metriche e grafici dettagliati per il tuo sistema StorageGRID .

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Informazioni su questo compito

La pagina Metriche consente di accedere alle interfacce utente di 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'uso da parte del supporto tecnico. Alcune funzionalità e voci di menu all'interno di questi strumenti sono intenzionalmente non funzionali e sono soggette a modifiche. Vedi l'elenco di ["metriche Prometheus comunemente utilizzate"](#) .

Passi

1. Come indicato dal supporto tecnico, seleziona **SUPPORTO > Strumenti > Metriche**.

Di seguito è riportato un esempio della pagina Metriche:

Metrics

Access charts and metrics to help troubleshoot issues.

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

Prometheus

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

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

- [https://\[redacted\]](https://[redacted])

Grafana

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

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

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

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 di 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 versioni 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, puoi collaborare con il supporto tecnico per eseguire la diagnostica sul tuo sistema StorageGRID e analizzare i risultati.

- ["Esaminare le metriche di supporto"](#)
- ["Metriche di Prometheus comunemente utilizzate"](#)

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Informazioni su questo compito

La pagina Diagnostica esegue una serie di controlli diagnostici sullo stato attuale della griglia. Ogni controllo diagnostico può avere uno dei tre stati:

-

✓ **Normale:** Tutti i valori rientrano nell'intervallo normale.

• ⚠ **Attenzione:** uno o più valori sono al di fuori dell'intervallo normale.

• ✖ **Attenzione:** uno o più valori sono significativamente al di fuori dell'intervallo normale.

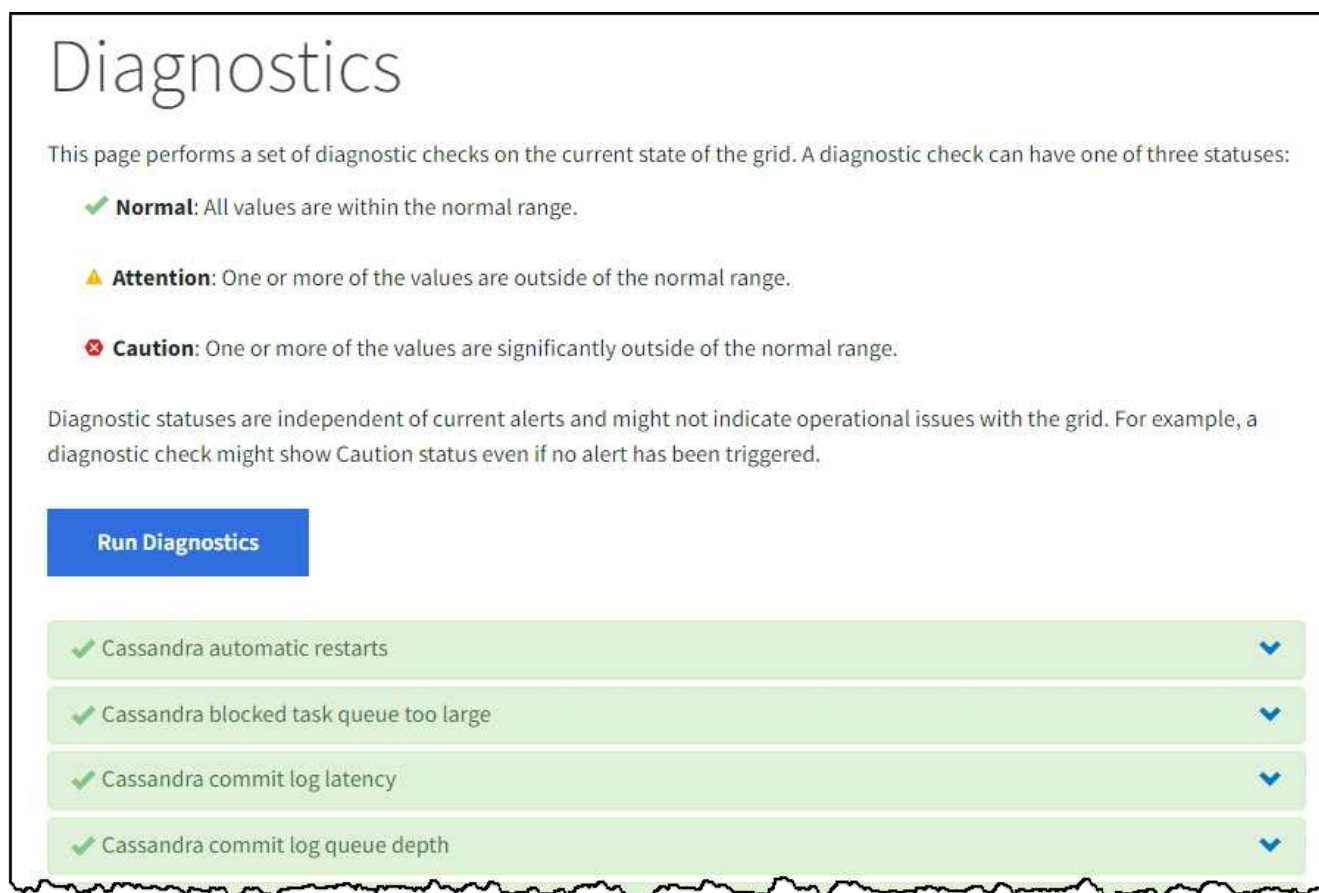
Gli stati diagnostici sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con la rete. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato Attenzione anche se non è stato attivato alcun avviso.

Passi

1. Selezionare **SUPPORTO > Strumenti > Diagnostica**.

Viene visualizzata la pagina Diagnostica, in cui sono elencati i risultati di ciascun controllo diagnostico. I risultati sono ordinati in base alla gravità (Attenzione, Attenzione e Normale). All'interno di ogni gravità, i risultati sono ordinati alfabeticamente.

In questo esempio, tutte le diagnosi hanno uno stato Normale.



The screenshot shows a web interface titled 'Diagnostics'. Below the title, it explains that the page performs diagnostic checks on the current state of the grid and that checks can have one of three statuses: Normal, Attention, or Caution. A blue button labeled 'Run Diagnostics' is visible. Below the button, there is a list of four diagnostic checks, each in a green box with a checkmark icon and a dropdown arrow on the right. All checks are marked as 'Normal'.

Diagnostic Check	Status
✓ Cassandra automatic restarts	Normal
✓ Cassandra blocked task queue too large	Normal
✓ Cassandra commit log latency	Normal
✓ Cassandra commit log queue depth	Normal

2. Per saperne di più su una diagnosi specifica, fare clic in un punto qualsiasi della riga.

Vengono visualizzati i dettagli sulla diagnosi e i suoi risultati attuali. Sono elencati i seguenti dettagli:

- **Stato:** lo stato attuale di questa diagnosi: Normale, Attenzione o Attenzione.
- **Query Prometheus:** se utilizzata per la diagnostica, l'espressione Prometheus utilizzata per generare i valori di stato. (L'espressione di Prometheus non viene utilizzata per tutte le diagnosi.)

- **Soglie:** se disponibili per la diagnosi, le soglie definite dal sistema per ogni stato diagnostico anomalo. (I valori soglia non vengono utilizzati per tutte le diagnosi.)



Non è possibile modificare queste soglie.

- **Valori di stato:** una tabella che mostra lo stato e il valore della diagnostica nell'intero sistema StorageGRID . In questo esempio viene mostrato l'utilizzo attuale 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 diagnosi è Normale.

CPU utilization

Checks the current CPU utilization on each node.

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

Status Normal

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

Thresholds

- Attention $\geq 75\%$
- Caution $\geq 95\%$

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

3. **Facoltativo:** Per visualizzare i grafici Grafana correlati a questa diagnosi, fare clic sul collegamento **Dashboard Grafana**.

Questo collegamento non viene visualizzato per tutte le diagnosi.

Viene visualizzata la dashboard Grafana correlata. In questo esempio, viene visualizzata la dashboard del nodo che mostra l'utilizzo della CPU nel tempo per questo nodo, nonché altri grafici Grafana per il nodo.



È anche possibile accedere alle dashboard Grafana predefinite dalla sezione Grafana della pagina **SUPPORTO > Strumenti > Metriche**.



4. **Facoltativo:** Per visualizzare un grafico dell'espressione di Prometheus nel tempo, fare clic su **Visualizza in Prometheus**.

Appare un grafico di Prometeo dell'espressione utilizzata nella diagnosi.

☐ Enable query history

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

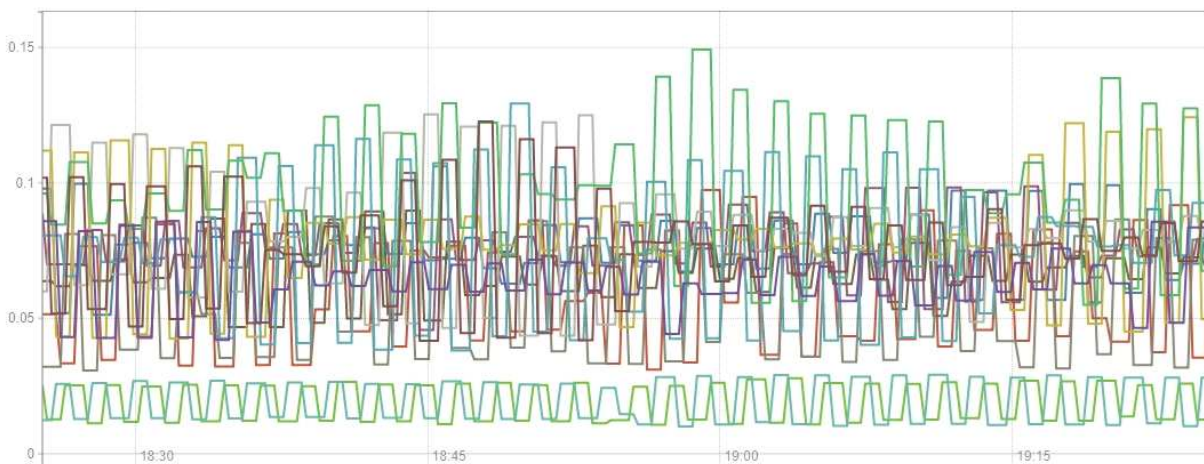
Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

- insert metric at cursor - ▾

Graph Console

1h ⏪ Until ⏩ Res. (s) ☐ stacked



Remove Graph

Add Graph

Crea applicazioni di monitoraggio personalizzate

È possibile creare applicazioni di monitoraggio e dashboard personalizzate utilizzando le metriche StorageGRID disponibili nell'API Grid Management.

Se si desidera monitorare metriche non visualizzate in una pagina esistente di Grid Manager o se si desidera creare dashboard personalizzate per StorageGRID, è possibile utilizzare l'API Grid Management per interrogare le metriche StorageGRID.

È anche possibile accedere direttamente alle metriche di Prometheus tramite uno strumento di monitoraggio esterno, come Grafana. Per utilizzare uno strumento esterno è necessario caricare o generare un certificato client amministrativo per consentire a StorageGRID di autenticare lo strumento per motivi di sicurezza. Vedi [il "Istruzioni per l'amministrazione StorageGRID"](#).

Per visualizzare le operazioni API delle metriche, incluso l'elenco completo delle metriche disponibili, vai a Grid Manager. Nella parte superiore della pagina, seleziona l'icona della guida e seleziona **Documentazione API > metriche**.

GET

`/grid/metric-labels/{label}/values` Lists the values for a metric label

GET

`/grid/metric-names` Lists all available metric names

GET

`/grid/metric-query` Performs an instant metric query at a single point in time

GET

`/grid/metric-query-range` Performs a metric query over a range of time

I dettagli su come implementare un'applicazione di monitoraggio personalizzata esulano dallo scopo di questa documentazione.

Risoluzione dei problemi del sistema StorageGRID

Risoluzione dei problemi di un sistema StorageGRID

Se si verifica un problema durante l'utilizzo di un sistema StorageGRID, fare riferimento ai suggerimenti e alle linee guida in questa sezione per individuare e risolvere il problema.

Spesso è possibile risolvere i problemi autonomamente; tuttavia, potrebbe essere necessario segnalare alcuni problemi al supporto tecnico.

Definisci il problema

Il primo passo per risolvere un problema è definirlo chiaramente.

Questa tabella fornisce esempi dei tipi di informazioni che potresti 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 gli oggetti non possono essere acquisiti in StorageGRID.
Quando è iniziato il problema?	L'acquisizione di oggetti è stata negata per la prima volta intorno alle 14:50 dell'8 gennaio 2020.
Come hai notato per la prima volta il problema?	Notificato dall'applicazione client. Ho ricevuto anche notifiche di avviso via email.
Il problema si verifica regolarmente o solo a volte?	Il problema persiste.
Se il problema si verifica regolarmente, quali passaggi lo causano?	Il problema si verifica ogni volta che un client tenta di acquisire un oggetto.

Domanda	Esempio di risposta
Se il problema si verifica in modo intermittente, quando si verifica? Annota gli orari di ogni incidente di cui sei a conoscenza.	Il problema non è intermittente.
Hai già riscontrato questo problema? Con quale frequenza hai avuto questo problema in passato?	È la prima volta che vedo questo problema.

Valutare il rischio e l'impatto sul sistema

Dopo aver 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 erogando servizi essenziali.

Questa tabella riassume l'impatto che il problema di esempio sta avendo sulle operazioni del sistema:

Domanda	Esempio di risposta
Il sistema StorageGRID può acquisire contenuti?	NO.
Le applicazioni client possono recuperare contenuti?	Alcuni oggetti possono essere recuperati, altri no.
I dati sono a rischio?	NO.
La capacità di svolgere attività imprenditoriale è gravemente compromessa?	Sì, perché le applicazioni client non possono archiviare oggetti nel sistema StorageGRID e i dati non possono essere recuperati in modo coerente.

Raccogliere dati

Dopo aver definito il problema e valutato il rischio e l'impatto, raccogliere i dati per l'analisi. Il tipo di dati più utile da raccogliere dipende dalla natura del problema.

Tipologia di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Crea una cronologia delle modifiche recenti	Le modifiche apportate al sistema StorageGRID , alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.	• Crea una cronologia delle modifiche recenti

Tipologia di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Avvisi di revisione	Gli avvisi possono aiutarti a determinare rapidamente la causa principale di un problema, fornendo indizi importanti sui problemi sottostanti che potrebbero esserne la causa. Esamina l'elenco degli avvisi correnti per verificare se StorageGRID ha identificato la causa principale di un problema. Per ulteriori informazioni, consultare gli avvisi attivati in passato.	• "Visualizza gli avvisi correnti e risolti"
Monitorare gli eventi	Gli eventi includono qualsiasi errore di sistema o evento di guasto per un nodo, compresi errori come gli errori di rete. Monitora gli eventi per saperne di più sui problemi o per trovare aiuto nella risoluzione dei problemi.	• "Monitorare gli eventi"
Identificare le tendenze utilizzando grafici e report di testo	Le tendenze possono fornire indizi preziosi su quando si sono manifestati i primi problemi e possono aiutarti a capire con quale rapidità le cose stanno cambiando.	• "Utilizzare diagrammi e grafici" • "Utilizzare report di testo"
Stabilire le linee di base	Raccogliere informazioni sui livelli normali dei vari valori operativi. Questi valori di base e le deviazioni da essi possono fornire indizi preziosi.	• Stabilire le linee di base
Eseguire test di ingestione e recupero	Per risolvere i problemi di prestazioni relativi all'acquisizione e al recupero, utilizzare una workstation per archiviare e recuperare gli oggetti. Confronta i risultati con quelli ottenuti utilizzando l'applicazione client.	• "Monitorare le prestazioni PUT e GET"
Rivedi i messaggi di audit	Esaminare i messaggi di controllo per seguire in dettaglio le operazioni StorageGRID. I dettagli nei messaggi di controllo possono essere utili per risolvere molti tipi di problemi, compresi quelli relativi alle prestazioni.	• "Rivedi i messaggi di audit"
Controllare le posizioni degli oggetti e l'integrità dell'archiviazione	Se riscontri problemi di stoccaggio, verifica che gli oggetti siano posizionati dove previsto. Verificare l'integrità dei dati degli oggetti su un nodo di archiviazione.	• "Monitorare le operazioni di verifica degli oggetti" • "Confermare le posizioni dei dati degli oggetti" • "Verificare l'integrità dell'oggetto"

Tipologia di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Raccogliere dati per il supporto tecnico	L'assistenza tecnica potrebbe chiederti di raccogliere dati o di esaminare informazioni specifiche per aiutarti a risolvere i problemi.	• "Raccogli file di registro e dati di sistema" • "Attivare manualmente un pacchetto AutoSupport" • "Esaminare le metriche di supporto"

Crea una cronologia delle modifiche recenti

Quando si verifica un problema, è opportuno considerare cosa è cambiato di recente e quando si sono verificati tali cambiamenti.

- Le modifiche apportate al sistema StorageGRID , alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.
- Una cronologia delle modifiche può aiutarti a identificare quali modifiche potrebbero essere responsabili di un problema e in che modo ciascuna modifica potrebbe averne influenzato lo sviluppo.

Crea una tabella delle modifiche recenti apportate al tuo sistema che includa informazioni su quando si è verificata ciascuna modifica e tutti i dettagli rilevanti sulla modifica, come informazioni su cos'altro stava accadendo mentre la modifica era in corso:

Tempo di cambiamento	Tipo di modifica	Dettagli
Per esempio: • Quando hai iniziato il ripristino del nodo? • Quando è stato completato l'aggiornamento del software? • Hai interrotto il processo?	Quello che è successo? Che cosa hai fatto?	Documentare tutti i dettagli rilevanti relativi alla modifica. Per esempio: • Dettagli delle modifiche alla rete. • Quale hotfix è stato installato. • Come sono cambiati i carichi di lavoro dei clienti. Assicurati di annotare se si verificano più modifiche contemporaneamente. Ad esempio, questa modifica è stata apportata mentre era in corso un aggiornamento?

Esempi di cambiamenti significativi recenti

Ecco alcuni esempi di cambiamenti potenzialmente significativi:

- Il sistema StorageGRID è stato installato, ampliato o ripristinato di recente?
- Il sistema è stato aggiornato di recente? È stato applicato un hotfix?
- Di recente è stato riparato o cambiato qualche componente hardware?
- La politica ILM è stata aggiornata?

- Il carico di lavoro del cliente è cambiato?
- L'applicazione client o il suo comportamento sono cambiati?
- Hai modificato i bilanciatori del carico oppure aggiunto o rimosso un gruppo ad alta disponibilità di nodi amministrativi o nodi gateway?
- Sono stati avviati dei compiti che potrebbero richiedere molto tempo per essere completati? Alcuni esempi:
 - Ripristino di un nodo di archiviazione non riuscito
 - Dismissione del nodo di archiviazione
- Sono state apportate modifiche all'autenticazione utente, ad esempio l'aggiunta di un tenant o la modifica della configurazione LDAP?
- È in corso la migrazione dei dati?
- I servizi della piattaforma sono stati abilitati o modificati di recente?
- La conformità è stata abilitata di recente?
- Sono stati aggiunti o rimossi pool di archiviazione cloud?
- Sono state apportate modifiche alla compressione o alla crittografia dell'archiviazione?
- Ci sono state modifiche all'infrastruttura di rete? Ad esempio, VLAN, router o DNS.
- Sono state apportate modifiche alle fonti NTP?
- Sono state apportate modifiche alle interfacce Grid, Admin o Client Network?
- Sono state apportate altre modifiche al sistema StorageGRID o al suo ambiente?

Stabilire le linee di base

È possibile stabilire i valori di base per il sistema registrando i livelli normali di vari valori operativi. In futuro, sarà possibile confrontare i valori attuali con questi valori di base per individuare e risolvere i valori anomali.

Proprietà	Valore	Come ottenere
Consumo medio di spazio di archiviazione	GB consumati/giorno Percentuale consumata/giorno	Vai al Grid Manager. Nella pagina Nodi, seleziona l'intera griglia o un sito e vai alla scheda Archiviazione. Nel grafico Spazio di archiviazione utilizzato - Dati oggetto, individuare un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare la quantità di spazio di archiviazione 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/giorno Percentuale consumata/giorno	Vai al Grid Manager. Nella pagina Nodi, seleziona l'intera griglia o un sito e vai alla scheda Archiviazione. Nel grafico Spazio di archiviazione utilizzato - Metadati oggetto, individuare un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare la quantità di spazio di archiviazione 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, seleziona Prestazioni > Operazioni S3 oppure Prestazioni > Operazioni Swift. Per visualizzare le velocità e i conteggi di acquisizione e recupero per un sito o un nodo specifico, selezionare NODI > sito o Nodo di archiviazione > Oggetti. Posiziona il cursore sul grafico Ingest and Retrieve per S3.
Operazioni S3/Swift non riuscite	Operazioni	Selezionare SUPPORTO > Strumenti > Topologia griglia . Nella scheda Panoramica nella sezione Operazioni API, visualizza il valore per Operazioni S3 - Non riuscite o Operazioni Swift - Non riuscite.
Tasso di valutazione ILM	Oggetti/secondo	Dalla pagina Nodi, seleziona grid > ILM. Nel grafico della coda ILM, trova un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare un valore di base per il tasso di valutazione del tuo sistema.
Frequenza di scansione ILM	Oggetti/secondo	Selezionare NODI > griglia > ILM. Nel grafico della coda ILM, trova un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare un valore di base per la velocità di scansione del tuo sistema.
Oggetti in coda dalle operazioni client	Oggetti/secondo	Selezionare NODI > griglia > ILM. Nel grafico della coda ILM, trova un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare un valore di base per gli Oggetti in coda (dalle operazioni client) per il tuo sistema.

Proprietà	Valore	Come ottenere
Latenza media delle query	Millisecondi	Selezionare NODI > Nodo di archiviazione > Oggetti . Nella tabella Query, visualizza il valore per Latenza media.

Analizzare i dati

Utilizza le informazioni raccolte per determinare la causa del problema e le possibili soluzioni.

L'analisi dipende dal problema, ma in generale:

- Individua i punti di errore e i colli di bottiglia utilizzando gli avvisi.
- Ricostruire la cronologia dei problemi utilizzando la cronologia degli avvisi e i grafici.
- Utilizzare i grafici per individuare anomalie e confrontare la situazione problematica con il normale funzionamento.

Lista di controllo delle informazioni di escalation

Se non riesci a risolvere il problema da solo, contatta l'assistenza tecnica. Prima di contattare l'assistenza tecnica, raccogliere le informazioni elencate nella tabella seguente per facilitare la risoluzione dei problemi.

	Articolo	Note
	Enunciato del problema	Quali sono i sintomi del problema? Quando è iniziato il problema? Si verifica in modo costante o intermittente? Se si verifica in modo intermittente, in quali momenti? Definisci il problema
	Valutazione dell'impatto	Qual è la gravità del problema? Qual è l'impatto sull'applicazione client? • Il client si è già connesso correttamente in precedenza? • Il client può acquisire, recuperare ed eliminare dati?
	ID di sistema StorageGRID	Selezionare MANUTENZIONE > Sistema > Licenza . L'ID del sistema StorageGRID viene visualizzato come parte della licenza corrente.
	Versione del software	Nella parte superiore di Grid Manager, seleziona l'icona della guida e seleziona Informazioni per visualizzare la versione StorageGRID .

	Articolo	Note
	Personalizzazione	Riassumi la configurazione del tuo sistema StorageGRID . Ad esempio, elenca quanto segue: • La griglia utilizza la compressione dell'archiviazione, la crittografia dell'archiviazione o la conformità? • ILM realizza oggetti replicati o con codice di cancellazione? ILM garantisce la ridondanza del sito? Le regole ILM utilizzano i comportamenti di ingestione Balanced, Strict o Dual Commit?
	File di registro e dati di sistema	Raccogli file di registro e dati di sistema per il tuo sistema. Selezionare SUPPORTO > Strumenti > Registri. È possibile raccogliere i log per l'intera griglia o per nodi selezionati. Se si raccolgono i log solo per nodi selezionati, assicurarsi di includere almeno un nodo di archiviazione che disponga del servizio ADC. (I primi tre nodi di archiviazione in un sito includono il servizio ADC.) "Raccogli file di registro e dati di sistema"
	Informazioni di base	Raccogliere informazioni di base sulle operazioni di acquisizione, sulle operazioni di recupero e sul consumo di spazio di archiviazione. Stabilire le linee di base
	Cronologia delle modifiche recenti	Crea una cronologia che riepiloghi tutte le modifiche recenti apportate al sistema o al suo ambiente. Crea una cronologia delle modifiche recenti
	Cronologia degli sforzi per diagnosticare il problema	Se hai adottato misure per diagnosticare o risolvere autonomamente il problema, assicurati di annotare i passaggi eseguiti e il risultato.

Risolvere i problemi relativi agli oggetti e all'archiviazione

Confermare le posizioni dei dati degli oggetti

A seconda del problema, potresti voler ["confermare dove vengono archiviati i dati dell'oggetto"](#) . Ad esempio, potresti voler verificare che la policy ILM funzioni come previsto e che i dati degli oggetti vengano archiviati dove previsto.

Prima di iniziare

- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:

- **UUID**: Identificatore univoco universale dell'oggetto. Inserire il UUID in maiuscolo.
- **CBID**: Identificatore univoco dell'oggetto all'interno StorageGRID . È possibile ottenere il CBID di un oggetto dal registro di controllo. Inserire il CBID in maiuscolo.
- **Chiave oggetto e bucket S3**: quando un oggetto viene ingerito tramite ["Interfaccia S3"](#) , l'applicazione client utilizza una combinazione di bucket e chiave oggetto per memorizzare e identificare l'oggetto.

Passi

1. Selezionare **ILM > Ricerca metadati oggetto**.
2. Digitare l'identificatore dell'oggetto nel campo **Identificatore**.

È possibile immettere un UUID, CBID, bucket S3/chiave oggetto o contenitore Swift/nome oggetto.

3. Se si desidera cercare una versione specifica dell'oggetto, immettere l'ID della versione (facoltativo).

4. Seleziona **Cerca**.

IL ["risultati della ricerca dei metadati degli oggetti"](#) apparire. In questa pagina sono elencati i seguenti tipi di informazioni:

- Metadati di sistema, tra cui l'ID dell'oggetto (UUID), l'ID della 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 in cui l'oggetto è stato creato per la prima volta e la data e l'ora in cui l'oggetto è stato modificato per l'ultima volta.
- Qualsiasi coppia chiave-valore di metadati utente personalizzati associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore del tag oggetto associata all'oggetto.
- Per le copie di oggetti replicati, la posizione di archiviazione corrente di ciascuna copia.
- Per le copie di oggetti con codice di cancellazione, la posizione di archiviazione 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 oggetti multiparte, un elenco di segmenti di oggetti, inclusi gli identificatori di segmento e le dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono mostrati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di archiviazione interna non elaborato. Questi metadati grezzi includono metadati di sistema interni la cui persistenza da una versione all'altra non è garantita.

L'esempio seguente mostra i risultati della ricerca dei metadati dell'oggetto per un oggetto di test S3

archiviato 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": {
      "PAIRS": "2",

```

Errori dell'archivio oggetti (volume di archiviazione)

Lo storage sottostante su un nodo di storage è suddiviso in archivi di oggetti. Gli archivi di oggetti sono anche noti come volumi di archiviazione.

È possibile visualizzare le informazioni sull'archivio oggetti per ciascun nodo di archiviazione. Gli archivi degli oggetti vengono visualizzati nella parte inferiore della pagina **NODI > Nodo di archiviazione_ > Archiviazione**.

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

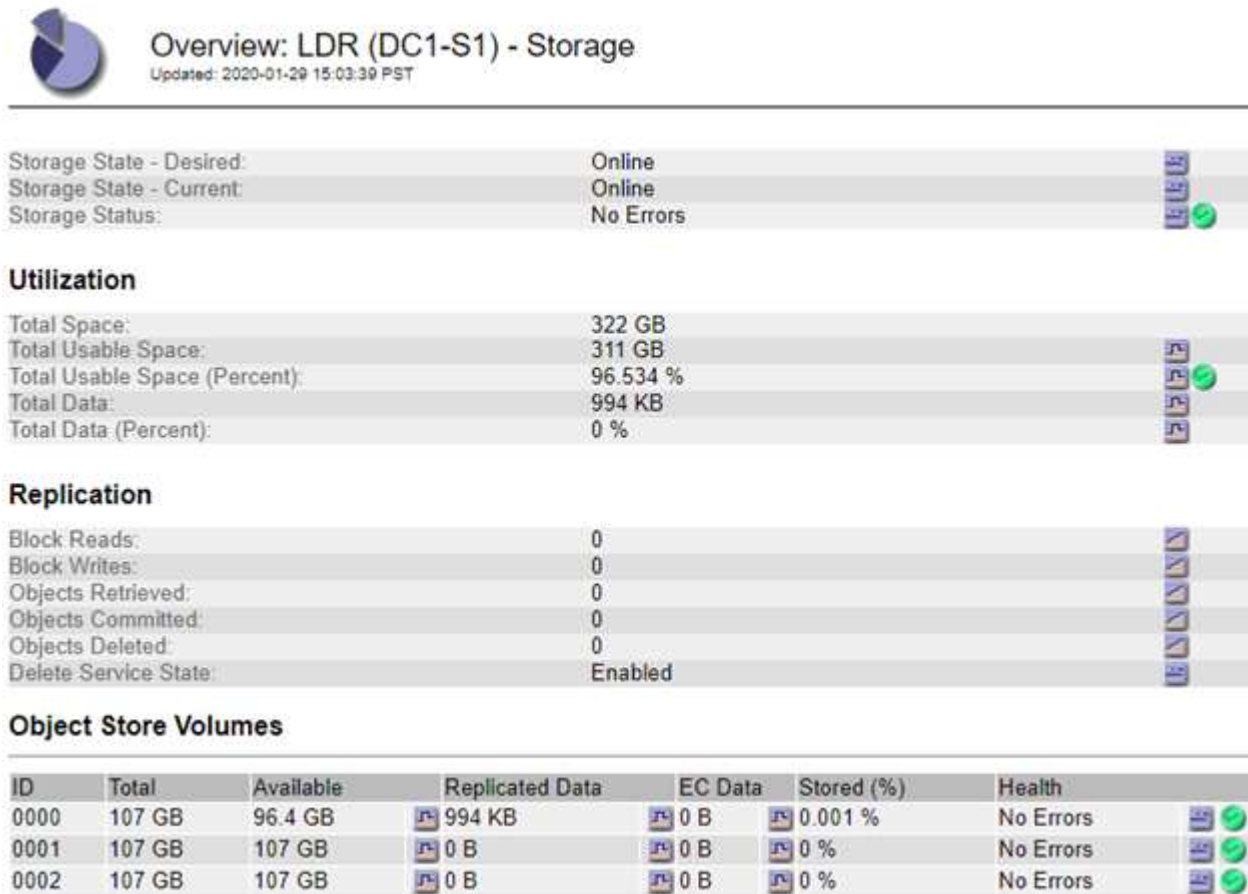
Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdC	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	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 vedere di più "dettagli su ciascun nodo di archiviazione", segui questi passaggi:

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **site > Storage Node > LDR > Storage > Panoramica > Principale**.



A seconda della natura del guasto, i guasti con un volume di archiviazione potrebbero riflettersi in "avvisi sul volume di archiviazione". Se un volume di archiviazione si guasta, è necessario ripararlo per ripristinare la piena funzionalità del nodo di archiviazione il prima possibile. Se necessario, puoi andare alla scheda **Configurazione** e "posizionare il nodo di archiviazione in uno stato di sola lettura" in modo che il sistema StorageGRID possa utilizzarlo per il recupero dei dati mentre ci si prepara per un ripristino completo del server.

Verificare l'integrità dell'oggetto

Il sistema StorageGRID verifica l'integrità dei dati degli oggetti sui nodi di archiviazione, controllando sia gli oggetti danneggiati che quelli mancanti.

Esistono due processi di verifica: la verifica in background e il controllo dell'esistenza dell'oggetto (in precedenza denominato verifica in foreground). Lavorano insieme per garantire l'integrità dei dati. La verifica in background viene eseguita automaticamente e controlla costantemente 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 cosa è la verifica dei precedenti?

Il processo di verifica in background controlla automaticamente e costantemente i nodi di archiviazione per individuare copie danneggiate dei dati degli oggetti e tenta automaticamente di riparare eventuali problemi

rilevati.

La verifica degli sfondi verifica l'integrità degli oggetti replicati e degli oggetti con codice di cancellazione, come segue:

- **Oggetti replicati:** se il processo di verifica in background rileva un oggetto replicato danneggiato, la copia danneggiata viene rimossa dalla sua posizione e messa in quarantena altrove nel nodo di archiviazione. Quindi, viene generata una nuova copia non danneggiata e posizionata per soddisfare i criteri ILM attivi. La nuova copia potrebbe non essere posizionata sul nodo di archiviazione utilizzato per la copia originale.



I dati degli oggetti danneggiati vengono messi in quarantena anziché essere eliminati dal sistema, in modo che sia ancora possibile accedervi. Per ulteriori informazioni sull'accesso ai dati degli oggetti in quarantena, contattare l'assistenza tecnica.

- **Oggetti con codice di cancellazione:** se il processo di verifica in background rileva che un frammento di un oggetto con codice di cancellazione è danneggiato, StorageGRID tenta automaticamente di ricostruire il frammento mancante sul posto sullo stesso nodo di archiviazione, utilizzando i dati rimanenti e i frammenti di parità. Se il frammento danneggiato non può essere ricostruito, viene effettuato 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 archiviazione. Non controlla gli oggetti in un Cloud Storage Pool. Per poter essere sottoposti alla verifica dei precedenti, gli oggetti devono avere più di quattro giorni.

La verifica degli sfondi avviene a una velocità continua, studiata per non interferire con le normali attività del sistema. La verifica dei precedenti non può essere interrotta. Tuttavia, è possibile aumentare la frequenza di verifica in background per verificare più rapidamente il contenuto di un nodo di archiviazione se si sospetta un problema.

Avvisi relativi alla verifica dei precedenti

Se il sistema rileva un oggetto danneggiato che non è in grado di correggere automaticamente (perché il danneggiamento impedisce l'identificazione dell'oggetto), viene attivato l'avviso **Oggetto danneggiato non identificato rilevato**.

Se la verifica in background non riesce a sostituire un oggetto danneggiato perché non riesce a individuarne un'altra copia, viene attivato l'avviso **Oggetti persi**.

Modificare il tasso di verifica in background

È possibile modificare la frequenza con cui la verifica in background controlla i dati degli oggetti replicati su un nodo di archiviazione se si hanno dubbi sull'integrità dei dati.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).

Informazioni su questo compito

È possibile modificare la frequenza di verifica per la verifica in background su un nodo di archiviazione:

- **Adattivo:** impostazione predefinita. L'attività è progettata per verificare un massimo di 4 MB/s o 10 oggetti/s (a seconda di quale valore venga superato per primo).

- **Alto**: la verifica dell'archiviazione procede rapidamente, a una velocità che può rallentare le normali attività del sistema.

Utilizzare il tasso di verifica elevato solo quando si sospetta che un errore hardware o software possa aver danneggiato i dati dell'oggetto. Una volta completata la verifica in background ad alta priorità, la frequenza di verifica viene automaticamente reimpostata su **Adattiva**.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **Nodo di archiviazione > LDR > Verifica**.
3. Selezionare **Configurazione > Principale**.
4. Vai a **LDR > Verifica > Configurazione > Principale**.
5. In Verifica in background, seleziona **Tasso di verifica > Alto** o **Tasso di verifica > Adatto**.

The screenshot shows the 'Configuration: LDR () - Verification' page. The 'Verification Rate' dropdown is highlighted with a green box and is set to 'Adaptive'. Other settings include 'Reset Missing Objects Count', 'Reset Corrupt Objects Count', and 'Delete Quarantined Objects', each with an unchecked checkbox. The 'Apply Changes' button is located at the bottom right.

6. Fare clic su **Applica modifiche**.
7. Monitorare i risultati della verifica in background per gli oggetti replicati.
 - a. Vai a **NODI > Nodo di archiviazione > Oggetti**.
 - b. Nella sezione Verifica, monitorare i valori per **Oggetti corrotti** e **Oggetti corrotti non identificati**.

Se la verifica in background rileva dati di oggetti replicati corrotti, la metrica **Oggetti corrotti** viene incrementata e StorageGRID tenta di estrarre l'identificatore dell'oggetto dai dati, come segue:

- Se è possibile estrarre l'identificatore dell'oggetto, StorageGRID crea automaticamente una nuova copia dei dati dell'oggetto. La nuova copia può essere creata in qualsiasi punto del sistema StorageGRID che soddisfi i criteri ILM attivi.
- Se non è possibile estrarre l'identificatore dell'oggetto (perché è danneggiato), la metrica **Oggetti danneggiati non identificati** viene incrementata e viene attivato l'avviso **Oggetto danneggiato non identificato rilevato**.

- c. Se vengono rilevati dati di oggetti replicati danneggiati, contattare l'assistenza tecnica per determinare la causa principale del danneggiamento.

8. Monitorare i risultati della verifica in background per gli oggetti con codice di cancellazione.

Se la verifica in background rileva frammenti danneggiati di dati di oggetti con codice di cancellazione, l'attributo Frammenti danneggiati rilevati viene incrementato. StorageGRID esegue il ripristino ricostruendo il frammento danneggiato sul posto, sullo stesso nodo di archiviazione.

- a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
- b. Selezionare **Nodo di archiviazione > LDR > Codifica di cancellazione**.
- c. Nella tabella Risultati di verifica, monitorare l'attributo Frammenti corrotti rilevati (ECCD).

9. Dopo che gli oggetti danneggiati sono stati ripristinati automaticamente dal sistema StorageGRID, reimpostare il conteggio degli oggetti danneggiati.

- a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
- b. Selezionare **Nodo di archiviazione > LDR > Verifica > Configurazione**.
- c. Selezionare **Reimposta conteggio oggetti danneggiati**.
- d. Fare clic su **Applica modifiche**.

10. Se sei sicuro che gli oggetti in quarantena non siano necessari, puoi eliminarli.



Se è stato attivato l'avviso **Oggetti persi**, il supporto tecnico potrebbe voler accedere agli oggetti in quarantena per risolvere il problema sottostante o tentare il recupero dei dati.

- a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
- b. Selezionare **Nodo di archiviazione > LDR > Verifica > Configurazione**.
- c. Selezionare **Elimina oggetti in quarantena**.
- d. Selezionare **Applica modifiche**.

Che cos'è il controllo dell'esistenza di un oggetto?

Il controllo dell'esistenza dell'oggetto verifica se tutte le copie replicate previste degli oggetti e dei frammenti con codice di cancellazione sono presenti su un nodo di archiviazione. Il controllo dell'esistenza dell'oggetto non verifica i dati dell'oggetto stesso (lo fa la verifica in background); fornisce invece un modo per verificare l'integrità dei dispositivi di archiviazione, soprattutto se un recente problema hardware potrebbe aver influito sull'integrità dei dati.

A differenza della verifica in background, che avviene automaticamente, è necessario avviare manualmente un processo di controllo dell'esistenza dell'oggetto.

Il controllo dell'esistenza degli oggetti legge i metadati di ogni oggetto archiviato in StorageGRID e verifica l'esistenza sia delle copie replicate degli oggetti sia dei frammenti degli oggetti con codice di cancellazione. Eventuali dati mancanti vengono gestiti come segue:

- **Copie replicate:** se manca una copia dei dati dell'oggetto replicato, StorageGRID tenta automaticamente di sostituire la copia con una copia archiviata altrove nel sistema. Il nodo di archiviazione esegue una copia esistente tramite una valutazione ILM, che determinerà che l'attuale criterio ILM non viene più rispettato per questo oggetto perché manca un'altra copia. Viene generata e posizionata una nuova copia per soddisfare le policy ILM attive del sistema. Questa nuova copia potrebbe non essere collocata nella stessa posizione in cui era archiviata la copia mancante.

- **Frammenti con codice di cancellazione:** se manca un frammento di un oggetto con codice di cancellazione, StorageGRID tenta automaticamente di ricostruire il frammento mancante in posizione sullo stesso nodo di archiviazione utilizzando i frammenti rimanenti. Se il frammento mancante non può essere ricostruito (perché sono andati persi troppi frammenti), ILM tenta di trovare un'altra copia dell'oggetto, che può utilizzare per generare un nuovo frammento con codice di cancellazione.

Esegui il controllo dell'esistenza dell'oggetto

È possibile creare ed eseguire un processo di controllo dell'esistenza di un oggetto alla volta. Quando si crea un processo, si selezionano i nodi di archiviazione e i volumi che si desidera verificare. Seleziona anche la coerenza del lavoro.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#) .
- Hai verificato che i nodi di archiviazione che desideri controllare siano online. Selezionare **NODI** per visualizzare la tabella dei nodi. Assicurarsi che non vengano visualizzate icone di avviso accanto al nome del nodo per i nodi che si desidera controllare.
- Hai verificato che le seguenti procedure **non** siano in esecuzione sui nodi che vuoi controllare:
 - Espansione della griglia per aggiungere un nodo di archiviazione
 - Disattivazione del nodo di archiviazione
 - Recupero di un volume di archiviazione non riuscito
 - Ripristino di un nodo di archiviazione con un'unità di sistema guasta
 - Riequilibrio della CE
 - Clonazione del nodo dell'appliance

Il controllo dell'esistenza dell'oggetto non fornisce informazioni utili mentre queste procedure sono in corso.

Informazioni su questo compito

Il completamento di un processo di controllo dell'esistenza di un oggetto può richiedere giorni o settimane, a seconda del numero di oggetti nella griglia, dei nodi e dei volumi di archiviazione selezionati e della coerenza selezionata. È possibile eseguire un solo processo alla volta, ma è possibile selezionare più nodi di archiviazione e volumi contemporaneamente.

Passi

1. Selezionare **MANUTENZIONE > Attività > Controllo esistenza oggetto**.
2. Seleziona **Crea lavoro**. Viene visualizzata la procedura guidata Crea un processo di controllo 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 **Nome nodo** nell'intestazione della colonna.

È possibile effettuare la ricerca per nome del nodo o per sito.

Non è possibile selezionare nodi che non sono connessi alla griglia.

4. Selezionare **Continua**.
5. Selezionare uno o più volumi per ciascun nodo nell'elenco. È possibile cercare volumi utilizzando il numero del volume di archiviazione o il nome del nodo.

Per selezionare tutti i volumi per ciascun nodo selezionato, seleziona la casella di controllo **Volume di archiviazione** nell'intestazione della colonna.

6. Selezionare **Continua**.

7. Selezionare la coerenza per il lavoro.

La coerenza determina quante copie dei metadati dell'oggetto vengono utilizzate per il controllo dell'esistenza dell'oggetto.

- **Strong-site**: due copie di metadati in un unico sito.
- **Strong-global**: due copie di metadati in ogni sito.
- **Tutti** (predefinito): tutte e tre le copie dei metadati in ciascun sito.

Per ulteriori informazioni sulla coerenza, consultare le descrizioni nella procedura guidata.

8. Selezionare **Continua**.

9. Rivedi e verifica le tue selezioni. È possibile selezionare **Precedente** per tornare a un passaggio precedente della procedura guidata e aggiornare le selezioni.

Viene generato un processo di controllo dell'esistenza dell'oggetto che viene eseguito finché non si verifica una delle seguenti situazioni:

- Il lavoro è completato.
- Metti in pausa o annulla il lavoro. Puoi riprendere un lavoro che hai messo in pausa, ma non puoi riprendere un lavoro che hai annullato.
- Il lavoro si blocca. Viene attivato l'avviso **Controllo esistenza oggetto bloccato**. Seguire le azioni correttive specificate per l'avviso.
- Il lavoro fallisce. Viene attivato l'avviso **Controllo esistenza oggetto fallito**. Seguire le azioni correttive specificate per l'avviso.
- Viene visualizzato il messaggio "Servizio non disponibile" o "Errore interno del server". Dopo un minuto, aggiorna la pagina per continuare a monitorare il lavoro.



Se necessario, è possibile uscire dalla pagina di controllo dell'esistenza dell'oggetto e tornare indietro per continuare a monitorare il processo.

10. Durante l'esecuzione del processo, visualizzare la scheda **Processo attivo** e annotare il valore di Copie di oggetti mancanti rilevate.

Questo valore rappresenta il numero totale di copie mancanti di oggetti replicati e di oggetti con codice di cancellazione con uno o più frammenti mancanti.

Se il numero di copie di oggetti mancanti rilevate è maggiore di 100, potrebbe esserci un problema con l'archiviazione del nodo di archiviazione.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job

Job history

Status: Accepted

Consistency control: All

Job ID: 2334602652907829302

Start time: 2021-11-10 14:43:02 MST

Missing object copies detected: 0

Elapsed time: —

Progress: 0%

Estimated time to completion: —

Pause

Cancel

Volumes

Details

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Una volta completato il lavoro, eseguire eventuali azioni aggiuntive richieste:

- Se il valore di Copie di oggetti mancanti rilevate è pari a zero, non sono stati rilevati problemi. Non è richiesta alcuna azione.
- Se il valore Copie di oggetti mancanti rilevate è maggiore di zero e non è stato attivato l'avviso **Oggetti persi**, 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 il valore Copie di oggetti mancanti rilevate è maggiore di zero e viene attivato l'avviso **Oggetti persi**, l'integrità dei dati potrebbe essere compromessa. Contattare l'assistenza tecnica.
- È possibile esaminare le copie degli oggetti persi utilizzando grep per estrarre i messaggi di controllo LLST: `grep LLST audit_file_name`.

Questa procedura è simile a quella per "investigare oggetti smarriti", sebbene per le copie degli oggetti si cerchi LLST invece di OLST.

12. Se per il processo è stata selezionata la coerenza strong-site o strong-global, attendere circa tre settimane per la coerenza dei metadati, quindi eseguire nuovamente il processo sugli stessi volumi.

Quando StorageGRID ha avuto il tempo di raggiungere la coerenza dei metadati per i nodi e i volumi inclusi nel processo, la riesecuzione del processo potrebbe cancellare le copie di oggetti mancanti segnalate erroneamente o determinare il controllo di copie di oggetti aggiuntive, se mancanti.

- Selezionare **MANUTENZIONE > Controllo esistenza oggetto > Cronologia lavori**.
- Determina quali lavori sono pronti per essere rieseguiti:

- i. Consultare la colonna **Ora di fine** per determinare quali lavori sono stati eseguiti più di tre settimane fa.
- ii. Per tali lavori, scansionare la colonna Controllo coerenza per strong-site o strong-global.
- c. Selezionare la casella di controllo per ogni processo che si desidera rieseguire, quindi selezionare **Riesegui**.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job
Job history

Delete
Rerun

Displaying 4 results

☐	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
☒	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
☐	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- d. Nella procedura guidata Riesegui processi, rivedere i nodi e i volumi selezionati e la coerenza.
- e. Quando sei pronto a rieseguire i processi, seleziona **Riesegui**.

Viene visualizzata la scheda Lavoro attivo. Tutti i lavori selezionati vengono rieseguiti come un unico lavoro con la coerenza di strong-site. Nel campo **Lavori correlati** nella sezione Dettagli sono elencati gli ID dei lavori originali.

Dopo aver finito

Se hai ancora dubbi sull'integrità dei dati, vai su **SUPPORTO > Strumenti > Topologia griglia > sito > Nodo di archiviazione > LDR > Verifica > Configurazione > Principale** e aumenta la frequenza di verifica in background. La verifica in background verifica la correttezza di tutti i dati degli oggetti memorizzati e ripara eventuali problemi rilevati. Individuare e riparare i potenziali problemi il più rapidamente possibile riduce il rischio di perdita di dati.

Risoluzione dei problemi S3 PUT Avviso di dimensione dell'oggetto troppo grande

L'avviso "Dimensione oggetto S3 PUT troppo grande" viene attivato se un tenant tenta un'operazione PutObject non multipart 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"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Determina quali tenant utilizzano oggetti di dimensioni superiori a 5 GiB, in modo da poterli avvisare.

Passi

1. Vai a **CONFIGURAZIONE > Monitoraggio > Server di audit e syslog**.
2. Se le scritture client sono normali, accedere al registro di controllo:

- a. Entra `ssh admin@primary_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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 di destinazione del controllo.

Opzione	Destinazione
Nodi locali (predefiniti)	<code>/var/local/log/localaudit.log</code>
Nodi amministrativi/nodi locali	• Nodi amministrativi (primari e non primari): <code>/var/local/audit/export/audit.log</code> • Tutti i nodi: Il <code>/var/local/log/localaudit.log</code> in questa modalità il file è solitamente vuoto o mancante.
Server syslog esterno	<code>/var/local/log/localaudit.log</code>

A seconda delle impostazioni di destinazione dell'audit, immettere: `cd /var/local/log O /var/local/audit/export/`

Per saperne di più, fare riferimento a ["Seleziona le destinazioni delle informazioni di audit"](#) .

- f. Identificare quali tenant utilizzano oggetti di dimensioni superiori a 5 GiB.
 - i. Entra `zgrep SPUT * | egrep "CSIZ\ (UI64\): ([5-9] | [1-9] [0-9]+) [0-9] {9} "`
 - ii. Per ogni messaggio di controllo nei risultati, guarda `S3AI` campo per determinare l'ID dell'account tenant. Utilizzare gli altri campi nel messaggio per determinare quale indirizzo IP è stato utilizzato dal client, dal bucket e dall'oggetto:

Codice	Descrizione
SAIP	IP sorgente

Codice	Descrizione
S3AI	ID inquilino
S3BK	Secchio
S3KY	Oggetto
CSIZ	Dimensione (byte)

Esempi 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):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][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 client non sono normali, utilizzare l'ID tenant dall'avviso per identificare il tenant:

- Vai su **SUPPORTO > Strumenti > Registri**. Raccogliere i registri delle applicazioni per il nodo di archiviazione nell'avviso. Specificare 15 minuti prima e dopo l'avviso.
- Estrarre il file e andare su `bycast.log`:

```
/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
```

- Cerca nel registro `method=PUT` e identificare il cliente nel `clientIP` campo.

Esempio 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>
```

- Informare gli inquilini che la dimensione massima di PutObject è di 5 GiB e di utilizzare caricamenti multiparte per oggetti di dimensioni superiori a 5 GiB.
- Ignorare l'avviso per una settimana se l'applicazione è stata modificata.

Risolvere i problemi relativi ai dati degli oggetti persi e mancanti

Risolvere i problemi relativi ai dati degli oggetti persi e mancanti

Gli oggetti possono essere recuperati per diversi motivi, tra cui richieste di lettura da un'applicazione client, verifiche in background dei dati degli oggetti replicati, rivalutazioni ILM e ripristino dei dati degli oggetti durante il ripristino di un nodo di archiviazione.

Il sistema StorageGRID utilizza le informazioni sulla posizione contenute nei metadati di un oggetto per determinare da quale posizione recuperare l'oggetto. Se non viene trovata una copia dell'oggetto nella posizione prevista, il sistema tenta di recuperare un'altra copia dell'oggetto da un'altra posizione nel sistema, presupponendo che la policy ILM contenga una regola per creare due o più copie dell'oggetto.

Se il recupero ha esito positivo, 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 recuperarne un'altra copia, l'oggetto viene considerato perso e viene attivato l'avviso.
- Per le copie con codice di cancellazione, se non è possibile recuperare una copia dalla posizione prevista, l'attributo ECOR (Corrupt Copies Detected) viene incrementato di uno prima che venga effettuato un tentativo di recuperare una copia da un'altra posizione. Se non viene trovata nessun'altra copia, viene attivato l'avviso.

È necessario esaminare immediatamente tutti gli avvisi di **Oggetti persi** per determinare la causa principale della perdita e per stabilire se l'oggetto potrebbe ancora esistere in un nodo di archiviazione offline o altrimenti non disponibile. Vedere ["Indagare sugli oggetti smarriti"](#).

Nel caso in cui i dati degli oggetti senza copie vengano persi, non esiste alcuna soluzione di recupero. Tuttavia, è necessario reimpostare il contatore degli oggetti persi per evitare che gli oggetti persi noti mascherino nuovi oggetti persi. Vedere ["Reimposta il conteggio degli oggetti persi e mancanti"](#).

Indagare sugli oggetti smarriti

Quando viene attivato l'avviso **Oggetti smarriti**, è necessario indagare immediatamente. Raccogliere informazioni sugli oggetti interessati e contattare l'assistenza tecnica.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).
- Devi avere il `Passwords.txt` file.

Informazioni su questo compito

L'avviso **Oggetti persi** indica che StorageGRID ritiene che non vi siano copie di un oggetto nella griglia. I dati potrebbero essere andati persi definitivamente.

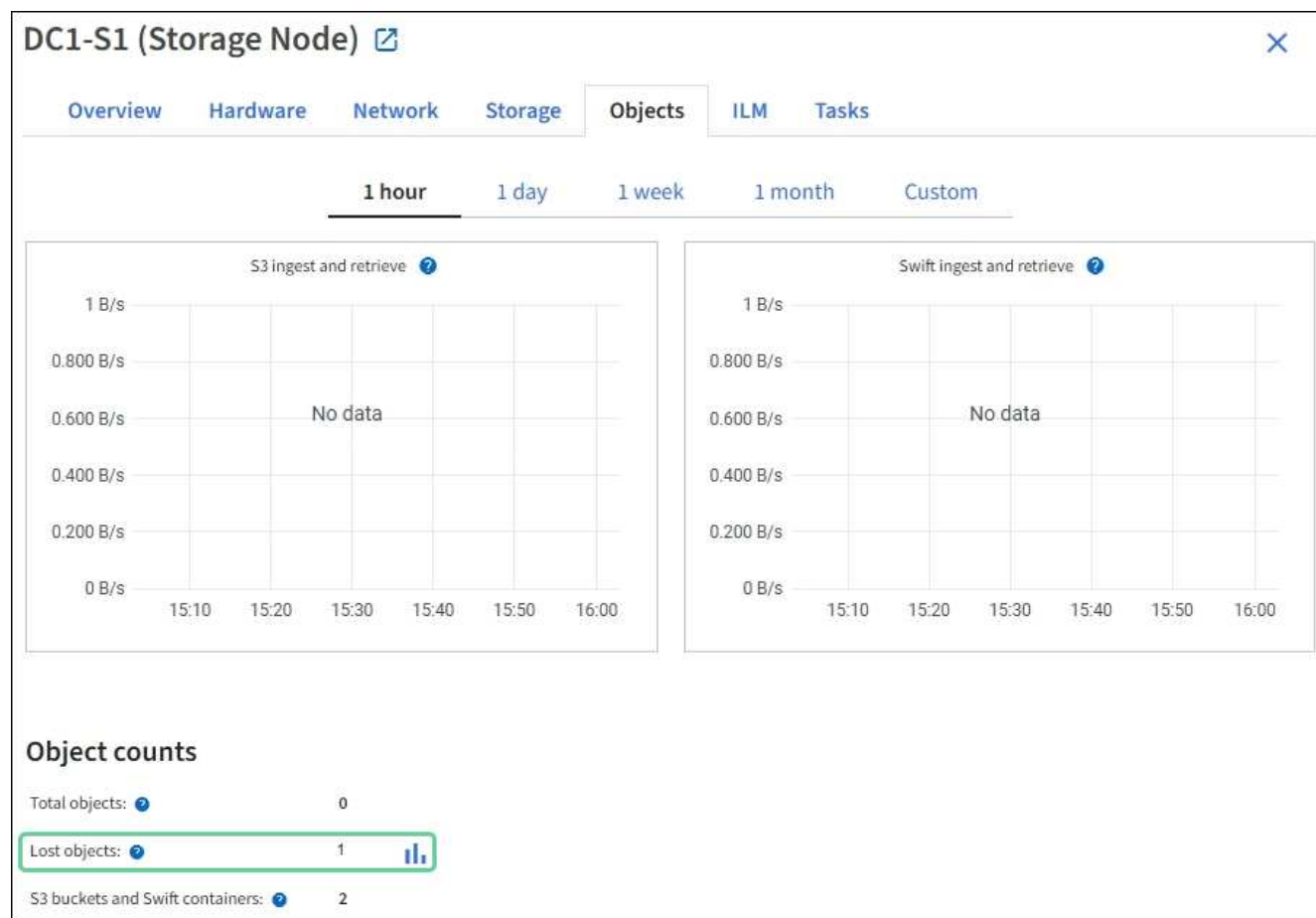
Indagare immediatamente sugli avvisi di oggetti smarriti. Potrebbe essere necessario adottare misure per evitare ulteriori perdite di dati. In alcuni casi, potresti riuscire a recuperare un oggetto smarrito se intervieni tempestivamente.

Passi

1. Selezionare **NODES**.

2. Selezionare **Nodo di archiviazione > Oggetti**.
3. Esamina il numero di oggetti smarriti mostrato nella tabella Conteggio oggetti.

Questo numero indica il numero totale di oggetti che questo nodo della griglia rileva come mancanti dall'intero sistema StorageGRID . Il valore è la somma dei contatori degli oggetti persi del componente Archivio dati all'interno dei servizi LDR e DDS.



4. Da un nodo di amministrazione, "accedere al registro di controllo" per determinare l'identificatore univoco (UUID) dell'oggetto che ha attivato l'avviso **Oggetti persi**:

a. Accedi al nodo della griglia:

i. Immettere il seguente comando: `ssh admin@grid_node_IP`

ii. Inserisci la password elencata nel `Passwords.txt` file.

iii. Immettere il seguente comando per passare alla root: `su -`

iv. Inserisci la password elencata nel `Passwords.txt` file. Quando si accede 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 di destinazione del controllo.

Opzione	Destinazione
Nodi locali (predefiniti)	/var/local/log/localaudit.log
Nodi amministrativi/nodi locali	• Nodi amministrativi (primari e non primari): /var/local/audit/export/audit.log • Tutti i nodi: Il /var/local/log/localaudit.log in questa modalità il file è solitamente vuoto o mancante.
Server syslog esterno	/var/local/log/localaudit.log

A seconda delle impostazioni di destinazione dell'audit, immettere: `cd /var/local/log O /var/local/audit/export/`

Per saperne di più, fare riferimento a ["Seleziona le destinazioni delle informazioni di audit"](#).

- Utilizzare `grep` per estrarre i messaggi di controllo Object Lost (OLST). Inserisci: `grep OLST audit_file_name`
- Prendere nota del 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. Cerca i metadati dell'oggetto smarrito utilizzando l'UUID:

- Selezionare **ILM > Ricerca metadati oggetto**.
- Inserisci l'UUID e seleziona **Cerca**.
- Esaminare le posizioni nei metadati e adottare le misure appropriate:

Metadati	Conclusione
Oggetto <identificatore_oggetto> non trovato	Se l'oggetto non viene trovato, viene restituito il messaggio "ERROR": "". Se l'oggetto non viene trovato, è possibile reimpostare il conteggio degli Oggetti persi per cancellare l'avviso. La mancanza di un oggetto indica che l'oggetto è stato eliminato intenzionalmente.

Metadati	Conclusione
Posizioni > 0	Se nell'output sono elencate delle posizioni, l'avviso Oggetti persi potrebbe essere un falso positivo. Conferma che gli oggetti esistono. Utilizzare l'ID nodo e il percorso file elencati nell'output per confermare che il file oggetto si trova nella posizione indicata. (La procedura per "ricerca di oggetti potenzialmente persi" spiega come utilizzare l'ID nodo per trovare il nodo di archiviazione corretto.) Se gli oggetti esistono, puoi reimpostare il conteggio degli Oggetti persi per cancellare l'avviso.
Posizioni = 0	Se nell'output non sono elencate posizioni, l'oggetto potrebbe essere mancante. Puoi provare a "cercare e ripristinare l'oggetto" oppure puoi contattare l'assistenza tecnica. L'assistenza tecnica potrebbe chiederti di verificare se è in corso una procedura di ripristino dell'archiviazione. Vedi le informazioni su "ripristino dei dati degli oggetti tramite Grid Manager" E "ripristino dei dati dell'oggetto su un volume di archiviazione".

Cercare e ripristinare oggetti potenzialmente persi

Potrebbe essere possibile trovare e ripristinare gli oggetti che hanno attivato un avviso di **Oggetto smarrito** e un allarme legacy di Oggetti smarriti (LOST) e che hai identificato come potenzialmente smarriti.

Prima di iniziare

- Hai l'UUID di qualsiasi oggetto smarrito, come identificato in "[Indagare sugli oggetti smarriti](#)".
- Tu hai il `Passwords.txt` file.

Informazioni su questo compito

È possibile seguire questa procedura per cercare copie replicate dell'oggetto smarrito in altre parti della griglia. Nella maggior parte dei casi, l'oggetto smarrito non verrà ritrovato. Tuttavia, in alcuni casi, potresti riuscire a trovare e ripristinare un oggetto replicato perso se intervieni tempestivamente.



Per ricevere assistenza su questa procedura, contattare l'assistenza tecnica.

Passi

1. Da un nodo di amministrazione, cerca nei registri di controllo le possibili posizioni degli oggetti:
 - a. Accedi al nodo della griglia:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla root: `su -`

iv. Inserisci la password elencata nel `Passwords.txt` file. Quando si accede 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 di destinazione del controllo.

Opzione	Destinazione
Nodi locali (predefiniti)	<code>/var/local/log/localaudit.log</code>
Nodi amministrativi/nodi locali	• Nodi amministrativi (primari e non primari): <code>/var/local/audit/export/audit.log</code> • Tutti i nodi: Il <code>/var/local/log/localaudit.log</code> in questa modalità il file è solitamente vuoto o mancante.
Server syslog esterno	<code>/var/local/log/localaudit.log</code>

A seconda delle impostazioni di destinazione dell'audit, immettere: `cd /var/local/log` O `/var/local/audit/export/`

Per saperne di più, fare riferimento a ["Seleziona le destinazioni delle informazioni di audit"](#).

c. Utilizzare `grep` per estrarre il ["messaggi di controllo associati all'oggetto potenzialmente perso"](#) e inviarli a un file di output. Inserisci: `grep uuid-value audit_file_name > output_file_name`

Per 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. Inserisci: `grep LLST output_file_name`

Per 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
86871083190743409]]
```

e. Trovare il campo PCLD e il campo NOID nel messaggio LLST.

Se presente, il valore di PCLD è il percorso completo su disco alla copia dell'oggetto replicato mancante. Il valore di NOID è l'ID del nodo dell'LDR in cui potrebbe essere trovata una copia dell'oggetto.

Se trovi la posizione di un oggetto, potresti riuscire a ripristinarlo.

a. Trova il nodo di archiviazione associato a questo ID nodo LDR. In Grid Manager, seleziona **SUPPORTO > Strumenti > Topologia griglia**. Quindi selezionare **Data Center > Storage Node > LDR**.

L'ID nodo per il servizio LDR si trova nella tabella Informazioni nodo. Esaminare le informazioni per ciascun nodo di archiviazione fino a trovare quello che ospita questo LDR.

2. Determinare se l'oggetto esiste sul nodo di archiviazione indicato nel messaggio di controllo:

a. Accedi al nodo della griglia:

- i. Immettere il seguente comando: `ssh admin@grid_node_IP`
- ii. Inserisci la password elencata nel `Passwords.txt` file.
- iii. Immettere il seguente comando per passare alla root: `su -`
- iv. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

b. Determina se esiste il percorso del file per l'oggetto.

Per il percorso del file dell'oggetto, utilizzare il valore di PCLD dal messaggio di controllo LLST.

Ad esempio, inserisci:

```
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 evitare caratteri speciali.

- Se il percorso dell'oggetto non viene trovato, l'oggetto viene perso e non può essere ripristinato utilizzando questa procedura. Contattare l'assistenza tecnica.
- Se il percorso dell'oggetto viene trovato, procedere con il passaggio successivo. È possibile

provare a ripristinare l'oggetto trovato in StorageGRID.

3. Se il percorso dell'oggetto è stato trovato, provare a ripristinare l'oggetto in StorageGRID:
 - a. Dallo stesso nodo di archiviazione, modificare la proprietà del file oggetto in modo che possa essere gestito da StorageGRID. Inserisci: `chown ldr-user:bycast 'file_path_of_object'`
 - b. Per accedere alla console LDR, effettuare il login tramite Telnet a localhost 1402. Inserisci: `telnet 0 1402`
 - c. Inserisci: `cd /proc/STOR`
 - d. Inserisci: `Object_Found 'file_path_of_object'`

Ad esempio, inserisci:

```
Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Emissione del Object_Found Il comando notifica alla griglia la posizione dell'oggetto. Attiva inoltre le policy ILM attive, che creano copie aggiuntive come specificato in ciascuna policy.



Se il nodo di archiviazione in cui hai trovato l'oggetto è offline, puoi copiare l'oggetto in qualsiasi nodo di archiviazione online. Posizionare l'oggetto in una qualsiasi directory `/var/local/rangedb` del nodo di archiviazione online. Quindi, emettere il `Object_Found` comando utilizzando quel percorso file all'oggetto.

- Se l'oggetto non può essere ripristinato, il `Object_Found` il comando fallisce. Contattare l'assistenza tecnica.
- Se l'oggetto è stato ripristinato correttamente su StorageGRID, viene visualizzato un messaggio di conferma. Per 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'
```

Proseguì con il passaggio successivo.

4. Se l'oggetto è stato ripristinato correttamente in StorageGRID, verificare che siano state create le nuove posizioni:
 - a. Sign in a Grid Manager utilizzando un ["browser web supportato"](#).
 - b. Selezionare **ILM > Ricerca metadati oggetto**.
 - c. Inserisci l'UUID e seleziona **Cerca**.
 - d. Esaminare i metadati e verificare le nuove posizioni.
5. Da un nodo di amministrazione, cercare nei registri di controllo il messaggio di controllo ORLM per questo oggetto per confermare che la gestione del ciclo di vita delle informazioni (ILM) abbia inserito le copie

come richiesto.

a. Accedi al nodo della griglia:

- i. Immettere il seguente comando: `ssh admin@grid_node_IP`
- ii. Inserisci la password elencata nel `Passwords.txt` file.
- iii. Immettere il seguente comando per passare alla root: `su -`
- iv. Inserisci la password elencata nel `Passwords.txt` file. Quando si accede come root, il prompt cambia da `$` a `#`.

b. Passare alla directory in cui si trovano i registri di controllo. Fare riferimento [asottofase 1. b](#).

c. Utilizzare `grep` per estrarre i messaggi di controllo associati all'oggetto in un file di output. Inserisci:
`grep uuid-value audit_file_name > output_file_name`

Per 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 controllo Object Rules Met (ORLM) da questo file di output. Inserisci: `grep ORLM output_file_name`

Per 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. Trova il campo `LOCS` nel messaggio di controllo.

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 dell'oggetto in due posizioni nella griglia.

6. ["Azzerare il conteggio degli oggetti persi e mancanti"](#) nel Grid Manager.

Reimposta il conteggio degli oggetti persi e mancanti

Dopo aver esaminato il sistema StorageGRID e verificato che tutti gli oggetti persi registrati sono andati persi definitivamente o che si tratta di un falso allarme, è possibile reimpostare il valore dell'attributo Oggetti persi su zero.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai "[autorizzazioni di accesso specifiche](#)".

Informazioni su questo compito

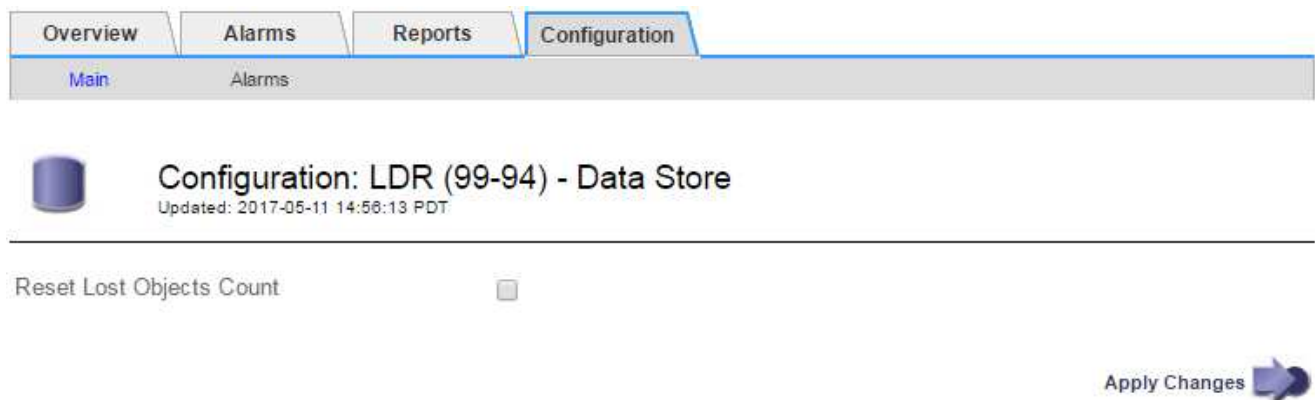
È possibile azzerare il contatore degli oggetti smarriti da una delle seguenti pagine:

- **SUPPORTO > Strumenti > Topologia griglia > Sito > Nodo di archiviazione > LDR > Archivio dati > Panoramica > Principale**
- **SUPPORTO > Strumenti > Topologia griglia > Sito > Nodo di archiviazione > DDS > Archivio dati > Panoramica > Principale**

Queste istruzioni mostrano come reimpostare il contatore dalla pagina **LDR > Data Store**.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **Sito > Nodo di archiviazione > LDR > Archivio dati > Configurazione** per il nodo di archiviazione che presenta l'avviso **Oggetti persi** o l'allarme **PERSO**.
3. Seleziona **Reimposta conteggio oggetti smarriti**.



4. Fare clic su **Applica modifiche**.

L'attributo Oggetti smarriti viene reimpostato su 0 e l'avviso **Oggetti smarriti** e l'allarme **SMARRITO** vengono cancellati, operazione che può richiedere alcuni minuti.

5. Facoltativamente, reimpostare altri valori di attributi correlati che potrebbero essere stati incrementati durante il processo di identificazione dell'oggetto smarrito.
 - a. Selezionare **Sito > Nodo di archiviazione > LDR > Codifica di cancellazione > Configurazione**.
 - b. Selezionare **Reimposta conteggio errori di lettura** e **Reimposta conteggio copie danneggiate rilevate**.
 - c. Fare clic su **Applica modifiche**.

- d. Selezionare **Sito > Nodo di archiviazione > LDR > Verifica > Configurazione**.
- e. Selezionare **Reimposta conteggio oggetti mancanti e Reimposta conteggio oggetti danneggiati**.
- f. Se sei sicuro che gli oggetti in quarantena non siano necessari, puoi selezionare **Elimina oggetti in quarantena**.

Gli oggetti in quarantena vengono creati quando la verifica in background identifica una copia di un oggetto replicato corrotta. Nella maggior parte dei casi StorageGRID sostituisce automaticamente l'oggetto danneggiato ed è possibile eliminare in sicurezza gli oggetti in quarantena. Tuttavia, se viene attivato l'avviso **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 **Applica modifiche**, potrebbero essere necessari alcuni istanti prima che gli attributi vengano reimpostati.

Risoluzione dei problemi relativi all'avviso di spazio di archiviazione dati dell'oggetto insufficiente

L'avviso **Archiviazione dati oggetto insufficiente** monitora la quantità di spazio disponibile per l'archiviazione dei dati oggetto su ciascun nodo di archiviazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Informazioni su questo compito

L'avviso **Archiviazione dati oggetto insufficiente** viene attivato quando la quantità totale di dati oggetto replicati e codificati per la cancellazione 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 vera:

```
(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 della dimensione totale dei dati degli oggetti replicati e codificati per la cancellazione per un nodo di archiviazione.
- ``storagegrid_storage_utilization_usable_space_bytes`` è la quantità totale di spazio di archiviazione degli oggetti rimanente per un nodo di archiviazione.

Se viene attivato un avviso di **Archiviazione dati oggetto insufficiente**, importante o minore, è necessario eseguire una procedura di espansione il prima possibile.

Passi

1. Selezionare **AVVISI > Correnti**.

Viene visualizzata la pagina Avvisi.

2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Archiviazione dati oggetto insufficiente**, se necessario, e selezionare l'avviso che si desidera visualizzare.

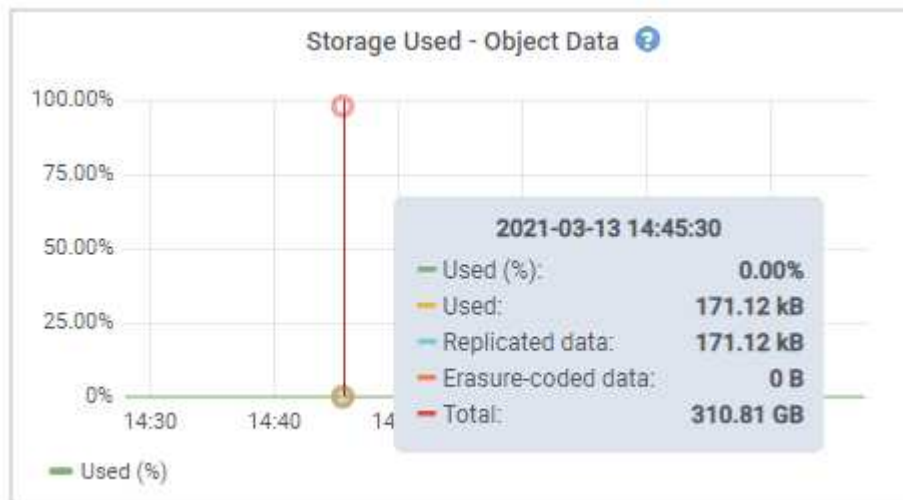


Selezionare l'avviso, non l'intestazione di un gruppo di avvisi.

3. Esaminare i dettagli nella finestra di dialogo e notare quanto segue:
 - Tempo attivato
 - Il nome del sito e del nodo
 - I valori correnti delle metriche per questo avviso
4. Selezionare **NODI > Nodo o sito di archiviazione_ > Archiviazione**.
5. Posiziona il cursore sul grafico Spazio di archiviazione utilizzato - Dati oggetto.

Vengono mostrati i seguenti valori:

- **Utilizzato (%)**: la percentuale dello spazio utilizzabile totale che è stata utilizzata per i dati dell'oggetto.
- **Utilizzato**: quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
- **Dati replicati**: una stima della quantità di dati di oggetti replicati su questo nodo, sito o griglia.
- **Dati con codice di cancellazione**: una stima della quantità di dati di oggetti con codice di cancellazione su questo nodo, sito o griglia.
- **Totale**: quantità totale di spazio utilizzabile su questo nodo, sito o griglia. Il valore utilizzato è il `storagegrid_storage_utilization_data_bytes` metrica.



6. Selezionare i controlli temporali sopra il grafico per visualizzare l'utilizzo dello spazio di archiviazione in diversi periodi di tempo.

Esaminare l'utilizzo dello spazio di archiviazione nel tempo può aiutare a capire quanto spazio di archiviazione è stato utilizzato prima e dopo l'attivazione dell'avviso e può aiutare a stimare quanto tempo potrebbe essere necessario affinché lo spazio rimanente del nodo si riempia.

7. Appena possibile, ["aggiungere capacità di archiviazione"](#) alla tua griglia.

È possibile aggiungere volumi di archiviazione (LUN) ai nodi di archiviazione esistenti oppure aggiungere nuovi nodi di archiviazione.



Per ulteriori informazioni, consultare ["Gestisci nodi di archiviazione completi"](#).

Risoluzione dei problemi relativi agli avvisi di override della filigrana di sola lettura bassa

Se si utilizzano valori personalizzati per le filigrane del volume di archiviazione, potrebbe essere necessario risolvere l'avviso **Sostituzione filigrana di sola lettura bassa**. Se possibile, dovresti aggiornare il tuo sistema per iniziare a utilizzare i valori ottimizzati.

Nelle versioni precedenti, i tre ["filigrane del volume di archiviazione"](#) erano impostazioni globali, ovvero gli stessi valori applicati a ogni volume di archiviazione su ogni nodo di archiviazione. A partire da StorageGRID 11.6, il software è in grado di ottimizzare queste filigrane per ciascun volume di archiviazione, in base alle dimensioni del nodo di archiviazione e alla capacità relativa del volume.

Quando si esegue l'aggiornamento a StorageGRID 11.6 o versione successiva, le filigrane ottimizzate di sola lettura e di lettura-scrittura vengono applicate automaticamente a tutti i volumi di archiviazione, a meno che non si verifichi una delle seguenti condizioni:

- Il sistema è prossimo alla capacità massima e non sarebbe in grado di accettare nuovi dati se fossero applicate filigrane ottimizzate. In questo caso StorageGRID non modificherà le impostazioni della filigrana.
- In precedenza hai impostato una qualsiasi delle filigrane del volume di archiviazione su un valore personalizzato. StorageGRID non sovrascriverà le impostazioni personalizzate della filigrana con valori ottimizzati. Tuttavia, StorageGRID potrebbe attivare l'avviso **Sostituzione filigrana di sola lettura bassa** se il valore personalizzato per la filigrana di sola lettura software del volume di archiviazione è troppo piccolo.

Comprendere l'avviso

Se si utilizzano valori personalizzati per le filigrane del volume di archiviazione, potrebbe essere attivato l'avviso **Sostituzione filigrana di sola lettura bassa** per uno o più nodi di archiviazione.

Ogni istanza dell'avviso indica che il valore personalizzato della filigrana di sola lettura software del volume di archiviazione è inferiore al valore minimo ottimizzato per quel nodo di archiviazione. Se si continua a utilizzare l'impostazione personalizzata, lo spazio disponibile sul nodo di archiviazione potrebbe esaurirsi prima di poter passare in sicurezza allo stato di sola lettura. Alcuni volumi di archiviazione potrebbero diventare inaccessibili (smontati automaticamente) quando il nodo raggiunge la capacità massima.

Ad esempio, supponiamo di aver precedentemente impostato la filigrana di sola lettura software del volume di archiviazione su 5 GB. Supponiamo ora che StorageGRID abbia calcolato i seguenti valori ottimizzati per i quattro volumi di archiviazione nel nodo di archiviazione A:

Volume 0	12 GB
Volume 1	12 GB
Volume 2	11 GB
Volume 3	15 GB

L'avviso **Sostituzione filigrana di sola lettura bassa** viene attivato per il nodo di archiviazione A perché la filigrana personalizzata (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 disponibile sul nodo potrebbe esaurirsi prima di poter passare in sicurezza allo stato di sola lettura.

Risolvi l'avviso

Seguire questi passaggi se sono stati attivati uno o più avvisi di **sostituzione della filigrana di sola lettura bassa**. Puoi utilizzare queste istruzioni anche se attualmente utilizzi impostazioni di filigrana personalizzate e desideri iniziare a utilizzare impostazioni ottimizzate anche se non sono stati attivati avvisi.

Prima di iniziare

- Hai completato l'aggiornamento a StorageGRID 11.6 o versione successiva.
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .

Informazioni su questo compito

È possibile risolvere l'avviso **Sostituzione filigrana di sola lettura bassa** aggiornando le impostazioni della filigrana personalizzata con le nuove sostituzioni filigrana. Tuttavia, se uno o più nodi di archiviazione sono quasi pieni o si hanno requisiti ILM speciali, è necessario prima visualizzare le filigrane di archiviazione ottimizzate e determinare se è sicuro utilizzarle.

Valutare l'utilizzo dei dati degli oggetti per l'intera griglia

Passi

1. Selezionare **NODES**.
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 archiviazione in ogni sito.

Nodes

View the list and status of sites and grid nodes.

Search... Q Total node count: 13

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
! DC1-SN1	Storage Node	71%	3%	30%
! DC1-SN2	Storage Node	25%	3%	42%
! DC1-SN3	Storage Node	63%	3%	42%
! DC1-SN4	Storage Node	65%	3%	41%

4. Seguire il passaggio appropriato:

- Se nessuno dei nodi di archiviazione è quasi pieno (ad esempio, tutti i valori dei **dati oggetto utilizzati** sono inferiori all'80%), è possibile iniziare a utilizzare le impostazioni di override. Vai a [Utilizza filigrane ottimizzate](#).
- Se le regole ILM utilizzano un comportamento di acquisizione rigoroso o se specifici pool di archiviazione sono quasi pieni, eseguire i passaggi in [Visualizza le filigrane di archiviazione ottimizzate](#) e [Determina se puoi utilizzare filigrane ottimizzate](#).

Visualizza le filigrane di archiviazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati calcolati per la filigrana di sola lettura software del volume di archiviazione. È possibile visualizzare i valori ottimizzati minimi e massimi per ciascun nodo di archiviazione nella griglia.

Passi

- Selezionare **SUPPORTO > Strumenti > Metriche**.
- Nella sezione Prometheus, seleziona il collegamento per accedere all'interfaccia utente di Prometheus.
- Per visualizzare il watermark minimo consigliato per la sola lettura software, 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 software per tutti i volumi

di archiviazione su ciascun nodo di archiviazione. Se questo valore è maggiore dell'impostazione personalizzata per la filigrana di sola lettura software del volume di archiviazione, viene attivato l'avviso **Sostituzione filigrana di sola lettura insufficiente** per il nodo di archiviazione.

4. Per visualizzare il limite massimo consigliato per la sola lettura software, 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 software per tutti i volumi di archiviazione su ciascun nodo di archiviazione.

5. Nota il valore massimo ottimizzato per ogni nodo di archiviazione.

Determina se puoi utilizzare watermark ottimizzati

Passi

1. Selezionare **NODES**.
2. Ripetere questi passaggi per ogni nodo di archiviazione online:
 - a. Selezionare **Nodo di archiviazione > Archiviazione**.
 - b. Scorrere verso il basso fino alla tabella Archivi oggetti.
 - c. Confronta il valore **Disponibile** per ciascun archivio oggetti (volume) con il limite massimo ottimizzato annotato per quel nodo di archiviazione.
3. Se almeno un volume su ogni nodo di archiviazione online ha più spazio disponibile rispetto al limite massimo ottimizzato per quel nodo, vai a [Utilizza filigrane ottimizzate](#) per iniziare a utilizzare le filigrane ottimizzate.

Altrimenti, espandi la griglia il prima possibile. O "[aggiungere volumi di archiviazione](#)" a un nodo esistente o "[aggiungere nuovi nodi di archiviazione](#)". Poi vai a [Utilizza filigrane ottimizzate](#) per aggiornare le impostazioni della filigrana.

4. Se è necessario continuare a utilizzare valori personalizzati per le filigrane del volume di archiviazione, "[silenzio](#)" O "[disabilitare](#)" l'avviso **Sostituzione filigrana di sola lettura bassa**.



Gli stessi valori di filigrana personalizzati vengono applicati a ogni volume di archiviazione su ogni nodo di archiviazione. L'utilizzo di valori inferiori a quelli consigliati per le filigrane del volume di archiviazione potrebbe causare l'inaccessibilità di alcuni volumi di archiviazione (smontaggio automatico) quando il nodo raggiunge la capacità massima.

Usa filigrane ottimizzate

Passi

1. Vai a **SUPPORTO > Altro > Filigrane di archiviazione**.
2. Selezionare la casella di controllo **Usa valori ottimizzati**.
3. Seleziona **Salva**.

Le impostazioni ottimizzate della filigrana del volume di archiviazione sono ora attive per ogni volume di archiviazione, in base alle dimensioni del nodo di archiviazione e alla capacità relativa del volume.

Risolvere i problemi relativi ai metadati

Se si verificano problemi con i metadati, gli avvisi ti informeranno sulla fonte dei problemi e sulle azioni consigliate da intraprendere. In particolare, è necessario aggiungere nuovi nodi di archiviazione se viene attivato l'avviso di spazio di archiviazione dei metadati insufficiente.

Prima di iniziare

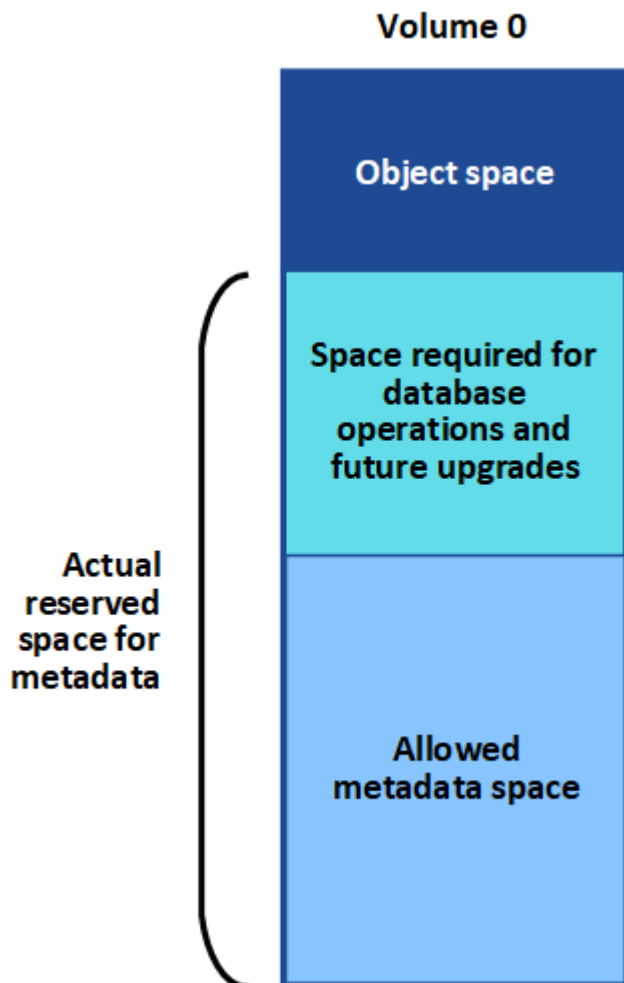
Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

Informazioni su questo compito

Seguire le azioni consigliate per ogni avviso correlato ai metadati attivato. Se viene attivato l'avviso

Archiviazione metadati insufficiente, è necessario aggiungere nuovi nodi di archiviazione.

StorageGRID riserva una certa quantità di spazio sul volume 0 di ciascun nodo di archiviazione per i metadati degli oggetti. Questo spazio, noto come *spazio riservato effettivo*, è suddiviso nello spazio consentito per i metadati degli oggetti (spazio dei metadati consentito) e nello spazio richiesto per le operazioni essenziali del database, come la compattazione e la riparazione. Lo spazio dei metadati consentito regola la capacità complessiva dell'oggetto.



Se i metadati degli oggetti occupano più del 100% dello spazio consentito per i metadati, le operazioni del database non possono essere eseguite in modo efficiente e si verificheranno degli errori.

Puoi [monitorare la capacità dei metadati degli oggetti per ogni nodo di archiviazione](#) per aiutarti ad anticipare gli errori e correggerli prima che si verifichino.

StorageGRID utilizza la seguente metrica Prometheus per misurare il livello di riempimento dello spazio metadati consentito:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Quando questa espressione di Prometheus raggiunge determinate soglie, viene attivato l'avviso **Archiviazione metadati insufficiente**.

- **Minore:** i metadati dell'oggetto utilizzano il 70% o più dello spazio metadati consentito. Dovresti aggiungere nuovi nodi di archiviazione il prima possibile.
- **Maggiore:** i metadati dell'oggetto utilizzano il 90% o più dello spazio metadati consentito. È necessario aggiungere immediatamente nuovi nodi di archiviazione.



Quando i metadati degli oggetti utilizzano il 90% o più dello spazio metadati consentito, nella dashboard viene visualizzato un avviso. Se viene visualizzato questo avviso, è necessario aggiungere immediatamente nuovi nodi di archiviazione. Non devi mai consentire che i metadati degli oggetti utilizzino più del 100% dello spazio consentito.

- **Critico:** i metadati degli oggetti utilizzano il 100% o più dello spazio metadati 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 archiviazione.



Se la dimensione del volume 0 è inferiore all'opzione di archiviazione Spazio riservato ai metadati (ad esempio, in un ambiente non di produzione), il calcolo per l'avviso **Archiviazione metadati insufficiente** potrebbe essere impreciso.

Passi

1. Selezionare **AVVISI > Correnti**.
2. Dalla tabella degli avvisi, espandi il gruppo di avvisi **Archiviazione metadati insufficiente**, se necessario, e seleziona l'avviso specifico che desideri visualizzare.
3. Esaminare i dettagli nella finestra di dialogo di avviso.
4. Se è stato attivato un avviso importante o critico di **Archiviazione metadati insufficiente**, eseguire immediatamente un'espansione per aggiungere nodi di archiviazione.



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 hai bisogno di aggiungere capacità di metadati a un sito, dovresti anche [espandere altri siti](#) dallo stesso numero di nodi di archiviazione.

Dopo aver eseguito l'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti ai nuovi nodi, aumentando così la capacità complessiva dei metadati della griglia. Non è richiesta alcuna azione da parte dell'utente. L'avviso **Spazio di archiviazione metadati insufficiente** è stato cancellato.

Risolvere gli errori del certificato

Se riscontri un problema di sicurezza o di certificato quando provi a connetterti a StorageGRID tramite un browser Web, un client S3 o uno strumento di monitoraggio esterno, dovresti controllare il certificato.

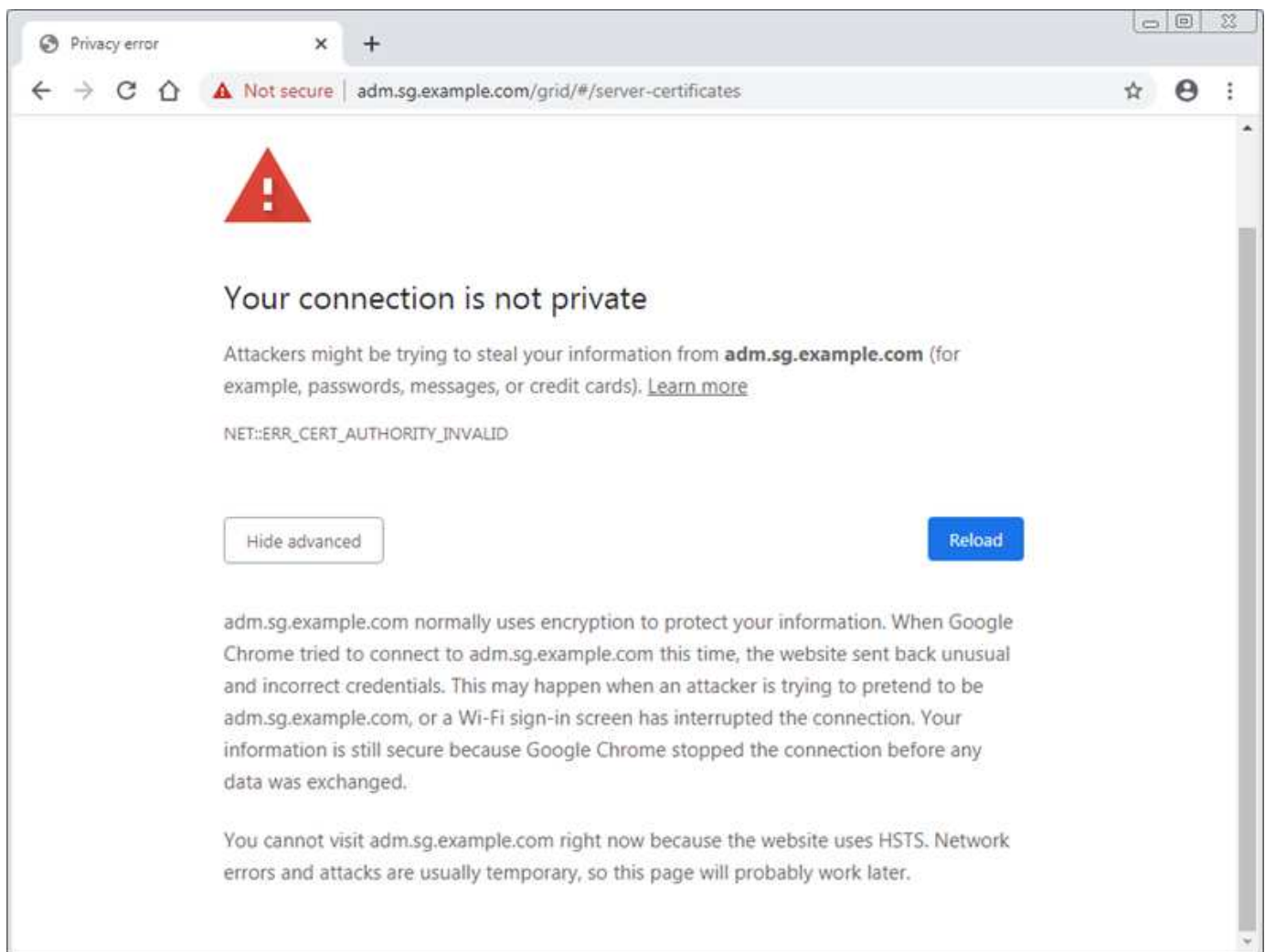
Informazioni su questo compito

Gli errori del certificato possono causare problemi quando si tenta di connettersi a StorageGRID tramite Grid Manager, Grid Management API, Tenant Manager o Tenant Management API. Gli errori del certificato possono verificarsi anche quando si tenta di connettersi a un client S3 o a uno strumento di monitoraggio esterno.

Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio anziché un indirizzo IP, il browser visualizza un errore di certificato senza un'opzione per ignorarlo se si verifica una delle seguenti situazioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Si passa da un certificato di interfaccia di gestione personalizzato al certificato del server predefinito.

L'esempio seguente mostra un errore del certificato quando il certificato dell'interfaccia di gestione personalizzata è scaduto:



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza**

del certificato server per l'interfaccia di gestione viene attivato quando il certificato 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 StorageGRID o dai certificati client. L'avviso **Scadenza dei certificati client configurati nella pagina Certificati** viene attivato quando un certificato client sta per scadere.

Passi

Se hai ricevuto una notifica di avviso relativa a un certificato scaduto, accedi ai dettagli del certificato: . Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi ["seleziona la scheda del certificato appropriata"](#) .

1. Verificare il periodo di validità del certificato. + Alcuni browser Web e client S3 non accettano certificati con un periodo di validità superiore a 398 giorni.
2. Se il certificato è scaduto o scadrà a breve, carica o genera un nuovo certificato.
 - Per un certificato del server, vedere i passaggi per ["configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#) .
 - Per un certificato client, vedere i passaggi per ["configurazione di un certificato client"](#) .
3. Per gli errori del certificato del server, provare una o entrambe le seguenti opzioni:
 - Assicurarsi che il nome alternativo del soggetto (SAN) del certificato sia compilato e che il SAN corrisponda all'indirizzo IP o al nome host del nodo a cui ci si sta connettendo.
 - Se si tenta di connettersi a StorageGRID utilizzando un nome di dominio:
 - i. Immettere l'indirizzo IP del nodo di amministrazione anziché il nome di dominio per aggirare l'errore di connessione e accedere a Grid Manager.
 - ii. Da Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e poi ["seleziona la scheda del certificato appropriata"](#) per installare un nuovo certificato personalizzato o continuare con il certificato predefinito.
 - iii. Nelle istruzioni per l'amministrazione StorageGRID, vedere i passaggi 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 StorageGRID .

Errori di accesso al nodo di amministrazione

Se si verifica un errore durante l'accesso a un nodo di amministrazione StorageGRID , il sistema potrebbe avere un problema con un ["networking"](#) O ["hardware"](#) problema, un problema con ["Servizi del nodo di amministrazione"](#) , o un ["problema con il database Cassandra"](#) sui nodi di archiviazione connessi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il `Passwords.txt` file.
- Hai ["autorizzazioni di accesso specifiche"](#) .

Informazioni su questo compito

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 di amministrazione:

- 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...

Passi

1. Attendi 10 minuti e prova ad accedere nuovamente.

Se l'errore non viene risolto automaticamente, passare al passaggio successivo.

2. Se il sistema StorageGRID dispone di più di un nodo amministrativo, provare ad accedere a Grid Manager da un altro nodo amministrativo per verificare lo stato di un nodo amministrativo non disponibile.
 - Se riesci ad accedere, puoi utilizzare le opzioni **Dashboard**, **NODI**, **Avvisi** e **SUPPORTO** per determinare la causa dell'errore.
 - Se hai un solo nodo di amministrazione o non riesci ancora ad accedere, vai al passaggio successivo.
3. Determina se l'hardware del nodo è offline.
4. Se l'accesso singolo (SSO) è abilitato per il sistema StorageGRID , fare riferimento ai passaggi per "[configurazione dell'accesso singolo](#)" .

Potrebbe essere necessario disattivare e riattivare temporaneamente l'SSO per un singolo nodo di amministrazione per risolvere eventuali problemi.



Se l'SSO è abilitato, non è possibile effettuare l'accesso utilizzando una porta con restrizioni. È necessario utilizzare la porta 443.

5. Verifica se l'account che stai utilizzando appartiene a un utente federato.

Se l'account utente federato non funziona, prova ad accedere a Grid Manager come utente locale, ad esempio root.

- Se l'utente locale può accedere:
 - i. Rivedi gli avvisi.
 - ii. Selezionare **CONFIGURAZIONE > Controllo accessi > Federazione identità**.
 - iii. Fare clic su **Test connessione** per convalidare le impostazioni di connessione per il server LDAP.
 - iv. Se il test fallisce, correggere eventuali errori di configurazione.
- Se l'utente locale non riesce ad accedere e sei sicuro che le credenziali siano corrette, vai al passaggio successivo.

6. Utilizzare Secure Shell (ssh) per accedere al nodo di amministrazione:

- a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

7. Visualizza lo stato di tutti i servizi in esecuzione sul nodo della griglia: `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. Conferma che il servizio `nginx-gw` è in esecuzione `# service nginx-gw status`

9. Usa Lumberjack per raccogliere i tronchi: `# /usr/local/sbin/lumberjack.rb`

Se l'autenticazione non riuscita si è verificata in passato, è possibile utilizzare le opzioni dello script Lumberjack `--start` e `--end` per specificare l'intervallo di tempo appropriato. Per i dettagli su queste opzioni, utilizzare `lumberjack -h`.

L'output sul terminale indica dove è stato copiato l'archivio dei log.

10. Esamina i seguenti log:

- `/var/local/log/bycast.log`
- `/var/local/log/bycast-err.log`
- `/var/local/log/nms.log`
- `**/*commands.txt`

11. Se non è stato possibile identificare alcun problema con il nodo di amministrazione, eseguire uno dei seguenti comandi per determinare gli indirizzi IP dei tre nodi di archiviazione che eseguono il servizio ADC nel sito. In genere, si tratta dei primi tre nodi di archiviazione installati nel sito.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

I nodi amministrativi utilizzano il servizio ADC durante il processo di autenticazione.

12. Dal nodo di amministrazione, utilizzare ssh per accedere a ciascuno dei nodi di archiviazione ADC, utilizzando gli indirizzi IP identificati.

13. Visualizza lo stato di tutti i servizi in esecuzione sul nodo della griglia: `storagegrid-status`

Assicurarsi che i servizi `idnt`, `acct`, `nginx` e `cassandra` siano tutti in esecuzione.

14. Ripeti i passaggi [Usa Lumberjack per raccogliere i tronchi](#) e [Registri di revisione](#) per rivedere i registri sui nodi di archiviazione.

15. Se non riesci a risolvere il problema, contatta l'assistenza tecnica.

Fornisci i registri raccolti al supporto tecnico. Vedere anche ["Riferimento ai file di registro"](#).

Problemi dell'interfaccia utente

L'interfaccia utente di Grid Manager o Tenant Manager potrebbe non rispondere come previsto dopo l'aggiornamento del software StorageGRID.

Passi

1. Assicurati di utilizzare un ["browser web supportato"](#).
2. Svuota la cache del tuo browser web.

La cancellazione della cache rimuove le risorse obsolete utilizzate dalla versione precedente del software StorageGRID e consente all'interfaccia utente di funzionare di nuovo correttamente. Per le istruzioni, consultare la documentazione del browser web.

Risolvi i problemi di rete, hardware e piattaforma

Esistono diverse attività che è possibile svolgere per determinare l'origine dei problemi

relativi alla rete, all'hardware e alla piattaforma StorageGRID .

Errori "422: Entità non elaborabile"

L'errore 422: Entità non elaborabile può verificarsi per diversi motivi. Controlla 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 tramite Windows Active Directory (AD). L'utilizzo dell'opzione Non utilizzare TLS non è supportato per i server AD che applicano la firma LDAP. È necessario selezionare l'opzione Usa STARTTLS o l'opzione Usa LDAPS per TLS.

Messaggio di errore	Causa principale e azione correttiva
<pre>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)</pre>	Questo messaggio viene visualizzato se si tenta di utilizzare una crittografia non supportata per stabilire una connessione Transport Layer Security (TLS) da StorageGRID a un sistema esterno utilizzato per identificare la federazione o i pool di archiviazione cloud. Controllare i cifrari offerti dal sistema esterno. Il sistema deve utilizzare uno dei cifrari supportati da StorageGRID per le connessioni TLS in uscita, come mostrato nelle istruzioni per l'amministrazione StorageGRID.

Avviso di mancata corrispondenza MTU della rete di rete

L'avviso **Mancata corrispondenza MTU della rete di griglia** viene attivato quando l'impostazione dell'unità di trasmissione massima (MTU) per l'interfaccia della rete di griglia (eth0) differisce in modo significativo tra i nodi della griglia.

Informazioni su questo compito

Le differenze nelle impostazioni MTU potrebbero indicare che alcune reti eth0, ma non tutte, sono configurate per i frame jumbo. Una mancata corrispondenza delle dimensioni MTU superiore a 1000 potrebbe causare problemi di prestazioni di rete.

Passi

1. Elenca le impostazioni MTU per eth0 su tutti i nodi.
 - Utilizzare la query fornita in Grid Manager.
 - Vai a *primary Admin Node IP address/metrics/graph* e inserisci la seguente query:
`node_network_mtu_bytes{device="eth0"}`
2. ["Modificare le impostazioni MTU"](#) se 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: sui nodi basati su Linux, se il valore MTU desiderato per la rete nel contenitore 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 contenitore.

Utilizzare i seguenti argomenti per modificare l'MTU sui nodi basati su Linux o VMware.

Argomenti posizionali	Descrizione
mtu	L'MTU da impostare. Deve essere compreso tra 1280 e 9216.
network	Le reti a cui applicare l'MTU. Includere uno o più dei seguenti tipi di rete: • griglia • amministratore • cliente

+

Argomenti facoltativi	Descrizione
-h, - help	Mostra il messaggio di aiuto ed esci.
-n node, --node node	Il nodo. L'impostazione predefinita è il nodo locale.

Avviso di errore del frame di ricezione della rete del nodo

Gli avvisi di **errore frame di ricezione della rete del nodo** possono essere causati da problemi di connettività tra StorageGRID e l'hardware di rete. Questo avviso scompare da solo una volta risolto il problema sottostante.

Informazioni su questo compito

Gli avvisi di **errore frame di ricezione della rete del nodo** possono essere causati dai seguenti problemi con l'hardware di rete che si connette a StorageGRID:

- La correzione degli errori in avanti (FEC) è richiesta e non è in uso
- Mancata corrispondenza tra porta switch e MTU NIC
- Elevati tassi di errore nei collegamenti
- Sovraccarico del buffer ad anello della NIC

Passi

1. Seguire i passaggi per la risoluzione dei problemi per tutte le potenziali cause di questo avviso in base alla configurazione della rete.
2. Eseguire i seguenti passaggi a seconda della causa dell'errore:

Disallineamento FEC



Questi passaggi sono applicabili solo per gli avvisi di **Errore frame di ricezione della rete del nodo** causati dalla mancata corrispondenza FEC sugli appliance StorageGRID .

- a. Controllare lo stato FEC della porta nello switch collegato al dispositivo StorageGRID .
- b. Controllare l'integrità fisica dei cavi dall'apparecchio all'interruttore.
- c. Se si desidera modificare le impostazioni FEC per provare a risolvere l'avviso, assicurarsi innanzitutto che l'appliance sia configurata per la modalità **Auto** nella pagina Configurazione collegamento del programma di installazione dell'appliance StorageGRID (vedere le istruzioni per l'appliance):
 - "SG6160"
 - "SGF6112"
 - "SG6000"
 - "SG5800"
 - "SG5700"
 - "SG110 e SG1100"
 - "SG100 e SG1000"
- d. Modificare le impostazioni FEC sulle porte dello switch. Se possibile, le porte dell'appliance StorageGRID regoleranno le proprie impostazioni FEC per adattarle.

Non è possibile configurare le impostazioni FEC sugli appliance StorageGRID . Al contrario, gli apparecchi tentano di scoprire e rispecchiare le impostazioni FEC sulle porte dello switch a cui sono collegati. Se i collegamenti vengono forzati a velocità di rete pari a 25 GbE o 100 GbE, lo switch e la scheda di rete potrebbero non riuscire a negoziare un'impostazione FEC comune. Senza un'impostazione FEC comune, la rete tornerà alla modalità "no-FEC". Quando la funzione FEC non è abilitata, le connessioni sono più soggette a errori causati da disturbi elettrici.



Gli apparecchi StorageGRID supportano Firecode (FC) e Reed Solomon (RS) FEC, ma anche nessun FEC.

Mancata corrispondenza tra porta switch e MTU NIC

Se l'avviso è causato da una mancata corrispondenza tra la porta dello switch e l'MTU della scheda di rete, verificare che la dimensione dell'MTU configurata sul nodo sia la stessa dell'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 suo MTU, cosa possibile con questa configurazione, potrebbe essere segnalato l'avviso **Errore frame ricezione rete nodo**. Se ritieni che questo sia ciò che sta accadendo, modifica l'MTU della porta dello switch in modo che corrisponda all'MTU dell'interfaccia di rete StorageGRID oppure modifica l'MTU dell'interfaccia di rete StorageGRID in modo che corrisponda alla porta dello switch, a seconda degli obiettivi o dei requisiti MTU end-to-end.



Per ottenere le migliori prestazioni di rete, tutti i nodi devono essere configurati con valori MTU simili sulle loro interfacce Grid Network. L'avviso **Mancata corrispondenza MTU della rete Grid** viene attivato se si verifica una differenza significativa nelle impostazioni MTU per la rete Grid sui singoli nodi. I valori MTU non devono essere gli stessi per tutti i tipi di rete. Vedere [Risoluzione dei problemi relativi all'avviso di mancata corrispondenza dell'MTU della rete Grid](#) per maggiori informazioni.



Vedi anche ["Cambia l'impostazione MTU"](#).

Elevati tassi di errore nei collegamenti

- a. Abilitare FEC, se non è già abilitato.
- 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 la causa del problema, contattare l'assistenza tecnica.



In un ambiente con un elevato rumore elettrico, è possibile che si riscontrino alti tassi di errore.

Sovraccarico del buffer ad anello della NIC

Se l'errore è un sovraccarico del buffer ad anello della NIC, contattare l'assistenza tecnica.

Il buffer ad anello può essere superato quando il sistema StorageGRID è sovraccarico e non è in grado di elaborare tempestivamente gli eventi di rete.

3. Monitorare il problema e contattare l'assistenza tecnica se l'avviso non si risolve.

Errori di sincronizzazione dell'ora

Potresti riscontrare problemi con la sincronizzazione oraria nella tua griglia.

Se si verificano problemi di sincronizzazione temporale, verificare di aver specificato almeno quattro sorgenti NTP esterne, ciascuna delle quali fornisca un riferimento Stratum 3 o superiore, e che tutte le sorgenti NTP esterne funzionino normalmente e siano accessibili dai nodi StorageGRID.



Quando ["specificando la sorgente NTP esterna"](#) per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Ora di Windows (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio orario delle versioni precedenti di Windows non è sufficientemente preciso e non è supportato da Microsoft per l'uso in ambienti ad alta precisione, come StorageGRID.

Linux: problemi di connettività di rete

Potrebbero verificarsi problemi con la connettività di rete per i nodi StorageGRID ospitati su host Linux.

Clonazione dell'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 delle reti su "true" nel file di configurazione del nodo. Questa impostazione fa sì che l'indirizzo MAC del contenitore StorageGRID utilizzi l'indirizzo MAC dell'host. Per creare file di configurazione del nodo, vedere le istruzioni

per ["Red Hat Enterprise Linux"](#) O ["Ubuntu o Debian"](#) .



Creare interfacce di rete virtuali separate da utilizzare da parte del sistema operativo host Linux. L'utilizzo delle stesse interfacce di rete per il sistema operativo host Linux e il contenitore StorageGRID potrebbe rendere il sistema operativo host irraggiungibile se la modalità promiscua non è stata abilitata sull'hypervisor.

Per ulteriori informazioni sull'abilitazione della clonazione MAC, vedere le istruzioni per ["Red Hat Enterprise Linux"](#) O ["Ubuntu o Debian"](#) .

Modalità promiscua

Se non si desidera utilizzare la clonazione degli indirizzi MAC e si preferisce 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 **Accetta** per Modalità promiscua, Modifiche indirizzo MAC e Trasmissioni contraffatte. 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 entrambi i punti.

Per ulteriori informazioni sull'utilizzo della modalità promiscua, consultare le istruzioni per ["Red Hat Enterprise Linux"](#) O ["Ubuntu o Debian"](#) .

Linux: lo stato del nodo è "orfano"

Un nodo Linux in stato orfano indica solitamente che il servizio StorageGRID o il demone del nodo StorageGRID che controlla il contenitore del nodo è morto inaspettatamente.

Informazioni su questo compito

Se un nodo Linux segnala di trovarsi in uno stato orfano, è necessario:

- Controllare i registri per errori e messaggi.
- Provare a riavviare il nodo.
- Se necessario, utilizzare i comandi del motore del contenitore per arrestare il contenitore del nodo esistente.
- Riavviare il nodo.

Passi

1. Controllare i registri sia del demone di servizio che del nodo orfano per individuare errori evidenti o messaggi relativi a un'uscita imprevista.
2. Accedi all'host come root o utilizzando un account con autorizzazione sudo.
3. Provare a 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 del contenitore e tutti i processi di controllo storagegrid-node. Ad esempio:

```
sudo docker stop --time secondscontainer-name
```

Per `seconds`, immettere il numero di secondi che si desidera attendere affinché il contenitore si arresti (in genere 15 minuti o meno). Per 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 di 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 dei nodi come previsto.

Informazioni su questo compito

Per visualizzare l'indirizzo IPv6 assegnato a un nodo della griglia:

1. Selezionare **NODI** e selezionare il nodo.
2. Selezionare **Mostra indirizzi IP aggiuntivi** accanto a **Indirizzi IP** nella scheda Panoramica.

Se l'indirizzo IPv6 non viene visualizzato e il nodo è installato su un host Linux, seguire questi passaggi per abilitare il supporto IPv6 nel kernel.

Passi

1. Accedi 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 dovrebbe essere 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Se il risultato non è 0, consultare la documentazione del sistema operativo per la modifica `sysctl` impostazioni. Quindi, prima di continuare, modifica il valore in 0.

3. Accedere al contenitore del nodo 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 dovrebbe essere 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Se il risultato è diverso da 1, questa procedura non si applica. Contattare l'assistenza tecnica.

5. Esci dal contenitore: `exit`

```
root@DC1-S1:~ # exit
```

6. Come root, modifica 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, salva e chiudi il file.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Eseguire questi comandi per riavviare il contenitore StorageGRID :

```
storagegrid node stop node-name
```

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

Risolvere i problemi di un server syslog esterno

Nella tabella seguente vengono descritti i messaggi di errore che potrebbero essere correlati all'utilizzo di un server syslog esterno e vengono elencate 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, vedere:

- ["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
Non è possibile risolvere un indirizzo su un nome host	Il nome di dominio completo immesso per il server syslog non può essere risolto in un indirizzo IP. 1. Controlla il nome host inserito. Se hai inserito un indirizzo IP, assicurati che sia un indirizzo IP valido in notazione WXYZ ("decimale puntato"). 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. Potrebbe non esserci alcun servizio in ascolto sulla porta TCP o TLS per l'host oppure un firewall potrebbe bloccare l'accesso. 1. Verificare di aver inserito il nome di dominio completo (FQDN) o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Verificare che l'host per il servizio syslog stia eseguendo un demone syslog in ascolto sulla porta specificata. 3. Verificare che un firewall non stia bloccando l'accesso alle connessioni TCP/TLS dai nodi all'IP e alla porta del server syslog.
Rete irraggiungibile	Il server syslog non si trova su una subnet direttamente collegata. Un router ha restituito un messaggio di errore ICMP per indicare che non è riuscito a inoltrare i messaggi di prova dai nodi elencati al server syslog. 1. Verificare di aver inserito il nome di dominio completo o l'indirizzo IP corretto per il server syslog. 2. Per ogni nodo elencato, controllare l'elenco delle subnet della rete Grid, gli elenchi delle subnet delle reti amministrative e i gateway della rete client. Verificare che siano configurati per instradare il traffico verso il server syslog tramite l'interfaccia di rete e il gateway previsti (Grid, Admin o Client).
Host non raggiungibile	Il server syslog si trova su una subnet direttamente collegata (subnet utilizzata dai nodi elencati per i loro indirizzi IP Grid, Admin o Client). I nodi hanno tentato di inviare messaggi di prova, ma non hanno ricevuto risposte alle richieste ARP per l'indirizzo MAC del server syslog. 1. Verificare di aver inserito il nome di dominio completo 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
Connessione scaduta	È stato effettuato un tentativo di connessione TCP/TLS, ma per molto tempo non è stata ricevuta alcuna risposta dal server syslog. Potrebbe esserci un errore di configurazione del routing oppure un firewall potrebbe interrompere il traffico senza inviare alcuna risposta (una configurazione comune). 1. Verificare di aver inserito il nome di dominio completo o l'indirizzo IP corretto per il server syslog. 2. Per ogni nodo elencato, controllare l'elenco delle subnet della rete Grid, gli elenchi delle subnet delle reti amministrative e i gateway della rete client. Verificare che siano configurati per instradare il traffico verso il server syslog utilizzando l'interfaccia di rete e il gateway (Grid, Admin o Client) tramite i quali si prevede di raggiungere il server syslog. 3. Verificare che un firewall non stia bloccando 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 è stata successivamente chiusa. Le ragioni potrebbero essere: • Il server syslog potrebbe essere stato 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 inserito il nome di dominio completo (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 TCP, verificare che anche il server syslog utilizzi TCP. 3. Verificare che non sia configurato un firewall intermedio per chiudere le connessioni TCP inattive.
Errore del certificato TLS	Il certificato del server ricevuto dal server syslog non era compatibile con il bundle di certificati CA e il certificato client forniti. 1. Verificare che il bundle di certificati CA e il certificato client (se presente) siano compatibili con il certificato del 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 rilevarne il motivo. Esaminare i log di debug forniti con questo errore per tentare di determinarne 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 rilevarne il motivo. 1. Esaminare i log di debug forniti con questo errore per tentare di determinarne la causa principale. 2. Verificare di aver inserito il nome di dominio completo (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 TCP, verificare che anche il server syslog utilizzi TCP. 4. Verificare che il pacchetto di certificati CA e il certificato client (se presente) siano compatibili con il certificato del 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 dei test dai nodi elencati. Uno o più nodi potrebbero essere inattivi. 1. Seguire i passaggi 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 controllo

Messaggi e registri di controllo

Queste istruzioni contengono informazioni sulla struttura e sul contenuto dei messaggi di controllo e dei registri di controllo StorageGRID . È possibile utilizzare queste informazioni per leggere e analizzare la traccia di controllo dell'attività del sistema.

Queste istruzioni sono destinate agli amministratori responsabili della produzione di report sull'attività e l'utilizzo del sistema che richiedono l'analisi dei messaggi di audit del sistema StorageGRID .

Per utilizzare il file di registro di testo, è necessario avere accesso alla condivisione di controllo configurata sul 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 controllo e le destinazioni dei registri"](#) .

Flusso e conservazione dei messaggi di audit

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. Dovresti capire come questi messaggi di controllo si spostano attraverso il sistema StorageGRID verso `audit.log` file.

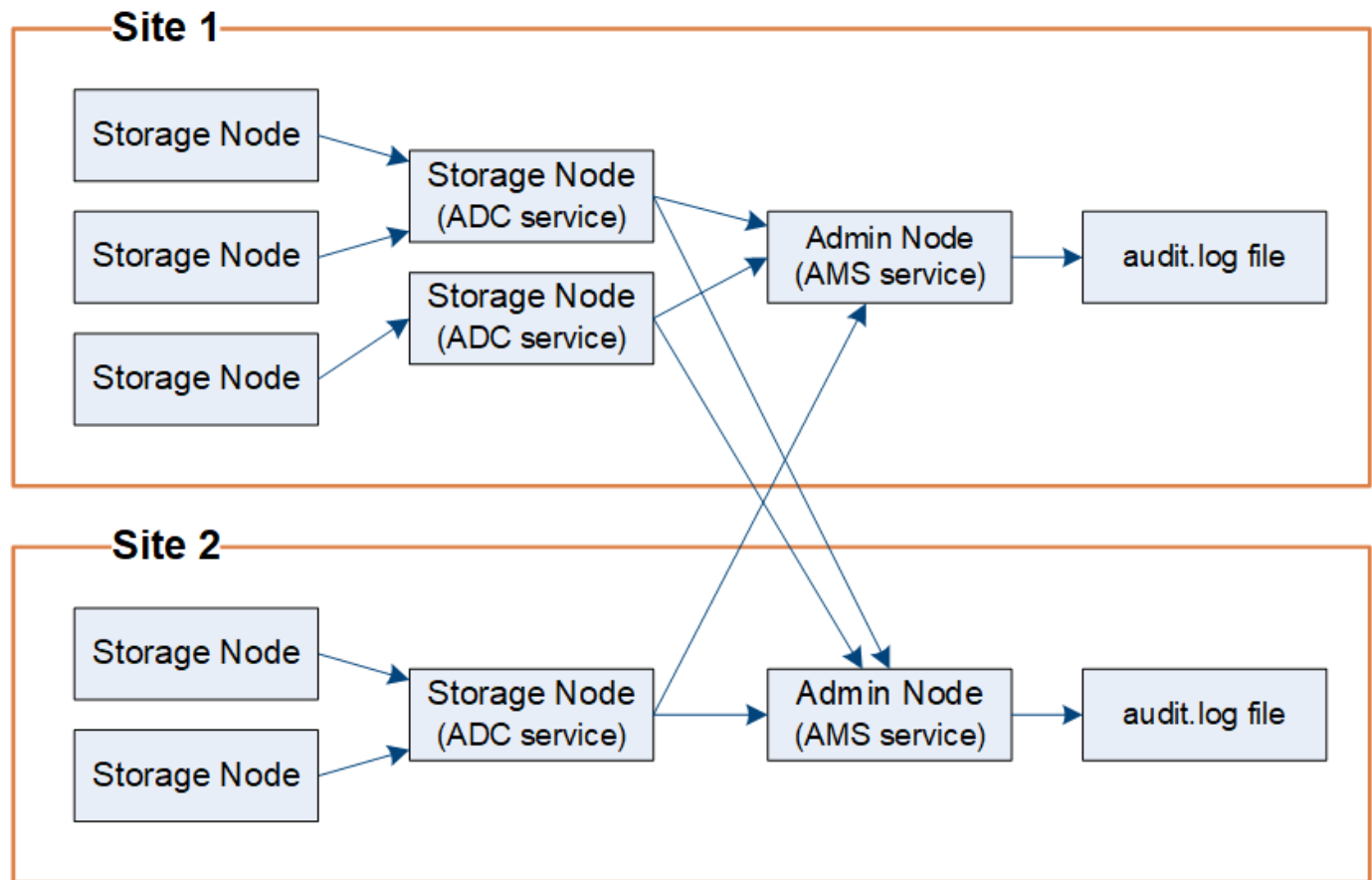
Flusso dei messaggi di audit

I messaggi di controllo vengono elaborati dai nodi di amministrazione e dai nodi di archiviazione che dispongono di un servizio di controller di dominio amministrativo (ADC).

Come mostrato nel diagramma del flusso dei messaggi di controllo, ogni nodo StorageGRID invia i propri messaggi di controllo a uno dei servizi ADC presso il sito del data center. Il servizio ADC viene abilitato automaticamente per i primi tre nodi di archiviazione installati in ciascun sito.

A sua volta, ogni servizio ADC funge da relay e invia la propria raccolta di messaggi di audit a ogni nodo amministrativo nel sistema StorageGRID, il che fornisce a ciascun nodo amministrativo un record completo dell'attività del sistema.

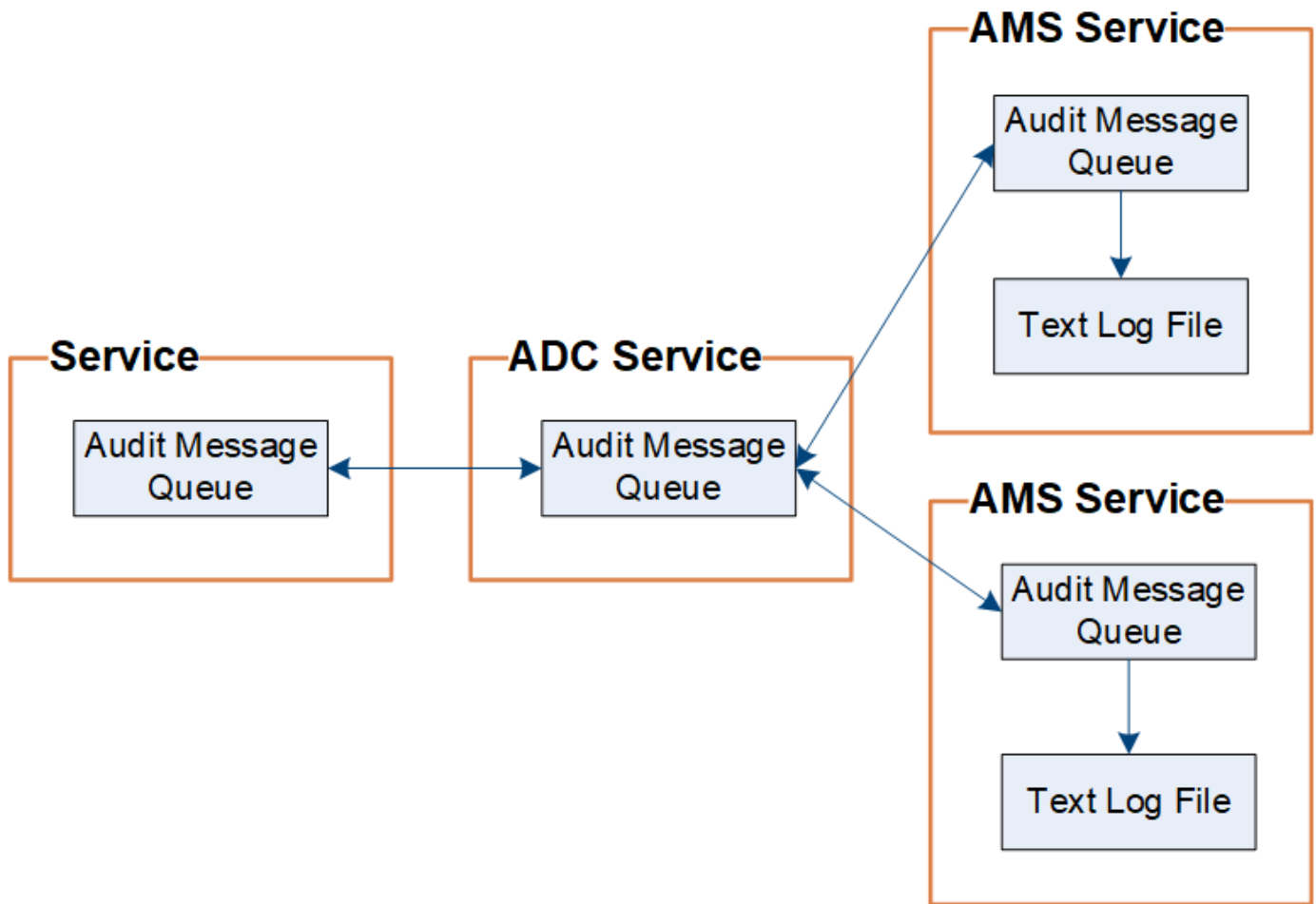
Ogni nodo di amministrazione memorizza i messaggi di controllo in file di registro di testo; il file di registro attivo è denominato `audit.log`.



Conservazione dei messaggi di controllo

StorageGRID utilizza un processo di copia ed eliminazione per garantire che nessun messaggio di controllo venga perso prima che possa essere scritto nel registro di controllo.

Quando un nodo genera o inoltra un messaggio di controllo, il messaggio viene memorizzato in una coda di messaggi di controllo sul disco di sistema del nodo della griglia. Una copia del messaggio viene sempre conservata in una coda di messaggi di controllo finché il messaggio non viene scritto nel file di registro di controllo nel nodo di amministrazione `/var/local/log` elenco. Ciò aiuta a prevenire la perdita di un messaggio di controllo durante il trasporto.



La coda dei messaggi di controllo può aumentare temporaneamente a causa di problemi di connettività di rete o di capacità di controllo insufficiente. Man mano che le code aumentano, consumano più spazio disponibile in ciascun nodo `/var/local/` elenco. Se il problema persiste e la directory dei messaggi di controllo di un nodo diventa troppo piena, i singoli nodi daranno priorità all'elaborazione del loro arretrato e diventeranno temporaneamente non disponibili per nuovi messaggi.

Nello specifico, potresti riscontrare i seguenti comportamenti:

- Se il `/var/local/log` Se la directory utilizzata da un nodo di amministrazione diventa piena, il nodo di amministrazione verrà contrassegnato come non disponibile per nuovi messaggi di controllo finché la directory non sarà più piena. Le richieste del client S3 non sono interessate. L'allarme XAMS (Unreachable Audit Repositories) viene attivato quando un repository di audit non è raggiungibile.
- Se il `/var/local/` Quando la directory utilizzata da un nodo di archiviazione con il servizio ADC è piena al 92%, il nodo verrà contrassegnato come non disponibile per i messaggi di controllo finché la directory non sarà piena solo all'87%. Le richieste del client S3 ad altri nodi non sono interessate. L'allarme NRLY (Available Audit Relays) viene attivato quando i relay di audit non sono raggiungibili.



Se non sono disponibili nodi di archiviazione con il servizio ADC, i nodi di archiviazione archiviano i messaggi di controllo localmente nel `/var/local/log/localaudit.log` file.

- Se il `/var/local/` la directory utilizzata da un nodo di archiviazione diventa piena all'85%, il nodo inizierà a rifiutare le richieste del client S3 con `503 Service Unavailable`.

I seguenti tipi di problemi possono causare un aumento notevole delle dimensioni delle code dei messaggi di controllo:

- Interruzione di un nodo di amministrazione o di un nodo di archiviazione con il servizio ADC. Se uno dei nodi del sistema è inattivo, i nodi rimanenti potrebbero accumulare arretrati.
- Un tasso di attività sostenuto che supera la capacità di audit del sistema.
- IL `/var/local/` spazio su un nodo di archiviazione ADC che si riempie per motivi non correlati ai messaggi di controllo. Quando ciò accade, il nodo smette di accettare nuovi messaggi di audit e dà priorità al suo arretrato attuale, il che può causare arretrati su altri nodi.

Avviso di coda di controllo di grandi dimensioni e allarme di messaggi di controllo in coda (AMQS)

Per aiutarti a monitorare le dimensioni delle code dei messaggi di controllo nel tempo, l'avviso **Coda di controllo di grandi dimensioni** e l'allarme AMQS legacy vengono attivati quando il numero di messaggi in una coda del nodo di archiviazione o in una coda del nodo di amministrazione raggiunge determinate soglie.

Se viene attivato l'avviso **Coda di controllo di grandi dimensioni** 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 dovrebbero risolversi nel tempo e possono essere ignorati.

Se l'avviso o l'allarme persiste e aumenta di gravità, visualizza un grafico delle dimensioni della coda. Se il numero aumenta costantemente nel corso di ore o giorni, è probabile che il carico di controllo abbia superato la capacità di controllo del sistema. Ridurre la frequenza operativa del client o diminuire il numero di messaggi di controllo registrati modificando il livello di controllo per Scritture client e Letture client su Errore o Disattivato. Vedere ["Configurare i messaggi di controllo e le destinazioni dei registri"](#).

Messaggi duplicati

Il sistema StorageGRID adotta un approccio conservativo in caso di guasto della rete o del nodo. Per questo motivo potrebbero esserci messaggi duplicati nel registro di controllo.

Accedi al file di registro di controllo

La condivisione di controllo contiene l'attivo `audit.log` file e tutti i file di registro di controllo compressi. È possibile accedere ai file di registro di controllo direttamente dalla riga di comando del nodo di amministrazione.

Prima di iniziare

- Hai ["autorizzazioni di accesso specifiche"](#).
- Devi avere il `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo di amministrazione.

Passi

1. Accedi a un nodo di amministrazione:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da \$ A # .

2. Andare alla directory contenente i file di registro di controllo:

```
cd /var/local/log
```

3. Visualizzare il file di registro di controllo corrente o salvato, a seconda delle necessità.

Rotazione del file di registro di controllo

I file dei registri di controllo vengono salvati nel nodo di amministrazione `/var/local/log` elenco. I file di registro di controllo attivi sono denominati `audit.log`.



Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati quando viene configurato un server syslog esterno. Vedere "[Configurare i messaggi di controllo e le destinazioni dei registri](#)".

Una volta al giorno, l'attivo `audit.log` il file viene salvato e ne viene creato uno nuovo `audit.log` il file è avviato. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`. Se in un singolo giorno viene creato più di un registro di controllo, i nomi dei file utilizzano la data di salvataggio del file, seguita da un numero, nel formato `yyyy-mm-dd.txt.n`. Per esempio, `2018-04-15.txt` E `2018-04-15.txt.1` sono il primo e il secondo file di registro 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. Nel tempo, ciò si traduce nel consumo dello spazio di archiviazione allocato per i log di controllo sul nodo di amministrazione. Uno script monitora il consumo di spazio del registro di controllo ed elimina i file di registro se necessario per liberare spazio nel `/var/local/log` elenco. I registri di controllo vengono eliminati in base alla data di creazione, partendo da quelli più vecchi. È possibile monitorare le azioni dello script nel seguente file: `/var/local/log/manage-audit.log`.

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

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

Formato del file di registro di controllo

Formato del file di registro di controllo

I file di registro di controllo si trovano su ogni nodo di amministrazione e contengono una raccolta di singoli messaggi di controllo.

Ogni messaggio di controllo contiene quanto segue:

- Il tempo coordinato universale (UTC) dell'evento che ha attivato il messaggio di controllo (ATIM) nel formato ISO 8601, seguito da uno spazio:

YYYY-MM-DDTHH:MM:SS.UUUUUU, Dove UUUUUU sono microsecondi.

- Il messaggio di controllo stesso, racchiuso tra parentesi quadre e che inizia con AUDT .

L'esempio seguente mostra tre messaggi di controllo in un file di registro di controllo (interruzioni di riga aggiunte per migliorare la leggibilità). Questi messaggi sono stati generati quando un tenant ha creato un bucket S3 e ha aggiunto due oggetti a tale bucket.

```
2019-08-07T18:43:30.247711
```

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-  
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547  
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][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-  
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547  
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][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-  
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547  
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 controllo nei file di registro di controllo non sono facili da leggere o

interpretare. Puoi usare il "[strumento di verifica e spiegazione](#)" per ottenere riepiloghi semplificati dei messaggi di controllo nel registro di controllo. Puoi usare il "[strumento di somma di controllo](#)" per riepilogare quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno richiesto queste operazioni.

Utilizzare lo strumento di verifica e spiegazione

Puoi usare il `audit-explain` strumento per tradurre i messaggi di controllo nel registro di controllo in un formato di facile lettura.

Prima di iniziare

- Hai "[autorizzazioni di accesso specifiche](#)".
- Devi avere il `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

Informazioni su questo compito

IL `audit-explain` strumento, disponibile sul nodo di amministrazione principale, fornisce riepiloghi semplificati dei messaggi di controllo in un registro di controllo.



IL `audit-explain` Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Elaborazione `audit-explain` le query possono consumare una grande quantità di potenza della CPU, il che potrebbe avere un impatto sulle operazioni StorageGRID .

Questo esempio mostra l'output tipico del `audit-explain` attrezzo. Questi quattro "**SPUT**" sono stati generati messaggi di controllo quando il tenant S3 con ID account 92484777680322627870 ha utilizzato richieste PUT S3 per creare un bucket denominato "bucket1" e aggiungere tre oggetti a tale 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 fare quanto segue:

- Elaborare registri di controllo semplici o compressi. Per esempio:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Elaborare più file contemporaneamente. Per esempio:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/log/*
```

- Accetta input da una pipe, che consente di filtrare e preelaborare l'input utilizzando `grep` comando o altri mezzi. Per esempio:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Poiché i registri di controllo possono essere molto grandi e lenti da analizzare, è possibile risparmiare tempo filtrando le parti che si desidera esaminare ed eseguendo `audit-explain` sulle parti, anziché sull'intero file.



IL `audit-explain` lo strumento non accetta file compressi come input inoltrato. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` strumento per decomprimere prima i file. Per esempio:

```
zcat audit.log.gz | audit-explain
```

Utilizzare il `help` (`-h`) opzione per vedere le opzioni disponibili. Per esempio:

```
$ audit-explain -h
```

Passi

1. Accedi al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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` Lo strumento stampa interpretazioni leggibili dall'uomo di tutti i messaggi nel file o nei file specificati.



Per ridurre la lunghezza delle righe e migliorare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se vuoi vedere i timestamp, usa il `timestamp(-t)` opzione.

Utilizzare lo strumento audit-sum

Puoi usare il `audit-sum` strumento per contare i messaggi di controllo di scrittura, lettura, intestazione ed eliminazione e per visualizzare il tempo minimo, massimo e medio (o dimensione) per ciascun tipo di operazione.

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche" .
- Devi avere il Passwords.txt file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

Informazioni su questo compito

IL `audit-sum` strumento, disponibile sul nodo di amministrazione primario, riepiloga quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno richiesto tali operazioni.



IL `audit-sum` Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Elaborazione `audit-sum` le query possono consumare una grande quantità di potenza della CPU, il che potrebbe avere un impatto sulle operazioni StorageGRID .

Questo esempio mostra l'output tipico del `audit-sum` attrezzo. Questo esempio mostra quanto tempo hanno richiesto le 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 orari per i seguenti messaggi di controllo S3, Swift e ILM in un registro di controllo.



I codici di controllo vengono rimossi dal prodotto e dalla documentazione quando le funzionalità diventano obsolete. Se riscontri un codice di controllo non elencato qui, controlla le versioni precedenti di questo argomento per le versioni SG più vecchie. Ad esempio, "[StorageGRID 11.8 Utilizzo della documentazione dello strumento di somma di controllo](#)".

Codice	Descrizione	Fare riferimento a
IDEL	Eliminazione avviata da ILM: registra quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: ILM ha avviato l'eliminazione"
SDEL	S3 DELETE: registra una transazione riuscita per eliminare un oggetto o un bucket.	"SDEL: S3 ELIMINA"

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"
KARITÉ	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	Swift DELETE: registra una transazione riuscita per eliminare un oggetto o un contenitore.	"WDEL: CANCELLA rapida"
WGET	Swift GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un contenitore.	"WGET: GET rapido"
WHEA	Swift HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un contenitore.	"WHEA: TESTA Veloce"
WPUT	Swift PUT: registra una transazione riuscita per creare un nuovo oggetto o contenitore.	"WPUT: PUT rapido"

IL `audit-sum` lo strumento può fare quanto segue:

- Elaborare registri di controllo semplici o compressi. Per esempio:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Elaborare più file contemporaneamente. Per esempio:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/log/*
```

- Accetta input da una pipe, che consente di filtrare e preelaborare l'input utilizzando `grep` comando o altri mezzi. Per 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 file compressi come input inoltrato. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` strumento per decomprimere prima i file. Per 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 oppure 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 guardare invece le dimensioni dell'oggetto.

Utilizzare il `help (-h)` opzione per vedere le opzioni disponibili. Per esempio:

```
$ audit-sum -h
```

Passi

1. Accedi al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Se si desidera analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, intestazione ed eliminazione, seguire questi passaggi:

- 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 del `audit-sum` attrezzo. Questo esempio mostra quanto tempo hanno richiesto le operazioni del protocollo.

message group average(sec)	count	min(sec)	max(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, con 1,13 secondi, ma le operazioni SGET e SPUT (S3 PUT) mostrano entrambe tempi molto lunghi nel caso peggiore, pari a circa 1.770 secondi.

b. Per mostrare le 10 operazioni di recupero più lente, utilizzare il comando `grep` per selezionare solo i messaggi SGET e aggiungere l'opzione di output lunga (`-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 cercare nel registro di controllo 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/r90l0aQ8JB-1566861764-4519.iso
      1624414429      10.96.101.125      object      5375001556
backup/r90l0aQ8JB-1566861764-6618.iso
      1533143793      10.96.101.125      object      5183661466
backup/r90l0aQ8JB-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 output di esempio, è possibile vedere che le tre richieste S3 GET più lente riguardavano oggetti di circa 5 GB di dimensione, ovvero molto più grandi degli altri oggetti. Le grandi dimensioni spiegano i lenti tempi di recupero nel caso peggiore.

3. Se vuoi determinare quali dimensioni degli oggetti vengono acquisiti e recuperati dalla tua griglia, usa l'opzione `dimensione(-s)`:

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

In questo esempio, la dimensione media dell'oggetto per SPUT è inferiore a 2,5 MB, ma la dimensione media per SGET è molto più grande. Il numero di messaggi SPUT è molto più elevato del numero di messaggi SGET, il che indica che la maggior parte degli oggetti non viene mai recuperata.

4. Se vuoi determinare se i recuperi sono stati lenti ieri:

- Emettere il comando sul registro di controllo appropriato e utilizzare l'opzione di raggruppamento per ora(-gt), seguito dal periodo di tempo (ad esempio, 15M, 1H, 10S):

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Questi risultati mostrano che il traffico S3 GET ha registrato un picco tra le 06:00 e le 07:00. Anche i tempi massimi e medi sono considerevolmente più alti in questi momenti e non aumentano gradualmente con l'aumentare del conteggio. Ciò suggerisce che da qualche parte è stata superata la capacità, forse nella rete o nella capacità della griglia di elaborare le richieste.

- b. Per determinare la dimensione degli oggetti recuperati ogni ora ieri, aggiungi l'opzione `dimensione(-s)` al comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average(B)	count	min(B)	max(B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Questi risultati indicano che alcuni recuperi molto grandi si sono verificati quando il traffico di recupero complessivo era al massimo.

- c. Per vedere più dettagli, usa il "[strumento di verifica e spiegazione](#)" per rivedere tutte le operazioni SGET durante quell'ora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se si prevede che l'output del comando `grep` sia composto da molte righe, aggiungere `less` comando per mostrare il contenuto del file di registro di controllo una pagina (una schermata) alla volta.

5. Se si desidera determinare se le operazioni SPUT sui bucket sono più lente delle operazioni SPUT sugli oggetti:
- a. Inizia utilizzando il `-go` opzione, che raggruppa separatamente i messaggi per le operazioni su oggetti e bucket:

```
grep SPUT sample.log | audit-sum -go
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.bucket 0.125	1	0.125	0.125
SPUT.object 0.236	12	0.025	1.019

I risultati mostrano che le operazioni SPUT per i bucket presentano caratteristiche prestazionali 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 average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ltd002 0.361	1564563	0.011	51.569

- c. Per determinare quali bucket hanno la dimensione dell'oggetto SPUT più grande, utilizzare entrambi `-gb` e il `-s` opzioni:

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ldt002 0.352	1564563	0.000	999.972

Formato del messaggio di controllo

Formato del messaggio di controllo

I messaggi di controllo scambiati all'interno del sistema StorageGRID includono informazioni standard comuni a tutti i messaggi e contenuti specifici che descrivono l'evento o l'attività segnalata.

Se le informazioni riassuntive fornite dal ["audit-spiegazione"](#) E ["somma di controllo"](#) strumenti non è sufficiente, fare riferimento a questa sezione per comprendere il formato generale di tutti i messaggi di audit.

Di seguito è riportato un esempio di messaggio di controllo, così come potrebbe apparire nel file di registro di controllo:

```
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):9445736326500603516]]
```

Ogni messaggio di controllo contiene una stringa di elementi di attributo. L'intera stringa è racchiusa tra parentesi([]), e ogni elemento attributo nella stringa ha le seguenti caratteristiche:

- Racchiuso tra parentesi []
- Introdotto dalla stringa AUDT , che indica un messaggio di controllo
- Senza delimitatori (senza virgole o spazi) prima o dopo
- Terminato da un carattere di avanzamento riga \n

Ogni elemento include un codice attributo, un tipo di dati e un valore che vengono riportati nel seguente formato:


```
[ATTR(type):value] [ATTR(type):value] ...  
[ATTR(type):value]\n
```

Il numero di elementi attributo nel messaggio dipende dal tipo di evento del messaggio. Gli elementi attributo non sono elencati in un ordine particolare.

L'elenco seguente descrive gli elementi dell'attributo:

- `ATTR` è un codice di quattro caratteri per l'attributo segnalato. Alcuni attributi sono comuni a tutti i messaggi di controllo, mentre altri sono specifici dell'evento.
- `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 controllo vengono utilizzati diversi tipi di dati.

Tipo	Descrizione
UI32	Intero lungo senza segno (32 bit); può memorizzare i numeri da 0 a 4.294.967.295.
UI64	Numero intero doppio lungo 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	Un array di lunghezza variabile di caratteri UTF-8. I caratteri possono essere sottoposti a escape con le seguenti convenzioni: • La barra rovesciata è <code>\\</code>. • Il ritorno a capo è <code>\r</code>. • Le virgolette doppie sono <code>\"</code>. • L'avanzamento di riga (nuova riga) è <code>\n</code>. • I caratteri possono essere sostituiti dai loro equivalenti esadecimali (nel formato <code>\xHH</code>, dove HH è il valore esadecimale che rappresenta il carattere).

Dati specifici dell'evento

Ogni messaggio di controllo nel registro di controllo registra dati specifici di un evento di sistema.

Dopo l'apertura [AUDT: contenitore che identifica il messaggio stesso, il set successivo di attributi fornisce informazioni sull'evento o sull'azione descritta dal messaggio di controllo. Questi attributi sono evidenziati nel seguente esempio:

```
2018-12-05T08:24:45.921845 [AUDT:*[RSLT\(\FC32\):SUCS\]*
\[TIME\(\UI64\):11454\]\[SAIP\(\IPAD\):"10.224.0.100"\]\[S3AI\(\CSTR\):"60025621595611246499"\]
\[SACC\(\CSTR\):"account"\]\[S3AK\(\CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRs
KJA=="\]\[SUSR\(\CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(\CSTR\):"60025621595611246499"\]\[SBAC\(\CSTR\):"account"\]\[S3BK\(\CSTR\):"bucket"\]
\[S3KY\(\CSTR\):"object"\]\[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 elemento (sottolineato nell'esempio) identifica quale evento ha generato il messaggio. Questo messaggio di esempio include il "KARITÉ" codice 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 elementi comuni.

Codice	Tipo	Descrizione
IN MEZZO	FC32	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 controllo.
ANID	UI32	ID nodo: 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 . Questo ID non può essere modificato.
ASES	UI64	Identificatore della sessione di audit: nelle versioni precedenti, questo elemento indicava l'ora in cui il sistema di audit veniva inizializzato dopo l'avvio del servizio. Questo valore temporale è stato misurato in microsecondi a partire 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 controllo.

Codice	Tipo	Descrizione
ASQN	UI64	Conteggio sequenza: nelle versioni precedenti, questo contatore veniva incrementato per ogni messaggio di controllo generato sul nodo della griglia (ANID) e reimpostato a zero al riavvio del servizio. Nota: questo elemento è obsoleto e non compare più nei messaggi di controllo.
ATID	UI64	ID traccia: identificatore condiviso dall'insieme dei messaggi attivati da un singolo evento.
ATIM	UI64	Timestamp: ora in cui è stato generato l'evento che ha attivato il messaggio di controllo, misurata in microsecondi a partire dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Si noti che la maggior parte degli strumenti disponibili per convertire il timestamp in data e ora locali si basano sui millisecondi. Potrebbe essere necessario arrotondare o troncare il timestamp registrato. L'ora leggibile dall'uomo che appare all'inizio del messaggio di controllo nel <code>audit.log</code> il file è l'attributo ATIM nel formato ISO 8601. La data e l'ora sono rappresentate come <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code> , dove il <code>T</code> è un carattere stringa letterale che indica l'inizio del segmento temporale della data. <code>UUUUUU</code> sono microsecondi.
ATYP	FC32	Tipo di evento: identificatore di quattro caratteri dell'evento registrato. Questo regola il contenuto del "payload" del messaggio: gli attributi che sono inclusi.
AVERE	UI32	Versione: la versione del messaggio di controllo. Con l'evoluzione del software StorageGRID, 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 elaborare 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, viene utilizzato NONE anziché SUCS, in modo che il messaggio non venga filtrato accidentalmente.

Esempi di messaggi di audit

Puoi trovare informazioni dettagliate in ogni messaggio di controllo. Tutti i messaggi di controllo utilizzano lo stesso formato.

Di seguito è riportato un esempio di messaggio di controllo come potrebbe apparire nel `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):"s3small11"] [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 controllo contiene informazioni sull'evento registrato, nonché informazioni sul messaggio di controllo stesso.

Per identificare quale evento viene registrato dal messaggio di controllo, 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):"s3small11"] [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'inserimento di un oggetto in un bucket.

Il seguente messaggio di controllo 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\):"s3small11"] [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, annotare il timestamp UTC (Universal Coordinated Time) all'inizio del messaggio di controllo. Questo valore è una versione leggibile dall'uomo dell'attributo ATIM del messaggio di controllo stesso:

2014-07-17T21:17:58.959669

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"]][S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"]][S3BK(CSTR):"s3small11"]][S3KY(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):1579224144102530435]]
```

ATIM registra il tempo, in microsecondi, trascorso dall'inizio dell'epoca UNIX. Nell'esempio, il valore 1405631878959669 si traduce in 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 controllo 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 controllo specifici dell'API S3.

I messaggi di controllo sono collegati tramite identificatori specifici per ciascun protocollo.

Protocollo	Codice
Collegamento delle operazioni S3	S3BK (secchio), S3KY (chiave) o entrambi
Collegamento delle operazioni Swift	WCON (contenitore), WOBJ (oggetto) o entrambi
Collegamento delle operazioni interne	CBID (identificatore interno dell'oggetto)

Tempistica dei messaggi di audit

A causa di fattori quali le differenze di temporizzazione 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 da quello mostrato negli esempi di questa sezione.

Transazioni di acquisizione di oggetti

È possibile identificare le transazioni di acquisizione del client nel registro di controllo individuando i messaggi di controllo specifici dell'API S3.

Non tutti i messaggi di controllo generati durante una transazione di acquisizione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di acquisizione.

Messaggi di controllo di acquisizione S3

Codice	Nome	Descrizione	Traccia	Vedere
SPUT	Transazione S3 PUT	Una transazione di acquisizione S3 PUT è stata completata correttamente.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regole dell'oggetto soddisfatte	Per questo oggetto è stata soddisfatta la politica ILM.	CBID	"ORLM: Regole dell'oggetto soddisfatte"

Messaggi di controllo di acquisizione rapida

Codice	Nome	Descrizione	Traccia	Vedere
WPUT	Transazione PUT rapida	Una transazione di acquisizione Swift PUT è stata completata con successo.	CBID, WCON, WOBJ	"WPUT: PUT rapido"
ORLM	Regole dell'oggetto soddisfatte	Per questo oggetto è stata soddisfatta la politica ILM.	CBID	"ORLM: Regole dell'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 archiviazione (servizio LDR).

In questo esempio, la policy ILM attiva include la regola ILM Crea 2 copie.



Non tutti i messaggi di controllo generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione di acquisizione S3 (SPUT).

In questo esempio si 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 dell'oggetto soddisfatte

Il messaggio ORLM indica che la policy ILM è stata soddisfatta 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 con codice di cancellazione, il campo LOCS include l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione

```
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 oppure informazioni sul contenitore 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 controllo individuando i messaggi di controllo specifici dell'API S3.

Non tutti i messaggi di controllo generati durante una transazione di eliminazione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di eliminazione.

S3 elimina i messaggi di controllo

Codice	Nome	Descrizione	Traccia	Vedere
SDEL	S3 Elimina	Richiesta effettuata per eliminare l'oggetto da un bucket.	CBID, S3KY	"SDEL: S3 ELIMINA"

Eliminazione rapida dei messaggi di controllo

Codice	Nome	Descrizione	Traccia	Vedere
WDEL	Eliminazione rapida	Richiesta effettuata per eliminare l'oggetto da un contenitore o il contenitore stesso.	CBID, WOBJ	"WDEL: CANCELLA rapida"

Esempio: eliminazione dell'oggetto S3

Quando un client S3 elimina un oggetto da un nodo di archiviazione (servizio LDR), viene generato un messaggio di controllo che viene salvato nel registro di controllo.



Nell'esempio seguente non sono elencati tutti i messaggi di controllo generati durante una transazione di eliminazione. Sono elencati solo quelli relativi alla transazione di eliminazione S3 (SDEL).

SDEL: Elimina S3

L'eliminazione dell'oggetto inizia 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 identificarlo.

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 controllo individuando i messaggi di controllo specifici dell'API S3.

Non tutti i messaggi di controllo 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 del recupero S3

Codice	Nome	Descrizione	Traccia	Vedere
SGET	S3 GET	Richiesta effettuata per recuperare un oggetto da un bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Messaggi di controllo di recupero rapido

Codice	Nome	Descrizione	Traccia	Vedere
WGET	GET rapido	Richiesta effettuata per recuperare un oggetto da un contenitore.	CBID, WCON, WOBJ	"WGET: GET rapido"

Esempio: recupero di oggetti S3

Quando un client S3 recupera un oggetto da un nodo di archiviazione (servizio LDR), viene generato un messaggio di controllo che viene salvato nel registro di controllo.

Si noti che non tutti i messaggi di controllo generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione di recupero S3 (SGET).

SGET: S3 GET

Il recupero degli oggetti inizia 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 identificarlo.

```

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 del bucket lo consente, un client può recuperare oggetti in modo anonimo oppure può recuperare oggetti da un bucket di proprietà di un account tenant diverso. Il messaggio di controllo contiene informazioni sull'account tenant del proprietario del bucket, in modo da poter monitorare queste richieste anonime e tra account.

Nel seguente messaggio di esempio, il client invia una richiesta GetObject per un oggetto archiviato in un bucket di cui non è proprietario. I valori per SBAI e SBAC registrano l'ID e il nome dell'account tenant del proprietario del bucket, che differiscono dall'ID e dal nome dell'account tenant 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 Seleziona su un oggetto

Quando un client S3 emette una query S3 Select su un oggetto, vengono generati messaggi di controllo che vengono salvati nel registro di controllo.

Si noti che non tutti i messaggi di controllo generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione S3 Select (SelectObjectContent).

Ogni query genera due messaggi di controllo: uno che esegue l'autorizzazione della richiesta S3 Select (il campo S3SR è impostato su "select") e una successiva operazione GET standard che recupera i dati dall'archivio 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:identit
y::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 controllo vengono generati quando un client S3 aggiorna i metadati di un oggetto.

Messaggi di controllo dell'aggiornamento dei metadati S3

Codice	Nome	Descrizione	Traccia	Vedere
SUPD	Metadati S3 aggiornati	Generato quando un client S3 aggiorna i metadati per 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 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 controllo (**CONFIGURAZIONE > Monitoraggio > Server di controllo e syslog**). Vedere ["Configurare i messaggi di controllo e le destinazioni dei registri"](#).

```
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 controllo

Descrizioni dei messaggi di audit

Nelle sezioni seguenti sono elencate descrizioni dettagliate dei messaggi di controllo restituiti dal sistema. Ogni messaggio di controllo viene prima elencato in una tabella che raggruppa i messaggi correlati in base alla classe di attività che il messaggio rappresenta. Questi raggruppamenti sono utili sia per comprendere i tipi di attività sottoposte a audit, sia per selezionare il tipo desiderato di filtraggio dei messaggi di audit.

I messaggi di controllo sono inoltre elencati in ordine alfabetico in base ai rispettivi codici di 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 registri e sull'utilizzo di un server syslog esterno per le informazioni di controllo, vedere ["Configurare i messaggi di controllo e le destinazioni dei registri"](#)

Categorie di messaggi di audit

Messaggi di controllo del sistema

I messaggi di audit appartenenti alla categoria di audit del sistema vengono utilizzati per eventi correlati al sistema di audit stesso, agli stati dei nodi della griglia, alle 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	Frammento di dati con codice di cancellazione mancante: indica che è stato rilevato un frammento di dati con codice di cancellazione mancante.	"ECMC: frammento di dati codificato in modo cancellabile mancante"
ECOC	Frammento di dati con codice di cancellazione danneggiato: indica che è stato rilevato un frammento di dati con codice di cancellazione danneggiato.	"ECOC: Frammento di dati corrotti con codice di cancellazione"
ETAF	Autenticazione di sicurezza non riuscita: un tentativo di connessione tramite Transport Layer Security (TLS) non è riuscito.	"ETAF: Autenticazione di sicurezza non riuscita"
GNRG	Registrazione GNDS: un servizio che aggiorna o registra informazioni su se stesso nel sistema StorageGRID .	"GNRG: Registrazione GNDS"
GNUR	Annullamento della registrazione GNDS: un servizio ha annullato la registrazione dal sistema StorageGRID .	"GNUR: Annullamento della registrazione GNDS"
GTED	Attività di griglia terminata: il servizio CMN ha terminato l'elaborazione dell'attività di griglia.	"GTED: attività di griglia terminata"
GTST	Attività di griglia avviata: il servizio CMN ha iniziato a elaborare l'attività di griglia.	"GTST: Attività di griglia avviata"
GTSU	Attività di griglia inviata: un'attività di griglia è stata inviata al servizio CMN.	"GTSU: compito di griglia inviato"

Codice	Titolo e descrizione del messaggio	Vedere
LLST	Posizione persa: questo messaggio di controllo viene generato quando una posizione viene persa.	"LLST: Posizione persa"
OLST	Oggetto perso: l'oggetto richiesto non può essere individuato nel sistema StorageGRID .	"OLST: il sistema ha rilevato un oggetto smarrito"
SADD	Disattivazione controllo di sicurezza: la registrazione dei messaggi di controllo è stata disattivata.	"SADD: Disabilitazione controllo sicurezza"
SADE	Abilitazione controllo di sicurezza: la registrazione dei messaggi di controllo è stata ripristinata.	"SADE: Abilitazione controllo sicurezza"
SVRF	Verifica fallita dell'archivio oggetti: un blocco di contenuto non ha superato i controlli di verifica.	"SVRF: Errore di verifica dell'archivio oggetti"
SVRU	Verifica archivio oggetti sconosciuta: rilevati dati oggetto inattesi nell'archivio oggetti.	"SVRU: Verifica archivio oggetti sconosciuto"
SYSD	Arresto del nodo: è stato richiesto un arresto.	"SYSD: arresto del nodo"
SISTEMA	Arresto del nodo: un servizio ha avviato un arresto regolare.	"SYST: Arresto del nodo"
SIST	Avvio nodo: un servizio avviato; la natura dell'arresto precedente è indicata nel messaggio.	"SYSU: Avvio del nodo"

Messaggi di controllo dell'archiviazione degli oggetti

I messaggi di controllo appartenenti alla categoria di controllo dell'archiviazione degli oggetti vengono utilizzati per gli eventi correlati all'archiviazione e alla gestione degli oggetti all'interno del sistema StorageGRID . Tra questi rientrano l'archiviazione e il recupero di oggetti, i trasferimenti da nodo griglia a nodo griglia e le verifiche.



I codici di controllo vengono rimossi dal prodotto e dalla documentazione quando le funzionalità diventano obsolete. Se riscontri un codice di controllo non elencato qui, controlla le versioni precedenti di questo argomento per le versioni SG più vecchie. Ad esempio, "[Messaggi di controllo dell'archiviazione degli oggetti StorageGRID 11.8](#)".

Codice	Descrizione	Vedere
FRATELLO	Richiesta di sola lettura del bucket: un bucket è entrato o uscito dalla modalità di sola lettura.	"BROR: Richiesta di sola lettura del bucket"

Codice	Descrizione	Vedere
CBSE	Fine invio oggetto: l'entità sorgente ha completato un'operazione di trasferimento dati da nodo griglia a nodo griglia.	"CBSE: Fine invio oggetto"
CBRE	Fine ricezione oggetto: l'entità di destinazione ha completato un'operazione di trasferimento dati da nodo griglia a nodo griglia.	"CBRE: Oggetto Ricevente Fine"
CGRR	Richiesta di replica tra griglie: StorageGRID ha tentato un'operazione di replica tra griglie per replicare oggetti tra bucket in una connessione di federazione di griglia.	"CGRR: richiesta di replicazione tra griglie"
EBDL	Eliminazione bucket vuoto: lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione di bucket vuoto).	"EBDL: Eliminazione bucket vuoto"
EBKR	Richiesta di 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 archiviato e verificato e ora può essere richiesto.	"SCMT: richiesta di commit dell'archivio oggetti"
SREM	Rimozione archivio oggetti: un blocco di contenuto è stato eliminato da un nodo della griglia e non può più essere richiesto direttamente.	"SREM: Rimozione dell'archivio oggetti"

Il cliente ha letto i messaggi di controllo

I messaggi di controllo di lettura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per recuperare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
S3SL	Richiesta S3 Select: registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere dettagli sul messaggio di errore e sul codice di errore. La richiesta potrebbe non essere andata a buon fine.	Cliente S3	"S3SL: Richiesta di selezione S3"

Codice	Descrizione	Utilizzato da	Vedere
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 controllo includerà il campo S3SR.	Cliente S3	"SGET: S3 GET"
KARITÉ	S3 HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	Cliente S3	"SHEA: TESTA S3"
WGET	Swift GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un contenitore.	Cliente Swift	"WGET: GET rapido"
WHEA	Swift HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un contenitore.	Cliente Swift	"WHEA: TESTA Veloce"

Il cliente scrive messaggi di audit

I messaggi di controllo di scrittura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per creare o modificare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
OVWR	Sovrascrittura oggetto: registra una transazione per sovrascrivere un oggetto con un altro oggetto.	Client S3 e Swift	"OVWR: sovrascrittura oggetto"
SDEL	S3 DELETE: registra una transazione riuscita per eliminare un oggetto o un bucket. Nota: se la transazione opera su una sottorisorsa, il messaggio di controllo includerà il campo S3SR.	Cliente S3	"SDEL: S3 ELIMINA"
SPOS	S3 POST: registra una transazione riuscita per ripristinare un oggetto dallo storage AWS Glacier a un Cloud Storage Pool.	Cliente S3	"SPOS: S3 POST"
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 controllo includerà il campo S3SR.	Cliente S3	"SPUT: S3 PUT"
SUPD	Metadati S3 aggiornati: registra una transazione riuscita per aggiornare i metadati per un oggetto o un bucket esistente.	Cliente S3	"SUPD: Metadati S3 aggiornati"

Codice	Descrizione	Utilizzato da	Vedere
WDEL	Swift DELETE: registra una transazione riuscita per eliminare un oggetto o un contenitore.	Cliente Swift	"WDEL: CANCELLA rapida"
WPUT	Swift PUT: registra una transazione riuscita per creare un nuovo oggetto o contenitore.	Cliente Swift	"WPUT: PUT rapido"

Messaggio di controllo di gestione

La categoria Gestione registra le richieste degli utenti nell'API di gestione.

Codice	Titolo e descrizione del messaggio	Vedere
MGAU	Messaggio di controllo dell'API di gestione: un registro delle richieste degli utenti.	"MGAU: Messaggio di audit di gestione"

Messaggi di controllo ILM

I messaggi di audit appartenenti alla categoria di audit ILM vengono utilizzati per eventi correlati alle operazioni di gestione del ciclo di vita delle informazioni (ILM).

Codice	Titolo e descrizione del messaggio	Vedere
IDEL	Eliminazione avviata da ILM: questo messaggio di controllo viene generato quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: ILM ha avviato l'eliminazione"
LKCU	Pulizia degli oggetti sovrascritti. Questo messaggio di controllo viene generato quando un oggetto sovrascritto viene rimosso automaticamente per liberare spazio di archiviazione.	"LKCU: Pulizia degli oggetti sovrascritti"
ORLM	Regole oggetto soddisfatte: questo messaggio di controllo viene generato quando i dati dell'oggetto vengono archiviati come specificato dalle regole ILM.	"ORLM: Regole dell'oggetto soddisfatte"

Riferimento al messaggio di audit

BROR: Richiesta di sola lettura del bucket

Il servizio LDR genera questo messaggio di controllo 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 eliminati.

Codice	Campo	Descrizione
BKHD	UUID del bucket	L'ID del bucket.

Codice	Campo	Descrizione
BROV	Valore della richiesta di sola lettura del bucket	Se il bucket viene reso di sola lettura o sta abbandonando lo stato di sola lettura (1 = di sola lettura, 0 = non di sola lettura).
FRATELLI	Motivo di sola lettura del bucket	Il motivo per cui il bucket viene reso di sola lettura o abbandona lo stato di sola lettura. Ad esempio, emptyBucket.
S3AI	ID account tenant S3	ID dell'account tenant che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.

CBRB: Oggetto Ricevi Inizio

Durante il normale funzionamento del sistema, i blocchi di contenuto vengono trasferiti continuamente tra diversi nodi man mano che i dati vengono consultati, replicati e conservati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo a un altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a 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 sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo conteggio sequenziale richiesto. Se l'operazione ha esito positivo, il trasferimento inizia da questo conteggio sequenziale.
CTES	Conteggio previsto della sequenza finale	Indica l'ultimo conteggio sequenziale richiesto. In caso di esito positivo, il trasferimento è considerato completato quando è stato ricevuto questo conteggio sequenziale.

Codice	Campo	Descrizione
RSLT	Stato di inizio del trasferimento	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato con successo.

Questo messaggio di controllo indica che è stata avviata un'operazione di trasferimento dati da nodo a nodo su un singolo contenuto, come identificato dal suo identificatore del blocco di contenuto. L'operazione richiede i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale previsto". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e, se combinate con i messaggi di controllo dell'archiviazione, per verificare i conteggi delle repliche.

CBRE: Oggetto Ricevente Fine

Quando il trasferimento di un blocco di contenuto da un nodo a un altro è completato, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a 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 sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il conteggio della sequenza in cui è iniziato il trasferimento.
CTAS	Conteggio effettivo della sequenza finale	Indica l'ultimo conteggio sequenziale trasferito correttamente. Se il conteggio effettivo della sequenza finale è uguale al conteggio della sequenza iniziale e il risultato del trasferimento non è andato a buon fine, non è stato scambiato alcun dato.

Codice	Campo	Descrizione
RSLT	Risultato del trasferimento	Il risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: trasferimento completato con successo; tutti i conteggi delle sequenze richiesti sono stati inviati. CONL: connessione persa durante il trasferimento CTMO: timeout della connessione durante l'avvio 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 controllo indica che è stata completata un'operazione di trasferimento dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale effettivo". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se abbinato ai messaggi di controllo dell'archiviazione, può essere utilizzato anche per verificare i conteggi delle repliche.

CBSB: Inizio invio oggetto

Durante il normale funzionamento del sistema, i blocchi di contenuto vengono trasferiti continuamente tra diversi nodi man mano che i dati vengono consultati, replicati e conservati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo a un altro, questo messaggio viene emesso dall'entità sorgente.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a 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 sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.

Codice	Campo	Descrizione
CTSS	Avvia conteggio sequenza	Indica il primo conteggio sequenziale richiesto. Se l'operazione ha esito positivo, il trasferimento inizia da questo conteggio sequenziale.
CTES	Conteggio previsto della sequenza finale	Indica l'ultimo conteggio sequenziale richiesto. In caso di esito positivo, il trasferimento è considerato completato quando è stato ricevuto questo conteggio sequenziale.
RSLT	Stato di inizio del trasferimento	Stato al momento dell'avvio del trasferimento: SUCS: trasferimento avviato con successo.

Questo messaggio di controllo indica che è stata avviata un'operazione di trasferimento dati da nodo a nodo su un singolo contenuto, come identificato dal suo identificatore del blocco di contenuto. L'operazione richiede i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale previsto". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e, se combinate con i messaggi di controllo dell'archiviazione, per verificare i conteggi delle repliche.

CBSE: Fine invio oggetto

Quando il trasferimento di un blocco di contenuto da un nodo a un altro è completato, questo messaggio viene emesso dall'entità sorgente.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a 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 sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il conteggio della sequenza in cui è iniziato il trasferimento.

Codice	Campo	Descrizione
CTAS	Conteggio effettivo della sequenza finale	Indica l'ultimo conteggio sequenziale trasferito correttamente. Se il conteggio effettivo della sequenza finale è uguale al conteggio della sequenza iniziale e il risultato del trasferimento non è andato a buon fine, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	Il risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: Trasferimento completato con successo; tutti i conteggi delle sequenze richiesti sono stati inviati. CONL: connessione persa durante il trasferimento CTMO: timeout della connessione durante l'avvio 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 controllo indica che è stata completata un'operazione di trasferimento dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale effettivo". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se abbinato ai messaggi di controllo dell'archiviazione, può essere utilizzato anche per verificare i conteggi delle repliche.

CGRR: richiesta di replicazione tra griglie

Questo messaggio viene generato quando StorageGRID tenta un'operazione di replica tra griglie per replicare oggetti tra bucket in una connessione di federazione di griglie.

Codice	Campo	Descrizione
CSIZ	Dimensione dell'oggetto	La dimensione dell'oggetto in byte. L'attributo CSIZ è stato introdotto in StorageGRID 11.8. Di conseguenza, le richieste di replica tra griglie che coprono un aggiornamento StorageGRID dalla versione 11.7 alla 11.8 potrebbero avere una dimensione totale degli oggetti non accurata.
S3AI	ID account tenant S3	ID dell'account tenant proprietario del bucket da cui viene replicato l'oggetto.
GFID	ID di connessione della federazione di rete	ID della connessione di federazione della griglia utilizzata per la replica tra griglie.

Codice	Campo	Descrizione
OPER	operazione CGR	Tipo di operazione di replicazione tra griglie tentata: • 0 = Replica oggetto • 1 = Replica oggetto multiparte • 2 = Replica elimina marcatore
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket.
VSID	ID versione	ID della versione specifica di un oggetto che è stato replicato.
RSLT	Codice risultato	Restituisce un errore riuscito (SUCS) o generale (GERR).

EBDL: Eliminazione bucket vuoto

Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione di svuotamento del bucket).

Codice	Campo	Descrizione
CSIZ	Dimensione dell'oggetto	La dimensione dell'oggetto in byte.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
SEGC	UUID del contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Identificatore univoco universale	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, viene utilizzato NONE anziché SUCS, in modo che il messaggio non venga filtrato accidentalmente.

EBKR: Richiesta bucket vuoto

Questo messaggio indica che un utente ha inviato una richiesta per attivare o disattivare un bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di oggetti).

Codice	Campo	Descrizione
COSTRUIRE	UUID del bucket	L'ID del bucket.
EBJS	Configurazione JSON del bucket vuoto	Contiene il JSON che rappresenta la configurazione corrente del bucket vuoto.
S3AI	ID account tenant S3	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.

ECMC: frammento di dati codificato in modo cancellabile mancante

Questo messaggio di controllo indica che il sistema ha rilevato un frammento di dati mancante con codice di cancellazione.

Codice	Campo	Descrizione
VCMC	ID VCS	Il nome del VCS che contiene il blocco mancante.
MCID	ID del blocco	L'identificatore del frammento mancante con codice di cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo specifico messaggio. Viene utilizzato 'NONE' anziché 'SUCS' in modo che il messaggio non venga filtrato.

ECOC: Frammento di dati corrotti con codice di cancellazione

Questo messaggio di controllo indica che il sistema ha rilevato un frammento di dati con codice di cancellazione corrotto.

Codice	Campo	Descrizione
VCCO	ID VCS	Il nome del VCS che contiene il blocco danneggiato.
VLID	ID volume	Il volume RangeDB che contiene il frammento con codice di cancellazione danneggiato.
CCID	ID del blocco	L'identificatore del frammento corrotto con codice di cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo specifico messaggio. Viene utilizzato 'NONE' anziché 'SUCS' in modo che il messaggio non venga filtrato.

ETAF: Autenticazione di sicurezza non riuscita

Questo messaggio viene generato quando un tentativo di connessione tramite Transport Layer Security (TLS) non riesce.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP su cui l'autenticazione non è riuscita.
RUID	Identità utente	Un identificatore dipendente dal servizio che rappresenta l'identità dell'utente remoto.
RSLT	Codice motivo	Motivo del fallimento: SCNI: Impossibile stabilire una connessione sicura. CERM: Certificato mancante. CERT: Il certificato non è valido. CERE: Il certificato è scaduto. CERR: Il certificato è stato revocato. CSGN: la firma del certificato non è valida. CSGU: Il firmatario del certificato era sconosciuto. UCRM: le credenziali utente erano mancanti. UCRI: Le credenziali utente non erano valide. UCRU: Le credenziali utente non erano consentite. TOUT: Autenticazione scaduta.

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 fallisce a causa di certificati o credenziali non validi, inattesi o non consentiti, viene registrato un messaggio di controllo. Ciò consente di effettuare query su tentativi di accesso non autorizzati e altri problemi di connessione correlati alla sicurezza.

Il messaggio potrebbe essere causato da un'entità remota con una configurazione errata o da tentativi di presentare al sistema credenziali non valide o non consentite. Questo messaggio di controllo deve essere monitorato per rilevare tentativi di accesso non autorizzato al sistema.

GNRG: Registrazione GNDS

Il servizio CMN genera questo messaggio di controllo quando un servizio ha aggiornato o registrato informazioni su se stesso nel sistema StorageGRID .

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUCS: Riuscito • SUNV: Servizio non disponibile • GERR: Altro fallimento
GNID	Nodo ID	ID nodo del servizio che ha avviato la richiesta di aggiornamento.
GNTTP	Tipo di dispositivo	Il tipo di dispositivo del nodo della griglia (ad esempio, BLDR per un servizio LDR).
GNDV	Versione del modello del dispositivo	Stringa che identifica la versione del modello del dispositivo del nodo della griglia nel bundle DMDL.
GNGP	Gruppo	Il gruppo a cui appartiene il nodo della griglia (nel contesto dei costi dei collegamenti 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 Grid Nodes Bundle.

GNUR: Annullamento della registrazione GNDS

Il servizio CMN genera questo messaggio di controllo quando un servizio dispone di informazioni non registrate su se stesso dal sistema StorageGRID .

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUCS: Riuscito • SUNV: Servizio non disponibile • GERR: Altro fallimento
GNID	Nodo ID	ID nodo del servizio che ha avviato la richiesta di aggiornamento.

GTED: attività di griglia terminata

Questo messaggio di controllo indica che il servizio CMN ha terminato l'elaborazione dell'attività di griglia specificata e ha spostato l'attività nella tabella Cronologica. Se il risultato è SUCS, ABRT o ROLF, verrà visualizzato il messaggio di controllo corrispondente Grid Task Started. Gli altri risultati indicano che l'elaborazione di questa attività di griglia non è mai iniziata.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in modo univoco un'attività di griglia generata e consente di gestirla durante il suo ciclo di vita. Nota: l'ID attività viene assegnato al momento della generazione di un'attività della griglia, non al momento dell'invio. È possibile che una determinata attività della griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Inviato, Iniziato e Terminato.
RSLT	Risultato	Il risultato finale dello stato dell'attività della griglia: • SUCS: L'attività della griglia è stata completata con successo. • ABRT: L'attività della griglia è stata terminata senza un errore di rollback. • ROLF: L'attività di griglia è stata terminata e non è stato possibile completare il processo di rollback. • CANC: l'attività della griglia è stata annullata dall'utente prima di essere avviata. • EXPR: L'attività della griglia è scaduta prima di essere avviata. • IVLD: L'attività della griglia non era valida. • AUTH: L'attività di griglia non era autorizzata. • DUPL: l'attività della griglia è stata rifiutata come duplicata.

GTST: Attività di griglia avviata

Questo messaggio di controllo indica che il servizio CMN ha iniziato a elaborare l'attività di griglia specificata. Il messaggio di controllo segue immediatamente il messaggio Grid Task Submitted per le attività della griglia avviate dal servizio interno Grid Task Submission e selezionate per l'attivazione automatica. Per le attività della griglia inviate alla tabella In sospeso, questo messaggio viene generato quando l'utente avvia l'attività della griglia.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in modo univoco un'attività di griglia generata e consente di gestirla durante il suo ciclo di vita. Nota: l'ID attività viene assegnato al momento della generazione di un'attività della griglia, non al momento dell'invio. È possibile che una determinata attività della griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Inviato, Iniziato e Terminato.

Codice	Campo	Descrizione
RSLT	Risultato	Il risultato. Questo campo ha un solo valore: SUCS: L'attività della griglia è stata avviata correttamente.

GTSU: compito di griglia inviato

Questo messaggio di controllo indica che un'attività di griglia è stata inviata al servizio CMN.

Codice	Campo	Descrizione
TSID	ID attività	Identifica in modo univoco un'attività di griglia generata e consente di gestirla durante il suo ciclo di vita. Nota: l'ID attività viene assegnato al momento della generazione di un'attività della griglia, non al momento dell'invio. È possibile che una determinata attività della griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Inviato, Iniziato e Terminato.
TTYP	Tipo di attività	Il tipo di attività della griglia.
TVER	Versione dell'attività	Un numero che indica la versione dell'attività della griglia.
TDSC	Descrizione dell'attività	Una descrizione leggibile dall'uomo dell'attività della griglia.
IVA	Valido dopo il timestamp	Il momento più remoto (UINT64 microsecondi dal 1° gennaio 1970 - ora UNIX) in cui l'attività della griglia è valida.
VBTS	Valido prima del timestamp	L'ultima ora (UINT64 microsecondi dal 1° gennaio 1970 - ora UNIX) in cui l'attività della griglia è valida.
TSRC	Fonte	La fonte del compito: - TXTB: l'attività della griglia è stata inviata tramite il sistema StorageGRID come blocco di testo firmato. - GRIGLIA: l'attività della griglia è stata inviata tramite il servizio interno di invio delle attività della griglia.
ACTV	Tipo di attivazione	Il tipo di attivazione: - AUTO: l'attività della griglia è stata inviata per l'attivazione automatica. - PEND: l'attività della griglia è stata inviata alla tabella in sospeso. Questa è l'unica possibilità per la sorgente TXTB.

Codice	Campo	Descrizione
RSLT	Risultato	Il risultato dell'invio: • SUCS: L'attività della griglia è stata inviata correttamente. • FAIL: l'attività è stata spostata direttamente nella tabella storica.

IDEL: ILM ha avviato l'eliminazione

Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto.

Il messaggio IDEL viene generato in una di queste 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 suo periodo di conservazione è scaduto (presupponendo che l'impostazione di eliminazione automatica sia abilitata e la conservazione legale sia disattivata).
- **Per gli oggetti nei bucket S3 non conformi.** Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto perché nessuna istruzione di posizionamento nei criteri ILM attivi è attualmente applicabile all'oggetto.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CMPA	Conformità: Eliminazione automatica	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), indica se un oggetto conforme deve essere eliminato automaticamente al termine del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale.
CMPL	Conformità: Conservazione legale	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), indica se il bucket è attualmente sottoposto a un blocco legale.
CMPR	Conformità: Periodo di conservazione	Solo per oggetti nei bucket S3 conformi. Durata del periodo di conservazione dell'oggetto in minuti.
CTME	Conformità: tempo di acquisizione	Solo per oggetti nei bucket S3 conformi. Tempo di ingestione dell'oggetto. È possibile aggiungere a questo valore il periodo di conservazione in minuti per determinare quando l'oggetto può essere eliminato dal bucket.
DMRK	Elimina ID versione marcatore	ID versione del marcatore di eliminazione creato durante l'eliminazione di un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCATION	Posizioni	Posizione di archiviazione dei dati degli oggetti all'interno del sistema StorageGRID . Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato eliminato). CLEC: per gli oggetti con codifica di cancellazione, l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione 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 del nodo ARC della posizione dell'oggetto se i dati dell'oggetto sono archiviati.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
RSLT	Risultato	Il risultato dell'operazione ILM. SUCS: L'operazione ILM ha avuto successo.
REGOLA	Etichetta delle regole	• Se un oggetto in un bucket S3 conforme viene eliminato automaticamente perché il suo periodo di conservazione è scaduto, questo campo è vuoto. • Se l'oggetto viene eliminato perché non ci sono più istruzioni di posizionamento 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.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID della versione specifica di un oggetto che è stato eliminato. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

LKCU: Pulizia degli oggetti sovrascritti

Questo messaggio viene generato quando StorageGRID rimuove un oggetto sovrascritto che in precedenza necessitava di essere ripulito per liberare spazio di archiviazione. Un oggetto viene sovrascritto quando un client S3 scrive un oggetto in un percorso che contiene già 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	<i>Solo per uso interno.</i>
LUID	UUID dell'oggetto rimosso	L'identificatore dell'oggetto che è stato rimosso.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
SEGC	UUID del contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Identificatore univoco universale	L'identificatore dell'oggetto che esiste ancora. Questo valore è disponibile solo se l'oggetto non è stato eliminato.

LKDM: Pulizia degli oggetti trapelati

Questo messaggio viene generato quando un blocco trapelato viene pulito o eliminato. Un blocco può essere parte di un oggetto replicato o di un oggetto codificato tramite cancellazione.

Codice	Campo	Descrizione
OROLOGIO	Posizione del blocco	Il percorso del file del frammento trapelato che è stato eliminato.
CTYP	Tipo di blocco	Tipo di pezzo: ec: Erasure-coded object chunk repl: Replicated object chunk

Codice	Campo	Descrizione
LTyp	Tipo di perdita	I cinque tipi di perdite che possono essere rilevate: <code>object_leaked</code>: Object doesn't exist in the grid <code>location_leaked</code>: Object exists in the grid, but found location doesn't belong to object <code>mup_seg_leaked</code>: Multipart upload was stopped or not completed, and the segment/part was left out <code>segment_leaked</code>: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment <code>no_parent</code>: Container object is deleted, but object segment was left out and not deleted
CTIM	Tempo di creazione del blocco	Ora in cui è stato creato il frammento trapelato.
UUID	Identificatore univoco universale	L'identificatore dell'oggetto a cui appartiene il blocco.
CBID	Identificatore del blocco di contenuto	CBID dell'oggetto a cui appartiene il frammento trapelato.
CSIZ	Dimensione del contenuto	La dimensione del blocco in byte.

LLST: Posizione persa

Questo messaggio viene generato ogni volta che non è possibile trovare la posizione per una copia di un oggetto (replicata o con codice di cancellazione).

Codice	Campo	Descrizione
CBIL	CBID	Il CBID interessato.
ECPR	Profilo di codifica di cancellazione	Per dati di oggetti codificati tramite cancellazione. ID del profilo di codifica di cancellazione utilizzato.

Codice	Campo	Descrizione
LTyp	Tipo di posizione	CLDI (online): per dati di oggetti replicati CLEC (online): per dati di oggetti codificati con cancellazione CLNL (Nearline): per dati di oggetti replicati archiviati
NOID	ID nodo sorgente	L'ID del nodo su cui sono andate perse le posizioni.
PCLD	Percorso verso l'oggetto replicato	Il percorso completo alla posizione del disco in cui si trovano i dati dell'oggetto perso. Restituito solo quando LTyp ha un valore di CLDI (ovvero, per oggetti replicati). Prende la forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@</code>
RSLT	Risultato	Sempre NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.
TSRC	Sorgente di attivazione	UTENTE: attivato dall'utente SYST: Sistema attivato
UUID	ID univoco universale	Identificatore dell'oggetto interessato nel sistema StorageGRID .

MG AU: Messaggio di audit di gestione

La categoria Gestione registra le richieste degli utenti nell'API di gestione. Ogni richiesta HTTP che non sia una richiesta GET o HEAD a un URI API valido registra una risposta contenente il nome utente, l'IP e il tipo di richiesta all'API. Gli URI API non validi (ad esempio /api/v3-authorize) e le richieste non valide agli URI API validi non vengono registrati.

Codice	Campo	Descrizione
MDIP	Indirizzo IP di destinazione	L'indirizzo IP del server (destinazione).
MDNA	Nome di dominio	Il nome di dominio dell'host.
MPAT	Richiedi PATH	Il percorso della richiesta.

Codice	Campo	Descrizione
MPQP	Richiedi parametri di query	I parametri di query per la richiesta.
MRBD	Corpo della richiesta	Il contenuto del corpo della 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 ricavate 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 dismessi in POST /grid/servers/decommission 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	Metodo di richiesta HTTP: • INVIARE • METTERE • ELIMINARE • TOPPA
MRSC	Codice di risposta	Il codice di risposta.
Prezzo consigliato al pubblico	Corpo della risposta	Per impostazione predefinita, il contenuto della risposta (il corpo della risposta) viene registrato. 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 del client (sorgente).
MUUN	URN utente	L'URN (nome uniforme della risorsa) dell'utente che ha inviato la richiesta.
RSLT	Risultato	Restituisce l'esito positivo (SUCC) oppure l'errore segnalato dal backend.

OLST: il sistema ha rilevato un oggetto smarrito

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 smarrito.
NOID	Nodo ID	Se disponibile, l'ultima posizione nota, diretta o prossima alla linea, dell'oggetto smarrito. È possibile avere solo l'ID nodo senza un ID volume se le informazioni sul volume non sono disponibili.
SENTIERO	Secchio/chiave S3	Se disponibili, il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.
UUID	ID univoco universale	Identificatore dell'oggetto smarrito all'interno del sistema StorageGRID .
VOLI	ID volume	Se disponibile, l'ID volume del nodo di archiviazione per l'ultima posizione nota dell'oggetto perso.

ORLM: Regole dell'oggetto soddisfatte

Questo messaggio viene generato quando l'oggetto viene archiviato e copiato correttamente come specificato dalle regole ILM.



Il messaggio ORLM non viene generato quando un oggetto viene archiviato correttamente dalla regola predefinita Crea 2 copie se un'altra regola nel criterio utilizza il filtro avanzato Dimensione oggetto.

Codice	Campo	Descrizione
COSTRUIRE	Testata della benna	Campo ID bucket. Utilizzato per operazioni interne. Appare 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
LOCATION	Posizioni	Posizione di archiviazione dei dati degli oggetti all'interno del sistema StorageGRID . Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato eliminato). CLEC: per gli oggetti con codifica di cancellazione, l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione 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 del nodo ARC della posizione dell'oggetto se i dati dell'oggetto sono archiviati.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
RSLT	Risultato	Il risultato dell'operazione ILM. SUCS: L'operazione ILM ha avuto successo.
REGOLA	Etichetta delle regole	Etichetta leggibile dall'uomo assegnata alla regola ILM applicata a questo oggetto.
SEGC	UUID del contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
SGCB	Contenitore CBID	CBID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo per oggetti segmentati e multiparte.
STATISTICHE	Stato	Lo stato di funzionamento dell'ILM. FATTO: le operazioni ILM sull'oggetto sono state completate. DFER: L'oggetto è stato contrassegnato per una futura rivalutazione ILM. PRGD: L'oggetto è stato eliminato dal sistema StorageGRID . NLOC: i dati dell'oggetto non sono più disponibili nel sistema StorageGRID . Questo stato potrebbe indicare che tutte le copie dei dati dell'oggetto sono mancanti o danneggiate.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .

Codice	Campo	Descrizione
VSID	ID versione	ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Il messaggio di controllo 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.
- Per questa epoca sono soddisfatte le regole ILM per l'oggetto.
- Le regole ILM hanno eliminato l'oggetto.
- Il processo di verifica in background rileva che una copia dei dati dell'oggetto replicato è danneggiata. Il sistema StorageGRID esegue una valutazione ILM per sostituire l'oggetto danneggiato.

Informazioni correlate

- ["Transazioni di acquisizione di oggetti"](#)
- ["Transazioni di eliminazione degli oggetti"](#)

OVWR: sovrascrittura oggetto

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	Identificatore del blocco di contenuto (nuovo)	Il CBID del nuovo oggetto.
CSIZ	Dimensione oggetto precedente	La dimensione, in byte, dell'oggetto sovrascritto.
Disturbo ossessivo-compulsivo (OCBD)	Identificatore del blocco di contenuto (precedente)	Il CBID dell'oggetto precedente.
UUID	ID univoco universale (nuovo)	Identificatore del nuovo oggetto all'interno del sistema StorageGRID .
OUID	ID univoco universale (precedente)	Identificatore dell'oggetto precedente all'interno del sistema StorageGRID .

Codice	Campo	Descrizione
SENTIERO	Percorso oggetto S3	Il percorso dell'oggetto S3 utilizzato sia per l'oggetto precedente che per quello nuovo
RSLT	Codice risultato	Risultato della transazione di sovrascrittura dell'oggetto. Il risultato è sempre: SUCS: Riuscito
SGRP	Sito (gruppo)	Se presente, l'oggetto sovrascritto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito.

S3SL: Richiesta di selezione S3

Questo messaggio registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere dettagli sul messaggio di errore e sul codice di errore. La richiesta potrebbe non essere andata a buon fine.

Codice	Campo	Descrizione
BYSC	Byte scansionati	Numero di byte scansionati (ricevuti) dai nodi di archiviazione. È probabile che BYSC e BYPR siano diversi se l'oggetto è compresso. Se l'oggetto è compresso, BYSC avrà il conteggio dei byte compressi e BYPR i byte dopo la decompressione.
BYPR	Byte elaborati	Numero di byte elaborati. Indica quanti byte di "Byte scansionati" sono stati effettivamente elaborati o utilizzati da un processo S3 Select.
BYRT	Byte restituiti	Numero di byte restituiti al client da un processo S3 Select.
RIPRISTINO	Record elaborati	Numero di record o righe che un processo S3 Select ha ricevuto dai nodi di archiviazione.
RERT	Record restituiti	Numero di record o righe che un processo S3 Select ha restituito al client.
JOFI	Lavoro terminato	Indica se l'elaborazione del lavoro S3 Select è terminata o meno. Se questo è falso, il lavoro non è stato completato e i campi di errore probabilmente conterranno dei dati. Il cliente potrebbe aver ricevuto risultati parziali o nessun risultato.
REID	ID richiesta	Identificatore per la richiesta S3 Select.
EXTM	Tempo di esecuzione	Tempo, in secondi, impiegato per completare il processo S3 Select.

Codice	Campo	Descrizione
ERMG	Messaggio di errore	Messaggio di errore generato dal processo S3 Select.
ERTY	Tipo di errore	Tipo di errore generato dal processo S3 Select.
PRIMO	Stacktrace degli errori	Stacktrace di errore generato dal processo S3 Select.
S3BK	Secchio S3	Nome del bucket S3.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 dell'utente che ha inviato la richiesta.
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket.

SADD: Disabilitazione controllo sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha disattivato la registrazione dei messaggi di controllo; i messaggi di controllo non vengono più raccolti o recapitati.

Codice	Campo	Descrizione
AETM	Abilita metodo	Metodo utilizzato per disattivare l'audit.
AEUN	Nome utente	Nome utente che ha eseguito il comando per disabilitare la registrazione degli audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.

Il messaggio implica che la registrazione era precedentemente abilitata, ma ora è stata disabilitata. In genere, questa opzione viene utilizzata solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. Dopo l'attività di massa, l'audit viene ripristinato (SADE) e la possibilità di disabilitarlo viene bloccata in modo permanente.

SADE: Abilitazione controllo sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha ripristinato la registrazione dei messaggi di controllo; i messaggi di controllo vengono nuovamente raccolti e

recapitati.

Codice	Campo	Descrizione
AETM	Abilita metodo	Il metodo utilizzato per abilitare l'audit.
AEUN	Nome utente	Nome utente che ha eseguito il comando per abilitare la registrazione di controllo.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.

Il messaggio implica che la registrazione era stata precedentemente disabilitata (SADD), ma ora è stata ripristinata. In genere, questa opzione viene utilizzata solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. Dopo l'attività di massa, l'audit viene ripristinato e la possibilità di disabilitarlo viene bloccata in modo permanente.

SCMT: Commit dell'archivio oggetti

Il contenuto della griglia non viene reso disponibile o riconosciuto come memorizzato finché non viene eseguito il commit (ovvero finché non viene memorizzato in modo persistente). Il contenuto memorizzato in modo persistente è stato completamente scritto su disco e ha superato i relativi controlli di integrità. Questo messaggio viene visualizzato quando un blocco di contenuto viene salvato nell'archivio.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto impegnato nell'archiviazione permanente.
RSLT	Codice risultato	Stato al momento in cui l'oggetto è stato memorizzato sul disco: SUCS: Oggetto memorizzato correttamente.

Questo messaggio significa che un determinato blocco di contenuto è stato completamente archiviato e verificato e ora può essere richiesto. Può essere utilizzato per tracciare il flusso di dati all'interno del sistema.

SDEL: S3 ELIMINA

Quando un client S3 emette una transazione DELETE, viene effettuata una richiesta per rimuovere l'oggetto o il bucket specificato oppure per rimuovere una sotto-risorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto eliminato in byte. Le operazioni sui bucket non includono questo campo.
DMRK	Elimina ID versione marcatore	ID versione del marcatore di eliminazione creato durante l'eliminazione di un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
GFID	ID di connessione della federazione di griglia	ID di connessione della federazione di griglia associata a una richiesta di eliminazione della replica tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
GFSA	ID account sorgente della federazione di griglia	ID account del tenant sulla griglia di origine per una richiesta di eliminazione della replica tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). `x-amz-bypass-governance-retention`viene incluso automaticamente se presente nella richiesta.
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione DELETE. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito.

Codice	Campo	Descrizione
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento di carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di Livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUDM	Identificatore univoco universale per un marcatore di eliminazione	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 in seguito a una richiesta di eliminazione di un oggetto e UUID indica un oggetto.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID della versione specifica di un oggetto che è stato eliminato. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SGET: S3 GET

Quando un client S3 emette una transazione GET, viene effettuata una richiesta per recuperare un oggetto o elencare gli oggetti in un bucket, oppure 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	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.

Codice	Campo	Descrizione
CSIZ	Dimensione del 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 registrate, selezionati durante la configurazione. `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
LITÀ	ListObjectsV2	È stata richiesta una risposta in formato v2. Per i dettagli, vedere "AWS ListObjectsV2" . Solo per operazioni bucket GET.
NCHD	Numero di bambini	Include chiavi e prefissi comuni. Solo per operazioni bucket GET.
RANG	Lettura dell'intervallo	Solo per operazioni di lettura dell'intervallo. Indica l'intervallo di byte letti da questa richiesta. Il valore dopo la barra (/) indica la dimensione dell'intero oggetto.
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando.

Codice	Campo	Descrizione
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
Repubblica Ceca del Nord	Troncato o non troncato	Impostare su false se sono stati restituiti tutti i risultati. Impostare su true se sono disponibili più risultati da restituire. Solo per operazioni bucket GET.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	L'ID della versione specifica di un oggetto richiesto. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Quando un client S3 emette una transazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un oggetto o di un 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	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto controllato 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 registrate, selezionati durante la configurazione. <code>`X-Forwarded-For`</code> viene automaticamente incluso se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	L'ID della versione specifica di un oggetto richiesto. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SPOS: S3 POST

Quando un client S3 invia una richiesta POST Object, questo messaggio viene inviato dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). (Non previsto per SPOS).
RSLT	Codice risultato	Risultato della richiesta RestoreObject. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando. Impostare su "seleziona" per un'operazione di selezione S3.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SRCF	Configurazione delle sottorisorse	Ripristinare le informazioni.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	L'ID della versione specifica di un oggetto richiesto. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SPUT: S3 PUT

Quando un client S3 emette una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o bucket oppure per rimuovere una sotto-risorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CMPS	Impostazioni di conformità	Le impostazioni di conformità utilizzate durante la creazione del bucket, se presenti nella richiesta (troncate ai primi 1024 caratteri).
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
GFID	ID di connessione della federazione di griglia	ID di connessione della federazione di griglia associata a una richiesta PUT di replicazione tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
GFSA	ID account sorgente della federazione di griglia	ID account del tenant sulla griglia di origine per una richiesta PUT di replica tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. <code>`X-Forwarded-For`</code> viene automaticamente incluso se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). <code>`x-amz-bypass-governance-retention`</code> viene incluso automaticamente se presente nella richiesta.

Codice	Campo	Descrizione
LKEN	Blocco oggetto abilitato	Valore dell'intestazione della richiesta <code>x-amz-bucket-object-lock-enabled</code> , se presente nella richiesta.
LKLH	Blocco oggetto in attesa legale	Valore dell'intestazione della richiesta <code>x-amz-object-lock-legal-hold</code> , se presente nella richiesta PutObject.
LKMD	Modalità di mantenimento del blocco degli oggetti	Valore dell'intestazione della richiesta <code>x-amz-object-lock-mode</code> , se presente nella richiesta PutObject.
LKRU	Blocco oggetto Conserva fino alla data	Valore dell'intestazione della richiesta <code>x-amz-object-lock-retain-until-date</code> , se presente nella richiesta PutObject. I valori sono limitati a 100 anni dalla data in cui l'oggetto è stato ingerito.
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.

Codice	Campo	Descrizione
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SRCF	Configurazione delle sottorisorse	La nuova configurazione delle sottorisorse (troncata ai primi 1024 caratteri).
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
ULID	Carica ID	Incluso solo nei messaggi SPUT per le operazioni CompleteMultipartUpload. Indica che tutte le parti sono state caricate e assemblate.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.
VSST	Stato di controllo delle versioni	Il nuovo stato di controllo delle versioni di un bucket. Vengono utilizzati due stati: "abilitato" o "sospeso". Le operazioni sugli oggetti non includono questo campo.

SREM: Rimozione dell'archivio oggetti

Questo messaggio viene visualizzato quando il contenuto viene rimosso dall'archiviazione persistente e non è più accessibile tramite le API standard.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto eliminato dalla memoria permanente.
RSLT	Codice risultato	Indica il risultato delle operazioni di rimozione del contenuto. L'unico valore definito è: SUCS: Contenuto rimosso dall'archiviazione persistente

Questo messaggio di controllo indica che un determinato blocco di contenuto è stato eliminato da un nodo e non può più essere richiesto direttamente. Il messaggio può essere utilizzato per tracciare il flusso di contenuti eliminati 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	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta, durante l'aggiornamento delle impostazioni di conformità di un bucket.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato 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 registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUCS: riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID della versione specifica di un oggetto i cui metadati sono stati aggiornati. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SVRF: Errore di verifica dell'archivio oggetti

Questo messaggio viene visualizzato 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 sul disco, vengono eseguiti diversi controlli di verifica e integrità per garantire che i dati inviati all'utente richiedente siano identici ai dati originariamente inseriti nel sistema. Se uno di questi controlli fallisce, il sistema mette automaticamente in quarantena i dati dell'oggetto replicato corrotti 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.

Codice	Campo	Descrizione
RSLT	Codice risultato	Tipo di errore di verifica: CRCF: Controllo di ridondanza ciclico (CRC) non riuscito. HMAC: controllo del codice di autenticazione dei messaggi basato su hash (HMAC) non riuscito. EHSR: Hash del contenuto crittografato inaspettato. PHSR: Hash del contenuto originale inaspettato. SEQC: sequenza di dati errata sul disco. PERR: Struttura non valida del file su disco. DERR: Errore del disco. FNAM: Nome file errato.



Questo messaggio deve essere monitorato attentamente. Gli errori nella verifica del contenuto possono indicare imminenti guasti hardware.

Per determinare quale operazione ha attivato il messaggio, vedere il valore del campo AMID (ID modulo). Ad esempio, un valore SVFY indica che il messaggio è stato generato dal modulo Storage Verifier, ovvero una verifica in background, mentre STOR indica che il messaggio è stato attivato dal recupero del contenuto.

SVRU: Verifica archivio oggetti sconosciuto

Il componente di archiviazione del servizio LDR esegue continuamente la scansione di tutte le copie dei dati degli oggetti replicati nell'archivio oggetti. Questo messaggio viene visualizzato quando una copia sconosciuta o imprevista di dati di oggetti replicati viene rilevata nell'archivio oggetti e spostata nella directory di quarantena.

Codice	Campo	Descrizione
FPTH	Percorso del file	Percorso del file della copia dell'oggetto inaspettato.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato 'NONE' anziché 'SUCC' in modo che il messaggio non venga filtrato.



Il messaggio di controllo SVRU: Object Store Verify Unknown deve essere monitorato attentamente. Significa che sono state rilevate copie inaspettate di dati oggetto nell'archivio oggetti. Questa situazione dovrebbe essere indagata immediatamente per stabilire come sono state create queste copie, perché potrebbe indicare imminenti guasti hardware.

SYSD: arresto del nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto l'arresto. In genere questo messaggio viene inviato solo dopo un successivo riavvio, perché 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	Arresto pulito	La natura della chiusura: SUCS: Il sistema è stato spento correttamente.

Il messaggio non indica se il server host è stato arrestato, ma solo il servizio di reporting. L'RSLT di un SYSD non può indicare uno spegnimento "sporco", perché il messaggio viene generato solo da spegnimenti "puliti".

SYST: Arresto del nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto l'arresto e che il servizio ha avviato la sequenza di arresto. SYST può essere utilizzato per determinare se l'arresto è stato richiesto prima del riavvio del servizio (a differenza di SYSD, che in genere viene inviato dopo il riavvio del servizio).

Codice	Campo	Descrizione
RSLT	Arresto pulito	La natura della chiusura: SUCS: Il sistema è stato spento correttamente.

Il messaggio non indica se il server host è stato arrestato, ma solo il servizio di reporting. Il codice RSLT di un messaggio SYST non può indicare uno spegnimento "sporco", perché il messaggio viene generato solo da spegnimenti "puliti".

SYSU: Avvio del nodo

Quando un servizio viene riavviato, questo messaggio viene generato per indicare se l'arresto precedente è stato pulito (comandato) o disordinato (inaspettato).

Codice	Campo	Descrizione
RSLT	Arresto pulito	La natura della chiusura: SUCS: Il sistema è stato spento correttamente. DSDN: Il sistema non è stato arrestato 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 discontinuità nella traccia di controllo.
- Determinare se un servizio non funziona correttamente durante il funzionamento (poiché la natura distribuita del sistema StorageGRID può mascherare questi guasti). Server Manager riavvia automaticamente un servizio non riuscito.

WDEL: CANCELLA rapida

Quando un client Swift emette una transazione DELETE, viene effettuata una richiesta per rimuovere l'oggetto o il contenitore specificato. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto eliminato in byte. Le operazioni sui contenitori non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. <code>`X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</code>
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.
RSLT	Codice risultato	Risultato della transazione DELETE. Il risultato è sempre: SUCS: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato 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.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.

Codice	Campo	Descrizione
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni sui contenitori non includono questo campo.
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

WGET: GET rapido

Quando un client Swift emette una transazione GET, viene effettuata una richiesta per recuperare un oggetto, elencare gli oggetti in un contenitore o elencare i contenitori in un account. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni su account e contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e contenitori non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. <code>`X-Forwarded-For`</code> viene automaticamente incluso se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre SUCS: riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni su account e contenitori non includono questo campo.
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

WHEA: TESTA Veloce

Quando un client Swift emette una transazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un account, di un contenitore o di un oggetto e recuperare eventuali metadati rilevanti. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni su account e contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e contenitori non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
RSLT	Codice risultato	Risultato della transazione HEAD. Il risultato è sempre: SUCS: riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni su account e contenitori non includono questo campo.
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

WPUT: PUT rapido

Quando un client Swift emette una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o contenitore. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui contenitori non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUCS: riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni sui contenitori non includono questo campo.

Codice	Campo	Descrizione
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

Espandi una griglia

Tipi di espansione

È possibile espandere la capacità o le funzionalità del sistema StorageGRID senza interrompere le operazioni del sistema.

Un'espansione StorageGRID consente di aggiungere:

- Volumi di archiviazione su nodi di archiviazione
- Nuovi nodi della griglia in un sito esistente
- Un sito completamente nuovo

Il motivo per cui si esegue l'espansione determina quanti nuovi nodi di ciascun tipo è necessario aggiungere e la posizione di tali nuovi nodi. Ad esempio, i requisiti dei nodi sono diversi se si esegue un'espansione per aumentare la capacità di archiviazione, aggiungere capacità di metadati o aggiungere ridondanza o nuove funzionalità.

Segui i passaggi per il tipo di espansione che stai eseguendo:

Aggiungere volumi di archiviazione

Segui i passaggi per [aggiunta di volumi di archiviazione ai nodi di archiviazione](#) .

Aggiungi nodi della griglia

1. Segui i passaggi per [aggiunta di nodi della griglia a un sito esistente](#) .
2. ["Aggiorna le subnet"](#) .
3. Distribuisci nodi della griglia:
 - ["Elettrodomestici"](#)
 - ["VMware"](#)
 - ["Linux"](#)



Con "Linux" si intende una distribuzione Red Hat Enterprise Linux, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Strumento matrice di interoperabilità NetApp \(IMT\)"](#) .

4. ["Eseguire l'espansione"](#) .
5. ["Configurare il sistema espanso"](#) .

Aggiungi nuovo sito

1. Segui i passaggi per [Aggiungere un nuovo sito](#) .
2. ["Aggiorna le subnet"](#) .
3. Distribuisci nodi della griglia:
 - ["Elettrodomestici"](#)
 - ["VMware"](#)
 - ["Linux"](#)



Con "Linux" si intende una distribuzione Red Hat Enterprise Linux, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Strumento matrice di interoperabilità NetApp \(IMT\)"](#) .

4. ["Eseguire l'espansione"](#) .
5. ["Configurare il sistema espanso"](#) .

Pianifica l'espansione StorageGRID

Aggiungere capacità di archiviazione

Linee guida per l'aggiunta di capacità dell'oggetto

È possibile espandere la capacità di archiviazione degli oggetti del sistema StorageGRID aggiungendo volumi di archiviazione ai nodi di archiviazione esistenti oppure aggiungendo nuovi nodi di archiviazione ai siti esistenti. È necessario aggiungere capacità di archiviazione in modo da soddisfare i requisiti della politica di gestione del

ciclo di vita delle informazioni (ILM).

Linee guida per l'aggiunta di volumi di archiviazione

Prima di aggiungere volumi di archiviazione ai nodi di archiviazione esistenti, rivedere le seguenti linee guida e limitazioni:

- È necessario esaminare le attuali regole ILM per determinare dove e quando ["aggiungere volumi di archiviazione"](#) per aumentare lo spazio di archiviazione disponibile per ["oggetti replicati"](#) O ["oggetti con codice di cancellazione"](#) .
- Non è possibile aumentare la capacità dei metadati del sistema aggiungendo volumi di archiviazione perché i metadati degli oggetti vengono archiviati solo sul volume 0.
- Ogni nodo di archiviazione basato su software può supportare un massimo di 48 volumi di archiviazione. Se è necessario aggiungere ulteriore capacità, è necessario aggiungere nuovi nodi di archiviazione.
- È possibile aggiungere uno o due ripiani di espansione a ciascun apparecchio SG6060. Ogni ripiano di espansione aggiunge 16 volumi di stoccaggio. Con entrambi i ripiani di espansione installati, l'SG6060 può supportare un totale di 48 volumi di archiviazione.
- È possibile aggiungere uno o due ripiani di espansione a ciascun elettrodomestico SG6160. Ogni ripiano di espansione aggiunge 60 volumi di stoccaggio. Con entrambi i ripiani di espansione installati, l'SG6160 può supportare un totale di 180 volumi di archiviazione.
- Non è possibile aggiungere volumi di archiviazione ad altri dispositivi di archiviazione.
- Non è possibile aumentare le dimensioni di un volume di archiviazione esistente.
- Non è possibile aggiungere volumi di archiviazione a un nodo di archiviazione contemporaneamente all'esecuzione di un aggiornamento del sistema, di un'operazione di ripristino o di un'altra espansione.

Dopo aver deciso di aggiungere volumi di archiviazione e aver determinato quali nodi di archiviazione è necessario espandere per soddisfare i criteri ILM, seguire le istruzioni per il tipo di nodo di archiviazione:

- Per aggiungere uno o due ripiani di espansione a un dispositivo di archiviazione SG6060, vai a ["Aggiungere uno scaffale di espansione al SG6060 distribuito"](#) .
- Per aggiungere uno o due ripiani di espansione a un dispositivo di archiviazione SG6160, vai a ["Aggiungere uno scaffale di espansione al SG6160 distribuito"](#)
- Per un nodo basato su software, seguire le istruzioni per ["aggiunta di volumi di archiviazione ai nodi di archiviazione"](#) .

Linee guida per l'aggiunta di nodi di archiviazione

Prima di aggiungere nodi di archiviazione ai siti esistenti, rivedere le seguenti linee guida e limitazioni:

- È necessario esaminare le attuali regole ILM per determinare dove e quando aggiungere nodi di archiviazione per aumentare lo spazio di archiviazione disponibile per ["oggetti replicati"](#) O ["oggetti con codice di cancellazione"](#) .
- Non dovresti aggiungere più di 10 nodi di archiviazione in una singola procedura di espansione.
- È possibile aggiungere nodi di archiviazione a più siti con un'unica procedura di espansione.
- È possibile aggiungere nodi di archiviazione e altri tipi di nodi in un'unica procedura di espansione.
- Prima di avviare la procedura di espansione, è necessario confermare che tutte le operazioni di riparazione dei dati eseguite come parte di un ripristino siano state completate. Vedere ["Controlla i lavori di riparazione dei dati"](#) .

- Se è necessario rimuovere i nodi di archiviazione prima o dopo aver eseguito un'espansione, non si dovrebbero dismettere più di 10 nodi di archiviazione in un'unica procedura di dismissione del nodo.

Linee guida per il servizio ADC sui nodi di archiviazione

Durante la configurazione dell'espansione, è necessario scegliere se includere il servizio Administrative Domain Controller (ADC) su ogni nuovo nodo di archiviazione. Il servizio ADC tiene traccia della posizione e della disponibilità dei servizi di rete.

- Il sistema StorageGRID richiede un ["quorum dei servizi ADC"](#) essere disponibili in ogni sede e in ogni momento.
- Almeno tre nodi di archiviazione in ogni sito devono includere il servizio ADC.
- Non è consigliabile aggiungere il servizio ADC a ogni nodo di archiviazione. L'inclusione di troppi servizi ADC può causare rallentamenti dovuti all'aumento della quantità di comunicazioni tra i nodi.
- Una singola griglia non dovrebbe avere più di 48 nodi di archiviazione 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, è necessario selezionare **Automatico**. Selezionare **Sì** solo se il nuovo nodo sostituirà un altro nodo di archiviazione che include il servizio ADC. Poiché non è possibile dismettere un nodo di archiviazione se rimangono troppo pochi servizi ADC, ciò garantisce che un nuovo servizio ADC sia disponibile prima che il vecchio servizio venga rimosso.
- Non è possibile aggiungere il servizio ADC a un nodo dopo averlo distribuito.

Aggiungere capacità di archiviazione per oggetti replicati

Se la policy di gestione del ciclo di vita delle informazioni (ILM) per la distribuzione include una regola che crea copie replicate degli oggetti, è necessario valutare la quantità di spazio di archiviazione da aggiungere e dove aggiungere i nuovi volumi di archiviazione o nodi di archiviazione.

Per indicazioni su dove aggiungere ulteriore spazio di archiviazione, esaminare le regole ILM che creano copie replicate. Se le regole ILM creano due o più copie di oggetti, pianificare di aggiungere spazio di archiviazione in ogni posizione in cui vengono create le copie di oggetti. Come semplice esempio, se si dispone di una griglia a due siti e di una regola ILM che crea una copia dell'oggetto in ciascun sito, è necessario ["aggiungere spazio di archiviazione"](#) a ciascun sito per aumentare la capacità complessiva degli oggetti della rete. Per informazioni sulla replicazione degli oggetti, vedere ["Che cosa è la replicazione"](#).

Per motivi di prestazioni, dovresti cercare di bilanciare la capacità di archiviazione e la potenza di elaborazione tra i siti. Pertanto, per questo esempio, dovresti aggiungere lo stesso numero di nodi di archiviazione a ciascun sito oppure volumi di archiviazione aggiuntivi in ciascun sito.

Se si dispone di una policy ILM più complessa che include regole che posizionano gli oggetti in posizioni diverse in base a criteri quali il nome del bucket o regole che modificano le posizioni degli oggetti nel tempo, l'analisi di dove è necessario lo storage per l'espansione sarà simile, ma più complessa.

Visualizzare graficamente la velocità con cui viene consumata la capacità di archiviazione complessiva può aiutare a capire quanto spazio di archiviazione aggiungere nell'espansione e quando sarà necessario ulteriore spazio di archiviazione. Puoi usare Grid Manager per ["monitorare e tracciare la capacità di archiviazione"](#).

Quando si pianifica la tempistica di un'espansione, bisogna tenere presente quanto tempo potrebbe essere necessario per procurarsi e installare ulteriore spazio di archiviazione.

Aggiungere capacità di archiviazione per oggetti con codice di cancellazione

Se la policy ILM include una regola che crea copie con codice di cancellazione, è necessario pianificare dove e quando aggiungere nuovo spazio di archiviazione. La quantità di spazio di archiviazione aggiunto e la tempistica dell'aggiunta possono influire sulla capacità di archiviazione utilizzabile della rete.

Il primo passo nella pianificazione di un'espansione dello storage è esaminare le regole della policy ILM che creano oggetti con codice di cancellazione. Poiché StorageGRID crea $k+m$ frammenti per ogni oggetto con codice di cancellazione e memorizza ogni frammento su un nodo di archiviazione diverso, è necessario assicurarsi che almeno $k+m$ nodi di archiviazione dispongano di spazio per i nuovi dati con codice di cancellazione dopo l'espansione. Se il profilo di codifica di cancellazione fornisce protezione contro la perdita del sito, è necessario aggiungere spazio di archiviazione a ciascun sito. Vedere ["Cosa sono gli schemi di codifica di cancellazione"](#) per informazioni sui profili di codifica di cancellazione.

Il numero di nodi da aggiungere dipende anche da quanto sono pieni i nodi esistenti quando si esegue l'espansione.

Raccomandazione generale per l'aggiunta di capacità di archiviazione per oggetti con codice di cancellazione

Se si desidera evitare calcoli dettagliati, è possibile aggiungere due nodi di archiviazione per sito quando i nodi di archiviazione esistenti raggiungono il 70% della capacità.

Questa raccomandazione generale fornisce risultati ragionevoli in un'ampia gamma di schemi di codifica di cancellazione sia per griglie a sito singolo sia per griglie in cui la codifica di cancellazione fornisce protezione contro la perdita del sito.

Per comprendere meglio i fattori che hanno portato a questa raccomandazione o per sviluppare un piano più preciso per il tuo sito, consulta ["Considerazioni per il ribilanciamento dei dati codificati con cancellazione"](#). Per una raccomandazione personalizzata ottimizzata per la tua situazione, contatta il tuo consulente NetApp Professional Services.

Considerazioni per il ribilanciamento dei dati codificati con cancellazione

Se si esegue un'espansione per aggiungere nodi di archiviazione e si utilizzano regole ILM per cancellare i dati del codice, potrebbe essere necessario eseguire la procedura di ribilanciamento del codice di cancellazione (EC) se non è possibile aggiungere un numero sufficiente di nodi di archiviazione per lo schema di codice di cancellazione utilizzato.

Dopo aver esaminato queste considerazioni, esegui l'espansione e poi vai a ["Ribilancia i dati codificati tramite cancellazione dopo l'aggiunta di nodi di archiviazione"](#) per eseguire la procedura.

Che cosa è il ribilanciamento della CE?

Il ribilanciamento EC è una procedura StorageGRID che potrebbe essere necessaria dopo l'espansione di un nodo di archiviazione. La procedura viene eseguita come script da riga di comando dal nodo di amministrazione primario. Quando si esegue la procedura di ribilanciamento EC, StorageGRID ridistribuisce i frammenti con codice di cancellazione tra i nodi di archiviazione esistenti e quelli appena aggiunti in un sito.

La procedura di riequilibrio della CE:

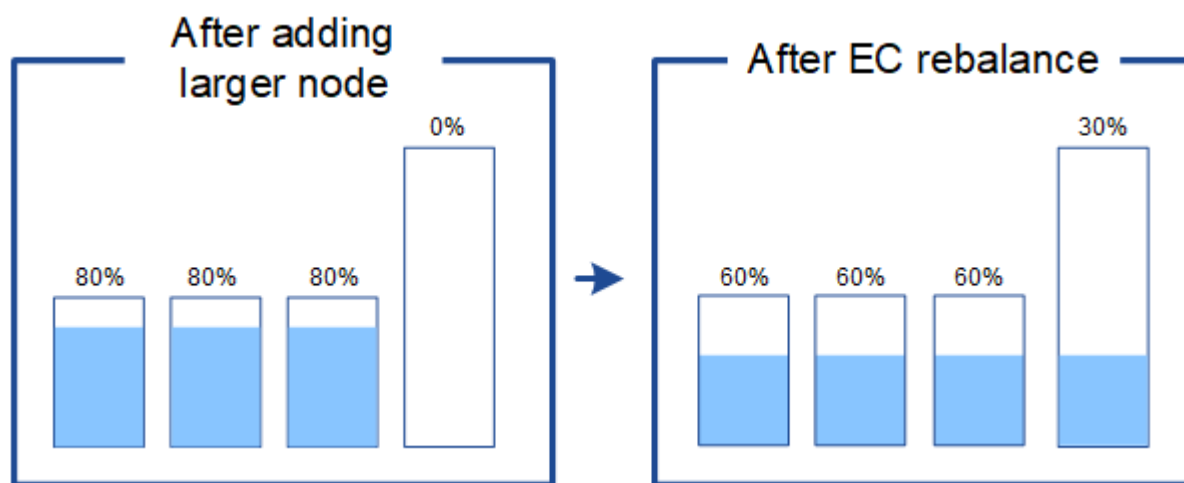
- Sposta solo i dati degli oggetti con codice di cancellazione. Non sposta i dati degli oggetti replicati.

- Ridistribuisce i dati all'interno di un sito. Non sposta dati tra siti.
- Ridistribuisce i dati tra tutti i nodi di archiviazione di un sito. Non ridistribuisce i dati all'interno dei volumi di archiviazione.
- Non considera l'utilizzo dei dati replicati su ciascun nodo di archiviazione quando si determina dove spostare i dati codificati in modo da essere cancellati.
- Ridistribuisce i dati codificati in modo uniforme tra i nodi di archiviazione senza considerare le capacità relative di ciascun nodo.
- Non distribuirà i dati con codice di cancellazione ai nodi di archiviazione pieni per oltre l'80%.
- Potrebbe ridurre le prestazioni delle operazioni ILM e delle operazioni client S3 durante l'esecuzione. Sono necessarie risorse aggiuntive per ridistribuire i frammenti di codifica di cancellazione.

Una volta completata la procedura di ribilanciamento della CE:

- I dati con codice di cancellazione verranno spostati dai nodi di archiviazione con meno spazio disponibile ai nodi di archiviazione con più spazio disponibile.
- La protezione dei dati degli oggetti con codice di cancellazione rimarrà invariata.
- I valori utilizzati (%) potrebbero essere diversi tra i nodi di archiviazione per due motivi:
 - Le copie degli oggetti replicati continueranno a consumare spazio sui nodi esistenti: la procedura di ribilanciamento EC non sposta i dati replicati.
 - I nodi con capacità maggiore saranno relativamente meno pieni rispetto ai nodi con capacità minore, anche se tutti i nodi finiranno con circa la stessa quantità di dati codificati in modo da essere cancellati.

Ad esempio, supponiamo che tre nodi da 200 TB siano riempiti all'80% ($200 \pm 0,8 = 160$ TB su ciascun nodo, ovvero 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 approssimativamente la stessa quantità di dati del codice di cancellazione ($480/4 = 120$ TB). Tuttavia, la percentuale utilizzata per il nodo più grande sarà inferiore alla percentuale utilizzata per i nodi più piccoli.



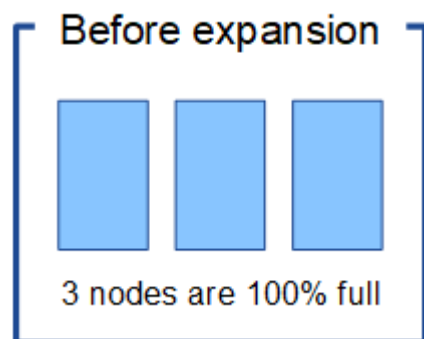
Quando ribilanciare i dati codificati con cancellazione

Consideriamo il seguente scenario:

- StorageGRID è in esecuzione in un unico sito, che contiene tre nodi di archiviazione.
- La policy ILM utilizza una regola di codifica di cancellazione 2+1 per tutti gli oggetti più grandi di 1,0 MB e

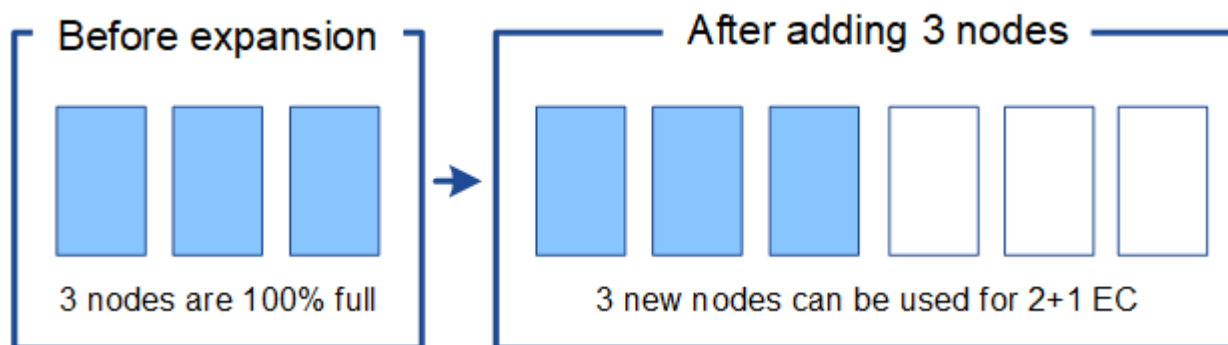
una regola di replica a 2 copie per gli oggetti più piccoli.

- Tutti i nodi di archiviazione sono completamente pieni. L'avviso **Archiviazione oggetti insufficiente** è stato attivato al livello di gravità maggiore.



Il ribilanciamento non è necessario se si aggiungono abbastanza nodi

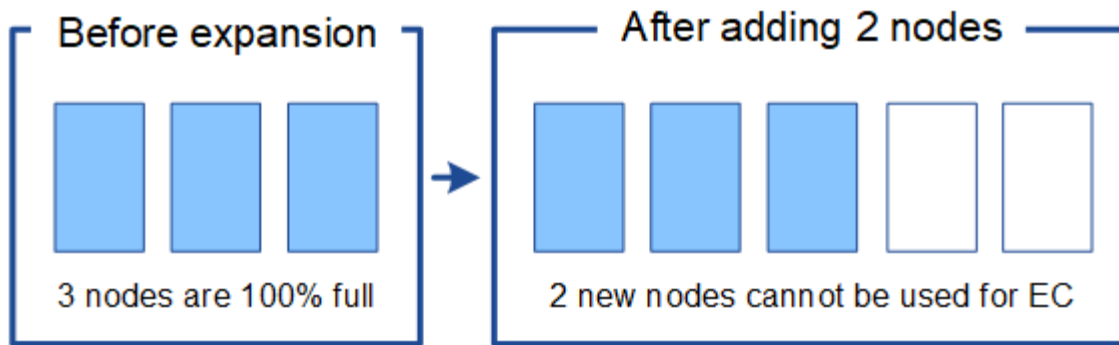
Per capire quando non è necessario il ribilanciamento EC, supponiamo di aver aggiunto tre (o più) nuovi nodi di archiviazione. In questo caso non è necessario eseguire il ribilanciamento EC. I nodi di archiviazione originali rimarranno pieni, ma i nuovi oggetti utilizzeranno i tre nuovi nodi per la codifica di cancellazione 2+1: i due frammenti di dati e il frammento di parità possono essere archiviati ciascuno su un nodo diverso.



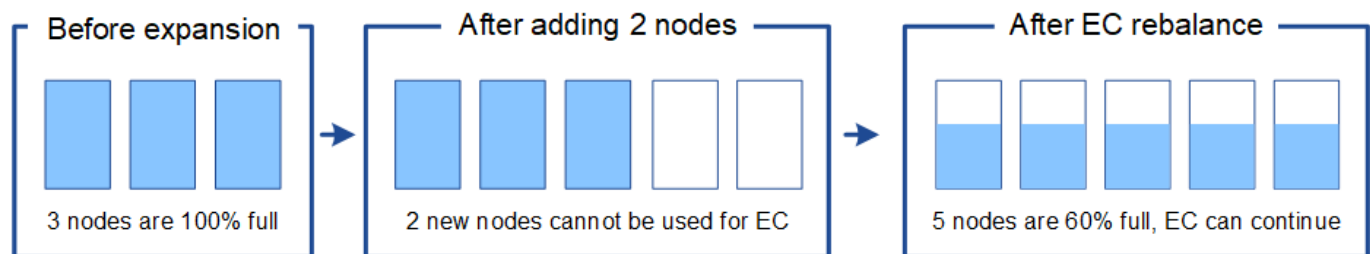
Sebbene in questo caso sia possibile eseguire la procedura di ribilanciamento EC, lo spostamento dei dati con codice di cancellazione esistenti ridurrà temporaneamente le prestazioni della griglia, il che potrebbe avere un impatto sulle operazioni del client.

È necessario ribilanciare se non è possibile aggiungere abbastanza nodi

Per capire quando è necessario il ribilanciamento EC, supponiamo di poter aggiungere solo due nodi di archiviazione anziché tre. Poiché lo schema 2+1 richiede che almeno tre nodi di archiviazione abbiano spazio disponibile, i nodi vuoti non possono essere utilizzati per nuovi dati con codice di cancellazione.



Per utilizzare i nuovi nodi di archiviazione, è necessario eseguire la procedura di ribilanciamento EC. Quando questa procedura viene eseguita, StorageGRID ridistribuisce i dati codificati in modo da essere cancellati e i frammenti di parità tra tutti i nodi di archiviazione del sito. In questo esempio, una volta completata la procedura di ribilanciamento EC, tutti e cinque i nodi sono ora pieni solo al 60% e gli oggetti possono continuare a essere inseriti nello schema di codifica di cancellazione 2+1 su tutti i nodi di archiviazione.



Raccomandazioni per il riequilibrio della CE

NetApp richiede il ribilanciamento EC se *tutte* le seguenti affermazioni sono vere:

- Per i dati degli oggetti si utilizza la codifica di cancellazione.
- L'avviso **Low Object Storage** è stato attivato per uno o più nodi di archiviazione in un sito, indicando che i nodi sono pieni all'80% o più.
- Non è possibile aggiungere un numero sufficiente di nuovi nodi di archiviazione per lo schema di codifica di cancellazione in uso. Vedere ["Aggiungere capacità di archiviazione per oggetti con codice di cancellazione"](#).
- I client S3 possono tollerare prestazioni inferiori per le operazioni di scrittura e lettura mentre è in esecuzione la procedura di ribilanciamento EC.

Facoltativamente, è possibile eseguire la procedura di ribilanciamento EC se si preferisce che i nodi di archiviazione siano riempiti a livelli simili e i client S3 possono tollerare prestazioni inferiori per le operazioni di scrittura e lettura mentre è in esecuzione la procedura di ribilanciamento EC.

Come la procedura di ribilanciamento EC interagisce con altre attività di manutenzione

Non è possibile eseguire determinate procedure di manutenzione contemporaneamente alla procedura di ribilanciamento EC.

Procedura	Consentito durante la procedura di ribilanciamento della CE?
Ulteriori procedure di ribilanciamento della CE	NO. È possibile eseguire una sola procedura di ribilanciamento EC alla volta.
Procedura di dismissione Lavoro di riparazione dei dati EC	NO. • Non è possibile avviare una procedura di dismissione 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 dismissione del nodo di archiviazione o una riparazione dei dati EC.
Procedura di espansione	NO. Se è necessario aggiungere nuovi nodi di archiviazione 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 aver eseguito la procedura di ribilanciamento EC. Se necessario, è possibile interrompere la procedura di ribilanciamento EC per eseguire un aggiornamento del software.
Procedura di clonazione del nodo dell'appliance	NO. Se è necessario clonare un nodo di archiviazione dell'appliance, eseguire la procedura di ribilanciamento EC dopo aver aggiunto il nuovo nodo.
Procedura di hotfix	Sì. È possibile applicare un hotfix 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 della CE interagisce con l'ILM

Mentre è in esecuzione la procedura di ribilanciamento EC, evitare di apportare modifiche ILM che potrebbero modificare la posizione degli oggetti con codice di cancellazione esistenti. Ad esempio, non iniziare a utilizzare una regola ILM che abbia un profilo di codifica di cancellazione diverso. Se è necessario apportare tali modifiche all'ILM, è necessario 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 archiviazione in ogni sito.

StorageGRID riserva spazio per i metadati degli oggetti sul volume 0 di ciascun nodo di archiviazione. In ogni sito vengono conservate tre copie di tutti i metadati degli oggetti, distribuite uniformemente tra tutti i nodi di archiviazione.

È possibile utilizzare Grid Manager per monitorare la capacità dei metadati dei nodi di archiviazione e stimare la velocità con cui tale capacità viene consumata. Inoltre, l'avviso **Archiviazione metadati insufficiente** viene attivato per un nodo di archiviazione quando lo spazio metadati utilizzato raggiunge determinate soglie.

Si noti che la capacità dei metadati degli oggetti di una griglia potrebbe essere consumata più velocemente della sua capacità di archiviazione degli oggetti, a seconda di come si utilizza la griglia. Ad esempio, se in genere si ingeriscono grandi quantità di piccoli oggetti o si aggiungono grandi quantità di metadati utente o tag agli oggetti, potrebbe essere necessario aggiungere nodi di archiviazione per aumentare la capacità dei metadati, anche se rimane una capacità di archiviazione degli oggetti sufficiente.

Per ulteriori informazioni, vedere quanto segue:

- ["Gestire l'archiviazione dei metadati degli oggetti"](#)
- ["Monitorare la capacità dei metadati degli oggetti per ogni nodo di archiviazione"](#)

Linee guida per aumentare la capacità dei metadati

Prima di aggiungere nodi di archiviazione per aumentare la capacità dei metadati, rivedere le seguenti linee guida e limitazioni:

- Supponendo che sia disponibile una capacità di archiviazione degli oggetti sufficiente, avere più spazio disponibile per i metadati degli oggetti aumenta il numero di oggetti che è possibile archiviare nel sistema StorageGRID .
- È possibile aumentare la capacità dei metadati di una griglia aggiungendo uno o più nodi di archiviazione a ciascun sito.
- Lo spazio effettivamente riservato ai metadati degli oggetti su un dato nodo di archiviazione dipende dall'opzione di archiviazione Spazio riservato ai metadati (impostazione a livello di sistema), dalla quantità di RAM allocata al nodo e dalle dimensioni del volume 0 del nodo.
- Non è possibile aumentare la capacità dei metadati aggiungendo volumi di archiviazione ai nodi di archiviazione esistenti, perché i metadati vengono archiviati 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 tuo sistema è limitata dalla capacità dei metadati del tuo sito più piccolo.
- Quando si aggiunge capacità di metadati, è necessario aggiungere lo stesso numero di nodi di archiviazione a ciascun sito.

I nodi di archiviazione solo metadati hanno requisiti hardware specifici:

- Quando si utilizzano appliance StorageGRID , i nodi solo metadati possono essere configurati solo su appliance SGF6112 con dodici unità da 1,9 TB o dodici unità da 3,8 TB.

- Quando si utilizzano nodi basati su software, le risorse dei nodi solo metadati devono corrispondere alle risorse dei nodi di archiviazione esistenti. Per esempio:
 - Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo su software devono soddisfare i seguenti requisiti minimi:
 - 128 GB di RAM
 - CPU a 8 core
 - SSD da 8 TB o spazio di archiviazione equivalente per il database Cassandra (rangedb/0)
 - Se il sito StorageGRID esistente utilizza nodi di archiviazione virtuali con 24 GB di RAM, CPU a 8 core e 3 TB o 4 TB di spazio di archiviazione dei metadati, i nodi basati solo su software devono utilizzare risorse simili (24 GB di RAM, CPU a 8 core e 4 TB di spazio di archiviazione dei metadati (rangedb/0).
- Quando si aggiunge un nuovo sito StorageGRID, la capacità totale dei metadati del nuovo sito deve corrispondere almeno ai siti StorageGRID esistenti e le risorse del nuovo sito devono corrispondere ai nodi di archiviazione nei siti StorageGRID esistenti.

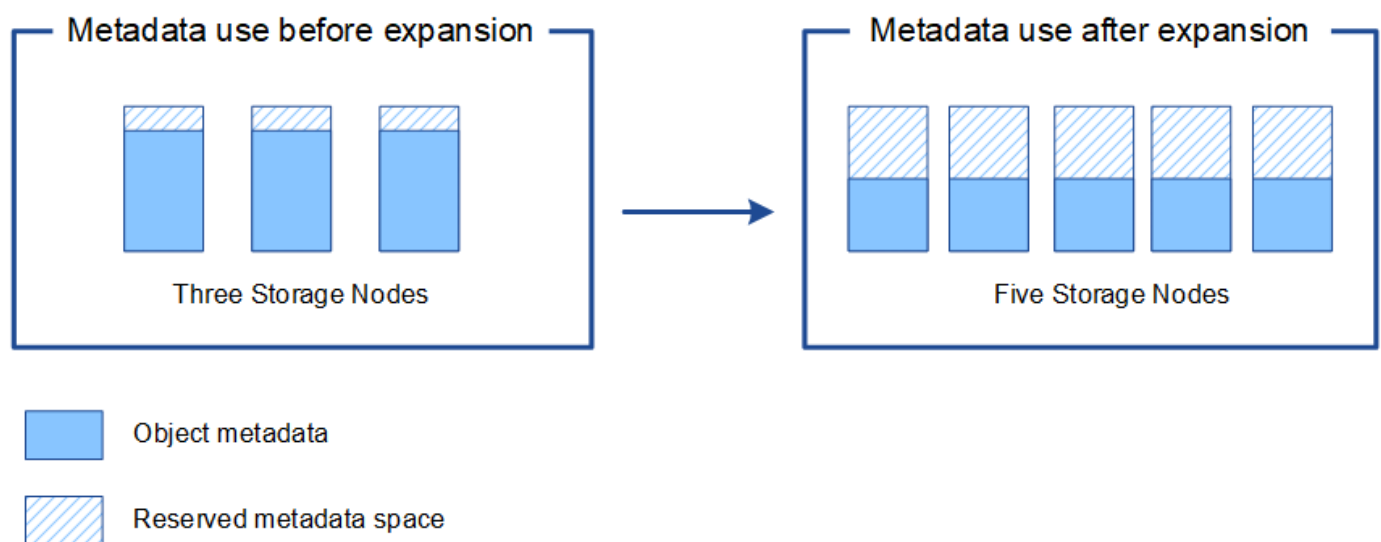
Vedi il "[descrizione di cosa è lo spazio riservato ai metadati](#)".

Come vengono ridistribuiti i metadati quando si aggiungono nodi di archiviazione

Quando si aggiungono nodi di archiviazione in un'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti ai nuovi nodi in ogni sito, aumentando così la capacità complessiva dei metadati della griglia. 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 archiviazione in un'espansione. Il lato sinistro della figura rappresenta il volume 0 di tre nodi di archiviazione prima di un'espansione. I metadati stanno consumando una porzione relativamente grande dello spazio metadati disponibile su ciascun nodo ed è stato attivato l'avviso **Spazio di archiviazione metadati insufficiente**.

Il lato destro della figura mostra come i metadati esistenti vengono ridistribuiti dopo che due nodi di archiviazione sono stati aggiunti al sito. La quantità di metadati su ciascun nodo è diminuita, l'avviso **Spazio di archiviazione metadati insufficiente** non viene più attivato e lo spazio disponibile per i metadati è aumentato.



Aggiungi nodi di griglia per aggiungere funzionalità al tuo sistema

È possibile aggiungere ridondanza o funzionalità aggiuntive a un sistema StorageGRID aggiungendo nuovi nodi della griglia ai siti esistenti.

Ad esempio, potresti scegliere di aggiungere nodi gateway da utilizzare in un gruppo ad alta disponibilità (HA) oppure potresti aggiungere un nodo di amministrazione in un sito remoto per consentire il monitoraggio tramite un nodo locale.

È possibile aggiungere uno o più dei seguenti tipi di nodi a uno o più siti esistenti in un'unica operazione di espansione:

- Nodi amministrativi non primari
- Nodi di archiviazione
- Nodi gateway

Quando ci si prepara ad aggiungere nodi alla griglia, tenere presente le seguenti limitazioni:

- Il nodo di amministrazione primario viene distribuito durante l'installazione iniziale. Non è possibile aggiungere un nodo amministrativo primario durante un'espansione.
- È possibile aggiungere nodi di archiviazione e altri tipi di nodi nella stessa espansione.
- Quando si aggiungono nodi di archiviazione, è necessario pianificare attentamente il numero e la posizione dei nuovi nodi. Vedere ["Linee guida per l'aggiunta di capacità dell'oggetto"](#).
- Se l'opzione **Imposta nuovo nodo predefinito** è **Non attendibile** nella scheda Reti client non attendibili nella pagina Controllo firewall, le applicazioni client che si connettono ai nodi di espansione tramite la rete client devono connettersi tramite una porta endpoint del bilanciatore del carico (**CONFIGURAZIONE > Sicurezza > Controllo firewall**). Vedi le istruzioni per ["modificare le impostazioni di sicurezza per il nuovo nodo"](#) e ["configurare gli endpoint del bilanciatore del carico"](#).

Aggiungi 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, esamina i seguenti requisiti e limitazioni:

- È possibile aggiungere un solo sito per ogni operazione di espansione.
- Non è possibile aggiungere nodi della griglia a un sito esistente come parte della stessa espansione.
- Tutti i siti devono includere almeno tre nodi di archiviazione.
- L'aggiunta di un nuovo sito non aumenta automaticamente il numero di oggetti che puoi archiviare. La capacità totale degli oggetti di una griglia dipende dalla quantità di spazio di archiviazione disponibile, dalla politica ILM e dalla capacità dei metadati in ciascun sito.
- Quando si dimensiona 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 l'archiviazione dei metadati degli oggetti"](#)
- ["Monitorare la capacità dei metadati degli oggetti per ogni nodo di archiviazione"](#)
- È necessario considerare la larghezza di banda di rete disponibile tra i siti e il livello di latenza della rete. Gli aggiornamenti dei metadati vengono replicati continuamente tra i siti, anche se tutti gli oggetti vengono archiviati 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 degli oggetti non vengano archiviate nel nuovo sito finché la procedura di espansione non sarà completata.

Ad esempio, prima di iniziare l'espansione, determinare se alcune regole utilizzano il pool di archiviazione predefinito (tutti i nodi di archiviazione). In tal caso, è necessario creare un nuovo pool di archiviazione contenente i nodi di archiviazione esistenti e aggiornare le regole ILM per utilizzare il nuovo pool di archiviazione. In caso contrario, gli oggetti verranno copiati nel nuovo sito non appena il primo nodo di quel sito diventerà attivo.

Per ulteriori informazioni sulla modifica di ILM quando si aggiunge un nuovo sito, vedere ["esempio di modifica di una politica ILM"](#).

Raccogli i materiali richiesti

Prima di eseguire un'operazione di espansione, raccogliere i materiali e installare e configurare qualsiasi nuovo hardware e rete.

Articolo	Note
Archivio di installazione di StorageGRID	Se si aggiungono nuovi nodi della griglia o un nuovo sito, è necessario scaricare ed estrarre l'archivio di installazione StorageGRID. È necessario utilizzare la stessa versione attualmente in esecuzione sulla griglia. Per i dettagli, vedere le istruzioni per download ed estrazione dei file di installazione StorageGRID. Nota: non è necessario scaricare file se si aggiungono nuovi volumi di archiviazione a nodi di archiviazione esistenti o si installa un nuovo dispositivo StorageGRID.
Computer portatile di servizio	Il portatile di servizio è dotato 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 recupero.

Articolo	Note
Frase segreta di provisioning	La passphrase viene creata e documentata quando il sistema StorageGRID viene installato per la prima volta. La passphrase di provisioning non è presente nel <code>Passwords.txt</code> file.
Documentazione StorageGRID	• "Amministra StorageGRID" • "Note di rilascio" • Istruzioni di installazione per la tua piattaforma ◦ "Installa StorageGRID su Red Hat Enterprise Linux" ◦ "Installa StorageGRID su Ubuntu o Debian" ◦ "Installa StorageGRID su VMware"
Documentazione attuale per la tua piattaforma	Per le versioni supportate, vedere "Strumento di matrice di interoperabilità (IMT)" .

Scarica ed estrai i file di installazione StorageGRID

Prima di poter aggiungere nuovi nodi della griglia o un nuovo sito, è necessario scaricare l'archivio di installazione StorageGRID appropriato ed estrarre i file.

Informazioni su questo compito

È necessario eseguire le operazioni di espansione utilizzando la versione di StorageGRID attualmente in esecuzione sulla griglia.

Passi

1. Vai a ["Download NetApp : StorageGRID"](#).
2. Selezionare la versione di StorageGRID attualmente in esecuzione sulla griglia.
3. Sign in 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 **Accetta e continua**.
5. Nella colonna **Installa StorageGRID** della pagina di download, seleziona `.tgz` O `.zip` file per la tua piattaforma.

La versione mostrata nel file di archivio di installazione deve corrispondere alla versione del software attualmente installato.

Utilizzare il `.zip` file se si utilizza Windows sul portatile di servizio.

Piattaforma	Archivio di installazione
Red Hat Enterprise Linux	StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .tgz

Piattaforma	Archivio di installazione
Ubuntu o Debian o Appliance	StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .tgz
VMware	StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .tgz
OpenStack/altro Hypervisor	Per espandere una distribuzione esistente su OpenStack, è necessario distribuire una macchina virtuale che esegua una delle distribuzioni Linux supportate elencate sopra e seguire le istruzioni appropriate per Linux.

- Scarica ed estrai il file di archivio.
- Segui i passaggi appropriati per la tua piattaforma per scegliere i file di cui hai bisogno, in base alla piattaforma, alla topologia della griglia pianificata e al modo in cui espanderai il tuo sistema StorageGRID .

I percorsi elencati nel passaggio per ciascuna piattaforma sono relativi alla directory di livello superiore installata dal file di archivio.

- Se si sta espandendo 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 StorageGRID .
	Una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Pacchetto RPM per l'installazione delle immagini dei nodi StorageGRID sugli host RHEL.
	Pacchetto RPM per l'installazione del servizio host StorageGRID sugli host RHEL.
Strumento di scripting di distribuzione	Descrizione
	Uno script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID .
	Uno script Python utilizzato per automatizzare la configurazione degli appliance StorageGRID .
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.

Percorso e nome del file	Descrizione
	Uno script Python di esempio che puoi utilizzare per accedere all'API di gestione della griglia quando è abilitato l'accesso singolo. È possibile utilizzare questo script anche per l'integrazione di Ping Federate.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Esempio di ruolo e playbook Ansible per la configurazione di host RHEL per la distribuzione di container StorageGRID . È possibile personalizzare il ruolo o il playbook in base alle proprie esigenze.
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO) tramite Active Directory o Ping Federate.
	Uno script di supporto chiamato dal compagno <code>storagegrid-ssoauth-azure.py</code> Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: prima di eseguire un aggiornamento, puoi utilizzare questi schemi per confermare che il codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova versione StorageGRID se non disponi di un ambiente StorageGRID non di produzione per i test di compatibilità dell'aggiornamento.

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 StorageGRID .
	Un file di licenza NetApp non di produzione che puoi utilizzare per test e distribuzioni di prova di concetto.
	Pacchetto DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.

Percorso e nome del file	Descrizione
	Checksum MD5 per il file <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Pacchetto DEB per l'installazione del servizio host StorageGRID su host Ubuntu o Debian.
Strumento di scripting di distribuzione	Descrizione
	Uno script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Uno script Python utilizzato per automatizzare la configurazione degli appliance StorageGRID.
	Uno script Python di esempio che puoi utilizzare per accedere all'API di gestione della griglia quando è abilitato l'accesso singolo. È possibile utilizzare questo script anche per l'integrazione di Ping Federate.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Esempio di ruolo e playbook Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID. È possibile personalizzare il ruolo o il playbook in base alle proprie esigenze.
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO) tramite Active Directory o Ping Federate.
	Uno script di supporto chiamato dal compagno <code>storagegrid-ssoauth-azure.py</code> Script Python per eseguire interazioni SSO con Azure.

Percorso e nome del file	Descrizione
	Schemi API per StorageGRID. Nota: prima di eseguire un aggiornamento, puoi utilizzare questi schemi per confermare che il codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova versione StorageGRID se non disponi di un ambiente StorageGRID non di produzione per i test di compatibilità dell'aggiornamento.

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 StorageGRID .
	Una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	File del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodi di griglia.
	Il file modello Open Virtualization Format(.ovf) e file manifesto(.mf) per distribuire il nodo di amministrazione primario.
	Il file modello(.ovf) e file manifesto(.mf) per distribuire nodi amministrativi non primari.
	Il file modello(.ovf) e file manifesto(.mf) per la distribuzione dei nodi gateway.
	Il file modello(.ovf) e file manifesto(.mf) per distribuire nodi di archiviazione basati su macchine virtuali.
Strumento di scripting di distribuzione	Descrizione
	Uno script shell Bash utilizzato per automatizzare la distribuzione di nodi di griglia virtuali.
	Un file di configurazione di esempio da utilizzare con <code>deploy-vsphere-ovftool.sh</code> sceneggiatura.

Percorso e nome del file	Descrizione
	Uno script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID .
	Uno script Python utilizzato per automatizzare la configurazione degli appliance StorageGRID .
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO). È possibile utilizzare questo script anche per l'integrazione di Ping Federate.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO) tramite Active Directory o Ping Federate.
	Uno script di supporto chiamato dal compagno <code>storagegrid-ssoauth-azure.py</code> Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: prima di eseguire un aggiornamento, puoi utilizzare questi schemi per confermare che il codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova versione StorageGRID se non disponi di un ambiente StorageGRID non di produzione per i test di compatibilità dell'aggiornamento.

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 dei nodi StorageGRID sui tuoi dispositivi.
	Checksum MD5 per il file <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .



Per l'installazione dell'appliance, questi file sono necessari solo se si desidera evitare il traffico di rete. L'appliance può scaricare i file richiesti dal nodo di amministrazione primario.

Verificare l'hardware e la rete

Prima di iniziare l'espansione del sistema StorageGRID , accertarsi di quanto segue:

- L'hardware necessario per supportare i nuovi nodi della griglia o il nuovo sito è stato installato e configurato.
- Tutti i nuovi nodi dispongono di percorsi di comunicazione bidirezionali verso tutti i nodi esistenti e nuovi (un requisito per la rete Grid). In particolare, verifica che le seguenti porte TCP siano aperte tra i nuovi nodi che stai aggiungendo nell'espansione e il nodo di amministrazione primario:
 - 1055
 - 7443
 - 8011
 - 10342

Vedere "[Comunicazioni interne al nodo della griglia](#)" .

- Il nodo di amministrazione primario può comunicare con tutti i server di espansione destinati a ospitare il sistema StorageGRID .
- Se uno qualsiasi dei nuovi nodi ha un indirizzo IP di rete Grid su una subnet non utilizzata in precedenza, è già stato "[aggiunta la nuova subnet](#)" all'elenco delle subnet della rete Grid. In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e ricominciare la procedura.
- Non si utilizza la traduzione degli indirizzi di rete (NAT) sulla rete Grid tra nodi della griglia o tra siti StorageGRID . Quando si utilizzano indirizzi IPv4 privati per la rete Grid, tali indirizzi devono essere direttamente instradabili da ogni nodo della griglia in ogni sito. L'utilizzo di NAT per collegare la rete Grid attraverso un segmento di rete pubblica è supportato solo se si utilizza un'applicazione di tunneling trasparente per tutti i nodi della griglia, ovvero se i nodi della griglia non richiedono la conoscenza degli indirizzi IP pubblici.

Questa restrizione NAT è specifica per i nodi della griglia e per la rete della griglia. Se necessario, è possibile utilizzare NAT tra client esterni e nodi della griglia, ad esempio per fornire un indirizzo IP pubblico per un nodo gateway.

Aggiungere volumi di archiviazione

Aggiungere volumi di archiviazione ai nodi di archiviazione

È possibile espandere la capacità di archiviazione dei nodi di archiviazione che sono al di sotto del numero massimo supportato di volumi. Potrebbe essere necessario aggiungere volumi di archiviazione a più di un nodo di archiviazione per soddisfare i requisiti ILM per copie replicate o con codice di cancellazione.

Prima di iniziare

Prima di aggiungere volumi di archiviazione, rivedere il "[linee guida per l'aggiunta di capacità di oggetti](#)" per assicurarti di sapere dove aggiungere volumi per soddisfare i requisiti della tua politica ILM.



Queste istruzioni si applicano solo ai nodi di archiviazione basati su software. Vedere ["Aggiungere uno scaffale di espansione al SG6060 distribuito"](#) o ["Aggiungere uno scaffale di espansione al SG6160 distribuito"](#) per scoprire come aggiungere volumi di archiviazione al modello SG6060 o SG6160 installando ripiani di espansione. Gli altri nodi di archiviazione dell'appliance non possono essere espansi.

Informazioni su questo compito

Lo storage sottostante di un nodo di storage è suddiviso in volumi di storage. I volumi di archiviazione sono dispositivi di archiviazione basati su blocchi formattati dal sistema StorageGRID e montati per archiviare oggetti. Ogni nodo di archiviazione può supportare fino a 48 volumi di archiviazione, denominati *archivi di oggetti* in Grid Manager.



I metadati degli oggetti vengono sempre memorizzati nell'archivio oggetti 0.

Ogni archivio di oggetti viene montato su un volume che corrisponde al suo ID. Ad esempio, l'archivio oggetti con un ID di 0000 corrisponde a `/var/local/rangedb/0` punto di montaggio.

Prima di aggiungere nuovi volumi di archiviazione, utilizzare Grid Manager per visualizzare gli archivi di oggetti correnti per ciascun nodo di archiviazione, nonché i punti di montaggio corrispondenti. È possibile utilizzare queste informazioni quando si aggiungono volumi di archiviazione.

Passi

1. Selezionare **NODI** > **sito** > **Nodo di archiviazione** > **Archiviazione**.
2. Scorrere verso il basso per visualizzare la quantità di spazio di archiviazione disponibile per ciascun volume e archivio oggetti.

Per i nodi di archiviazione dell'appliance, il nome mondiale di ciascun disco corrisponde all'identificatore mondiale del volume (WWID) visualizzato quando si visualizzano le proprietà del volume standard in SANtricity OS (il software di gestione connesso al controller di archiviazione dell'appliance).

Per aiutarti a interpretare le statistiche di lettura e scrittura del disco relative ai punti di montaggio del volume, la prima parte del nome mostrato nella colonna **Nome** della tabella Dispositivi disco (ovvero *sd*, *sdd*, *sde* e così via) corrisponde al valore mostrato nella colonna **Dispositivo** della tabella 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 per la piattaforma in uso per aggiungere nuovi volumi di archiviazione al nodo di archiviazione.
 - ["VMware: aggiungi volumi di archiviazione al nodo di archiviazione"](#)
 - ["Linux: aggiungi volumi SAN o collegati direttamente al nodo di archiviazione"](#)

VMware: aggiungi volumi di archiviazione al nodo di archiviazione

Se un nodo di archiviazione include meno di 16 volumi di archiviazione, 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 distribuzioni VMware.
 - ["Installa StorageGRID su VMware"](#)
- Tu hai il `Passwords.txt` file.
- Hai ["autorizzazioni di accesso specifiche"](#) .



Non tentare di aggiungere volumi di archiviazione a un nodo di archiviazione mentre è attivo un aggiornamento software, una procedura di ripristino o un'altra procedura di espansione.

Informazioni su questo compito

Il nodo di archiviazione non è disponibile per un breve periodo quando si aggiungono volumi di archiviazione. È necessario eseguire questa procedura su un nodo di archiviazione alla volta per evitare di influire sui servizi di griglia rivolti al client.

Passi

1. Se necessario, installare nuovo hardware di archiviazione e creare nuovi datastore VMware.
2. Aggiungere uno o più dischi rigidi alla macchina virtuale da utilizzare 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 dischi di macchine virtuali (VMDK). I VMDK sono più comunemente utilizzati e più facili da gestire, mentre gli RDM potrebbero offrire prestazioni migliori per carichi di lavoro che utilizzano dimensioni di oggetti 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 **Riavvia sistema operativo guest** in VMware vSphere Client oppure immettendo il seguente comando in una sessione ssh sulla macchina virtuale: `sudo reboot`



Non utilizzare **Spegnimento** o **Ripristino** per riavviare la macchina virtuale.

4. Configurare il nuovo storage per l'utilizzo da parte del nodo di storage:
 - a. Accedi al nodo della griglia:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password elencata nel `Passwords.txt` file.

iii. Immettere il seguente comando per passare alla root: `su -`

iv. Inserisci la password elencata nel `Passwords.txt` file. Quando si accede come root, il prompt cambia da `$` a `#`.

b. Configurare i nuovi volumi di archiviazione:

```
sudo add_rangedbs.rb
```

Questo script trova tutti i nuovi volumi di archiviazione e ti chiede di formattarli.

c. Inserisci **y** per accettare la formattazione.

d. Se uno qualsiasi dei volumi è stato precedentemente formattato, decidere se riformattarlo.

- Inserisci **y** per riformattare.
- Immettere **n** per saltare la riformattazione.

IL `setup_rangedbs.sh` lo script viene eseguito automaticamente.

5. Verificare che i servizi si avviino correttamente:

a. Visualizza un elenco dello stato di tutti i servizi sul server:

```
sudo storagegrid-status
```

Lo stato viene aggiornato automaticamente.

a. Attendi che tutti i servizi siano in esecuzione o verificati.

b. Uscire dalla schermata di stato:

```
Ctrl+C
```

6. Verificare che il nodo di archiviazione sia online:

a. Sign in a Grid Manager utilizzando un ["browser web supportato"](#).

b. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.

c. Selezionare **sito > Nodo di archiviazione > LDR > Archiviazione**.

d. Selezionare la scheda **Configurazione** e poi la scheda **Principale**.

e. Se l'elenco a discesa **Stato di archiviazione - Desiderato** è impostato su Sola lettura o Offline, selezionare **Online**.

f. Selezionare **Applica modifiche**.

7. Per vedere i nuovi archivi di oggetti:

a. Selezionare **NODI > sito > Nodo di archiviazione > Archiviazione**.

b. Visualizza i dettagli nella tabella **Archivi oggetti**.

Risultato

È possibile utilizzare la capacità estesa dei nodi di archiviazione per salvare i dati degli oggetti.

Linux: aggiungi volumi SAN o collegati direttamente al nodo di archiviazione

Se un nodo di archiviazione include meno di 48 volumi di archiviazione, è possibile

aumentarne la capacità aggiungendo nuovi dispositivi di archiviazione 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 archiviazione.

Prima di iniziare

- Hai accesso alle istruzioni per installare StorageGRID sulla tua piattaforma Linux.
 - ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
 - ["Installa StorageGRID su Ubuntu o Debian"](#)
- Tu hai il `Passwords.txt` file.
- Hai ["autorizzazioni di accesso specifiche"](#) .



Non tentare di aggiungere volumi di archiviazione a un nodo di archiviazione mentre è attivo un aggiornamento software, una procedura di ripristino o un'altra procedura di espansione.

Informazioni su questo compito

Il nodo di archiviazione non è disponibile per un breve periodo quando si aggiungono volumi di archiviazione. È necessario eseguire questa procedura su un nodo di archiviazione alla volta per evitare di influire sui servizi di griglia rivolti al client.

Passi

1. Installare il nuovo hardware di archiviazione.

Per ulteriori informazioni, consultare la documentazione fornita dal fornitore dell'hardware.

2. Creare nuovi volumi di archiviazione 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 archiviazione condivisi e consentire all'host Linux di accedervi.
 - Utilizzare lo stesso schema di denominazione persistente utilizzato per i volumi di archiviazione sul nodo di archiviazione esistente.
 - Se si utilizza la funzionalità di migrazione del nodo StorageGRID , rendere i nuovi volumi visibili agli altri host Linux che sono destinazioni di migrazione per questo nodo di archiviazione. Per ulteriori informazioni, consultare le istruzioni per l'installazione di StorageGRID per la piattaforma Linux.
3. Accedi all'host Linux che supporta il nodo di archiviazione come root o con un account che dispone dell'autorizzazione sudo.
4. Verificare che i nuovi volumi di archiviazione siano visibili sull'host Linux.

Potrebbe essere necessario ripetere la scansione dei dispositivi.

5. Eseguire il seguente comando per disabilitare temporaneamente il nodo di archiviazione:

```
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 archiviazione, che può essere trovato in `/etc/storagegrid/nodes/<node-name>.conf` .
7. Individuare la sezione del file di configurazione del nodo che contiene le mappature dei dispositivi a blocchi di archiviazione degli oggetti esistenti.

Nell'esempio, BLOCK_DEVICE_RANGEDB_00 A BLOCK_DEVICE_RANGEDB_03 sono le mappature dei dispositivi a blocchi di archiviazione degli oggetti esistenti.

```
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 archiviazione degli oggetti corrispondenti ai volumi di archiviazione dei blocchi aggiunti per questo nodo di archiviazione.

Assicurati di iniziare dal prossimo BLOCK_DEVICE_RANGEDB_nn . Non lasciare spazi vuoti.

- Sulla base dell'esempio sopra, inizia da BLOCK_DEVICE_RANGEDB_04 .
- Nell'esempio seguente, sono stati aggiunti al nodo quattro nuovi volumi di archiviazione a blocchi: 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 al file di configurazione del nodo per il nodo di archiviazione:

```
sudo storagegrid node validate <node-name>
```

Correggere eventuali errori o avvisi prima di procedere al passaggio successivo.



Se si osserva un errore simile al seguente, 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 è presente un file speciale valido per il dispositivo a blocchi (o un collegamento simbolico a un file speciale per il dispositivo a blocchi) in quella posizione.

```
Checking configuration file for node <node-name>...  
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>  
<path-name> is not a valid block device
```

Verifica di aver inserito il codice corretto <path-name> .

10. Eseguire il seguente comando per riavviare il nodo con le nuove mappature dei dispositivi a blocchi in atto:

```
sudo storagegrid node start <node-name>
```

11. Accedi al nodo di archiviazione come amministratore utilizzando la password elencata in `Passwords.txt` file.

12. Verificare che i servizi si avviino correttamente:

a. Visualizza un elenco dello stato di tutti i servizi sul server:

```
sudo storagegrid-status
```

Lo stato viene aggiornato automaticamente.

b. Attendi 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 archiviazione:

```
sudo add_rangedbs.rb
```

Questo script trova tutti i nuovi volumi di archiviazione e ti chiede di formattarli.

b. Immettere **y** per formattare i volumi di archiviazione.

c. Se uno qualsiasi dei volumi è stato precedentemente formattato, decidere se riformattarlo.

- Inserisci **y** per riformattare.
- Immettere **n** per saltare la riformattazione.

IL `setup_rangedbs.sh` lo script viene eseguito automaticamente.

14. Verificare che lo stato di archiviazione del nodo di archiviazione sia online:

- a. Sign in a Grid Manager utilizzando un ["browser web supportato"](#) .
 - b. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - c. Selezionare **sito > Nodo di archiviazione > LDR > Archiviazione**.
 - d. Selezionare la scheda **Configurazione** e poi la scheda **Principale**.
 - e. Se l'elenco a discesa **Stato di archiviazione - Desiderato** è impostato su Sola lettura o Offline, selezionare **Online**.
 - f. Fare clic su **Applica modifiche**.
15. Per vedere i nuovi archivi di oggetti:
- a. Selezionare **NODI > sito > Nodo di archiviazione > Archiviazione**.
 - b. Visualizza i dettagli nella tabella **Archivi oggetti**.

Risultato

Ora è possibile utilizzare la capacità ampliata dei nodi di archiviazione per salvare i dati degli oggetti.

Aggiungi nodi o siti della griglia

Aggiungi nodi griglia al sito esistente o aggiungi un nuovo sito

Seguire questa procedura per aggiungere nodi griglia a siti esistenti o per aggiungere un nuovo sito. È possibile eseguire solo un tipo di espansione alla volta.

Prima di iniziare

- Tu hai il ["Accesso root o autorizzazione di manutenzione"](#) .
- Tutti i nodi esistenti nella griglia sono attivi e funzionanti in tutti i siti.
- Tutte le precedenti procedure di espansione, aggiornamento, dismissione o ripristino sono state completate.



Non è possibile avviare un'espansione mentre è in corso un'altra procedura di espansione, aggiornamento, ripristino o dismissione attiva. Tuttavia, se necessario, è possibile sospendere una procedura di dismissione per avviare un'espansione.

Passi

1. ["Aggiorna le subnet per Grid Network"](#) .
2. ["Distribuisci nuovi nodi della griglia"](#) .
3. ["Eseguire l'espansione"](#) .

Aggiorna le subnet per Grid Network

Quando si aggiungono nodi della griglia o un nuovo sito in un'espansione, potrebbe essere necessario aggiornare o aggiungere subnet alla rete della griglia.

StorageGRID gestisce un elenco delle subnet di rete utilizzate per comunicare tra i nodi della griglia sulla rete Grid (eth0). Queste voci includono le subnet utilizzate per la rete Grid da ciascun sito nel sistema StorageGRID , nonché tutte le subnet utilizzate per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway della rete Grid.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[Autorizzazione di accesso alla manutenzione o alla root](#)".
- Hai la passphrase di provisioning.
- Si dispone degli indirizzi di rete, in notazione CIDR, delle subnet che si desidera configurare.

Informazioni su questo compito

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 delle subnet Grid Network prima di avviare l'espansione. In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e ricominciare la procedura.

Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete amministrativa 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

Passi

1. Selezionare **MANUTENZIONE > Rete > Rete a griglia**.
2. Selezionare **Aggiungi un'altra subnet** per aggiungere una nuova subnet in notazione CIDR.

Ad esempio, inserisci 10.96.104.0/22.

3. Immettere la passphrase di provisioning e selezionare **Salva**.
4. Attendi che le modifiche vengano applicate, quindi scarica un nuovo pacchetto di ripristino.
 - a. Selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino**.
 - b. Immettere 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. Viene utilizzato anche per recuperare il nodo di amministrazione primario.

Le subnet specificate vengono configurate automaticamente per il sistema StorageGRID .

Distribuisci nuovi nodi della griglia

I passaggi per distribuire nuovi nodi della griglia in un'espansione sono gli stessi utilizzati quando la griglia è stata installata per la prima volta. È necessario distribuire tutti i nuovi nodi della griglia prima di poter eseguire l'espansione.

Quando si espande una griglia, i nodi aggiunti non devono necessariamente corrispondere ai tipi di nodi esistenti. È possibile aggiungere nodi VMware, nodi basati su container Linux o nodi appliance.

VMware: distribuzione dei nodi della griglia

È necessario distribuire una macchina virtuale in VMware vSphere per ogni nodo VMware che si desidera aggiungere all'espansione.

Passi

1. ["Distribuisci il nuovo nodo come macchina virtuale"](#) e collegarlo a una o più reti StorageGRID .

Quando si distribuisce il nodo, è possibile rimappare le porte del nodo o aumentare le impostazioni della CPU o della memoria.

2. Dopo aver distribuito tutti i nuovi nodi VMware, ["eseguire la procedura di espansione"](#) .

Linux: Distribuisci nodi di griglia

È possibile distribuire i nodi della griglia su nuovi host Linux o su host Linux esistenti. Se hai bisogno di host Linux aggiuntivi per supportare i requisiti di CPU, RAM e storage dei nodi StorageGRID che vuoi aggiungere alla tua griglia, puoi prepararli nello stesso modo in cui hai preparato gli host quando li hai installati per la prima volta. Quindi, distribuisce i nodi di espansione nello stesso modo in cui hai distribuito i nodi della griglia durante l'installazione.

Prima di iniziare

- Hai le istruzioni per installare StorageGRID per la tua versione di Linux e hai esaminato i requisiti hardware e di archiviazione.
 - ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
 - ["Installa StorageGRID su Ubuntu o Debian"](#)
- Se si prevede di distribuire nuovi nodi della griglia su host esistenti, è necessario verificare che gli host esistenti dispongano di CPU, RAM e capacità di archiviazione sufficienti per i nodi aggiuntivi.
- Hai un piano per ridurre al minimo i domini di errore. Ad esempio, non dovresti distribuire tutti i nodi gateway su un singolo host fisico.



In una distribuzione di produzione, non eseguire più di un nodo di archiviazione su un singolo host fisico o virtuale. Utilizzando un host dedicato per ogni nodo di archiviazione si ottiene un dominio di errore isolato.

- Se il nodo StorageGRID utilizza storage assegnato da un sistema NetApp ONTAP , verificare che il volume non abbia un criterio di suddivisione in livelli FabricPool abilitato. La disattivazione della suddivisione in livelli FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di archiviazione.

Passi

1. Se si aggiungono nuovi host, accedere alle istruzioni di installazione per la distribuzione dei nodi StorageGRID .
2. Per distribuire i nuovi host, seguire le istruzioni per la preparazione degli host.
3. Per creare file di configurazione dei nodi e convalidare la configurazione StorageGRID , seguire le istruzioni per la distribuzione dei nodi della griglia.
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>]`

Dopo aver finito

Dopo aver distribuito tutti i nuovi nodi della griglia, puoi ["eseguire l'espansione"](#) .

Appliance: distribuzione di storage, gateway o nodi amministrativi non primari

Per installare il software StorageGRID su un nodo appliance, utilizzare StorageGRID Appliance Installer, 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 gateway o nodo di amministrazione non primario. Qualsiasi dispositivo può connettersi alla rete Grid, alla rete amministrativa e alla rete client.

Prima di iniziare

- L'apparecchio è stato installato in un rack o in un armadio, collegato alle reti e acceso.
- Hai completato il ["Configurare l'hardware"](#) passi.

La configurazione dell'hardware dell'appliance include i passaggi necessari per configurare le 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 Grid elencate nella pagina Configurazione IP del programma di installazione dell'appliance StorageGRID sono state definite nell'elenco delle subnet della rete Grid sul nodo di amministrazione primario.
- Il firmware StorageGRID Appliance Installer sull'appliance sostitutiva è compatibile con la versione del software StorageGRID attualmente in esecuzione sulla rete. Se le versioni non sono compatibili, è necessario aggiornare il firmware di StorageGRID Appliance Installer.
- Hai un portatile di servizio con un ["browser web supportato"](#) .
- Conosci uno degli indirizzi IP assegnati al controller di elaborazione dell'appliance. È possibile utilizzare l'indirizzo IP per qualsiasi rete StorageGRID collegata.

Informazioni su questo compito

Il processo di installazione di StorageGRID su un nodo appliance prevede le seguenti fasi:

- Specificare o confermare l'indirizzo IP del nodo di amministrazione primario e il nome del nodo dell'appliance.
- Si avvia l'installazione e si attende che i volumi vengano configurati e il software installato.

Durante l'installazione dell'apparecchio, l'installazione si interrompe. Per riprendere l'installazione, accedi a Grid Manager, approva tutti i nodi della griglia e completa il processo di installazione StorageGRID .



Se è necessario distribuire più nodi appliance contemporaneamente, è possibile automatizzare il processo di installazione utilizzando `configure-sga.py` Script di installazione dell'appliance.

Passi

1. Aprire un browser e immettere uno degli indirizzi IP del controller di elaborazione dell'appliance.

```
https://Controller_IP:8443
```

Viene visualizzata la home page del programma di installazione dell'appliance StorageGRID .

2. Nella sezione Connessione **Nodo amministrativo primario**, determinare se è necessario specificare l'indirizzo IP per il nodo amministrativo primario.

Se in precedenza sono stati installati altri nodi in questo data center, StorageGRID Appliance Installer può rilevare automaticamente questo indirizzo IP, presupponendo che il nodo di amministrazione primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente nella stessa subnet.

3. Se questo indirizzo IP non viene visualizzato o è necessario modificarlo, specificare l'indirizzo:

Opzione	Descrizione
Inserimento manuale dell'IP	a. Deselezionare la casella di controllo Abilita individuazione nodo amministratore. b. Inserire manualmente l'indirizzo IP. c. Fare clic su Salva. d. Attendi che lo stato della connessione per il nuovo indirizzo IP sia pronto.
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo Abilita individuazione nodo amministratore. b. Attendi che venga visualizzato l'elenco degli indirizzi IP rilevati. c. Selezionare il nodo di amministrazione primario per la griglia in cui verrà distribuito questo nodo di archiviazione dell'appliance. d. Fare clic su Salva. e. Attendi che lo stato della connessione per il nuovo indirizzo IP sia pronto.

4. Nel campo **Nome nodo**, immettere il nome che si desidera utilizzare per questo nodo dell'appliance e selezionare **Salva**.

Il nome del nodo viene assegnato a questo nodo dell'appliance nel sistema StorageGRID . Viene visualizzato nella pagina Nodi (scheda Panoramica) in Grid Manager. Se necessario, puoi modificare il nome quando approvi il nodo.

5. Nella sezione **Installazione**, conferma che lo stato corrente è "Pronto per avviare l'installazione di *nome nodo* nella griglia con nodo di amministrazione primario *admin_ip*" e che il pulsante **Avvia installazione** è abilitato.

Se il pulsante **Avvia installazione** non è abilitato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per le istruzioni, consultare le istruzioni di manutenzione dell'apparecchio.

6. Dalla home page di StorageGRID Appliance Installer, selezionare **Avvia installazione**.

NetApp® StorageGRID® Appliance Installer

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Home

The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node discovery

☐

Primary Admin Node IP

172.16.4.210

Connection state

Connection to 172.16.4.210 ready

Cancel

Save

Node name

Node name

NetApp-SGA

Cancel

Save

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Start Installation

Lo stato corrente cambia in "Installazione in corso" e viene visualizzata la pagina Installazione del monitor.

7. Se l'espansione include più nodi appliance, ripetere i passaggi precedenti per ogni appliance.



Se è necessario distribuire più nodi di archiviazione dell'appliance contemporaneamente, è possibile automatizzare il processo di installazione utilizzando lo script di installazione dell'appliance `configure-sga.py`.

8. Se è necessario accedere manualmente alla pagina Installazione monitor, selezionare **Installazione monitor** dalla barra dei menu.

La pagina Installazione del monitor mostra lo stato di avanzamento dell'installazione.

Monitor Installation

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

La barra di stato blu indica quale attività è attualmente in corso. Le barre di stato verdi indicano le attività completate con successo.



Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si sta rieseguendo un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "Ignorato".

9. Esaminare lo stato di avanzamento delle prime due fasi di installazione.

1. Configura l'appliance

Durante questa fase si verifica uno dei seguenti processi:

- Per un dispositivo di archiviazione, il programma di installazione si connette al controller di archiviazione, cancella qualsiasi configurazione esistente, comunica con SANtricity OS per configurare i volumi e configura le impostazioni host.
- Per un'appliance di servizi, il programma di installazione cancella qualsiasi configurazione esistente dalle unità nel controller di elaborazione e configura le impostazioni host.

2. Installa il sistema operativo

Durante 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 finché non viene visualizzato un messaggio nella finestra della console che richiede di utilizzare Grid Manager per approvare il nodo.



Attendi che tutti i nodi aggiunti in questa espansione siano pronti per l'approvazione prima di andare al Grid Manager per approvarli.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

Eseguire l'espansione

Quando esegui l'espansione, i nuovi nodi della griglia vengono aggiunti alla distribuzione StorageGRID esistente.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai la passphrase di provisioning.
- Hai distribuito tutti i nodi della griglia che verranno aggiunti in questa espansione.
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).

- Se si aggiungono nodi di archiviazione, si conferma che tutte le operazioni di riparazione dei dati eseguite come parte di un ripristino sono state completate. Vedere ["Controlla i lavori di riparazione dei dati"](#) .
- Se si aggiungono nodi di archiviazione e si desidera assegnare un grado di archiviazione personalizzato a tali nodi, è già stato fatto ["creato il grado di archiviazione personalizzato"](#) . Si dispone inoltre dell'autorizzazione di accesso Root oppure di entrambe le autorizzazioni Maintenance e ILM.
- Se stai aggiungendo un nuovo sito, hai esaminato e aggiornato le regole ILM. È necessario assicurarsi che le copie degli oggetti non vengano archiviate nel nuovo sito finché l'espansione non sarà completata. Ad esempio, se una regola utilizza il pool di archiviazione predefinito (**Tutti i nodi di archiviazione**), è necessario ["creare un nuovo pool di archiviazione"](#) che contiene solo i nodi di archiviazione esistenti e ["aggiornare le regole ILM"](#) e la politica ILM per utilizzare quel nuovo pool di archiviazione. In caso contrario, gli oggetti verranno copiati nel nuovo sito non appena il primo nodo di quel sito diventerà attivo.

Informazioni su questo compito

L'esecuzione dell'espansione comprende le seguenti attività principali da parte dell'utente:

1. Configurare l'espansione.
2. Avviare l'espansione.
3. Scarica un nuovo file del pacchetto di ripristino.
4. Monitorare le fasi e i passaggi di espansione finché tutti i nuovi nodi non saranno installati e configurati e tutti i servizi non saranno avviati.



Alcune fasi e passaggi di espansione potrebbero richiedere molto tempo per essere eseguiti su una griglia di grandi dimensioni. Ad esempio, lo streaming di Cassandra su un nuovo nodo di archiviazione potrebbe richiedere solo pochi minuti se il database Cassandra è vuoto. Tuttavia, se il database Cassandra include una grande quantità di metadati di oggetti, questa fase potrebbe richiedere diverse ore o più. Non riavviare alcun nodo di archiviazione durante le fasi "Espansione del cluster Cassandra" o "Avvio di Cassandra e streaming dei dati".

Passi

1. Selezionare **MANUTENZIONE > Attività > Espansione**.

Viene visualizzata la pagina Espansione griglia. Nella sezione Nodi in sospenso sono elencati i nodi pronti per essere aggiunti.

Grid Expansion

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Configure Expansion

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve

✕ Remove

Search

	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
	00:50:56:a7:7a:c0	rleo-010-096-106-151	Storage Node	VMware VM	10.96.106.151/22
	00:50:56:a7:0f:2e	rleo-010-096-106-156	API Gateway Node	VMware VM	10.96.106.156/22

2. Selezionare **Configura espansione**.

Viene visualizzata la finestra di dialogo Selezione sito.

3. Seleziona il tipo di espansione che vuoi avviare:

- Se si desidera aggiungere un nuovo sito, selezionare **Nuovo** e immettere il nome del nuovo sito.
- Se si desidera aggiungere uno o più nodi a un sito esistente, selezionare **Esistente**.

4. Seleziona **Salva**.

5. Esaminare l'elenco **Nodi in sospeso** e verificare che mostri tutti i nodi della griglia distribuiti.

Se necessario, puoi posizionare il cursore sull'indirizzo MAC della rete di griglia di un nodo per visualizzare i dettagli relativi a quel nodo.

Pending Nodes

Grid nodes are listed as

+

 Approve

×

 Remove

Grid Network MAC Address

00:50:56:a7:7a:c0

00:50:56:a7:0f:2e

Approved Nodes

leo-010-096-106-151

Storage Node

Network

Grid Network	10.96.106.151/22	10.96.104.1
Admin Network	Name	Type
Client Network		

Hardware

VMware VM

4 CPUs

8 GB RAM

Disks

55 GB

55 GB

55 GB



Se un nodo risulta mancante, verificare che sia stato distribuito correttamente.

6. Dall'elenco dei nodi in sospeso, approva i nodi che vuoi aggiungere a questa espansione.
 - a. Selezionare il pulsante di opzione accanto al primo nodo della griglia in sospeso che si desidera approvare.
 - b. Seleziona **Approva**.

Viene visualizzato il modulo di configurazione del nodo della griglia.

- c. Se necessario, modificare le impostazioni generali:

Campo	Descrizione
Sito	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	Nome di sistema per il nodo. I nomi di sistema sono necessari per le operazioni interne StorageGRID e non possono essere modificati.
Tipo di archiviazione (solo nodi di archiviazione)	• Dati e metadati ("combinati"): nodo di archiviazione di dati e metadati oggetto • Solo dati: nodo di archiviazione contenente solo dati oggetto (nessun metadato) • Solo metadati: nodo di archiviazione contenente solo metadati (nessun dato oggetto)

Campo	Descrizione
Ruolo NTP	Il ruolo del Network Time Protocol (NTP) del nodo della griglia: • Selezionare Automatico (predefinito) per assegnare automaticamente il ruolo NTP al nodo. Il ruolo primario verrà assegnato ai nodi di amministrazione, ai nodi di archiviazione con servizi ADC, ai nodi gateway e a tutti i nodi della griglia dotati di indirizzi IP non statici. Il ruolo Client verrà assegnato a tutti gli altri nodi della griglia. • Selezionare Primario per assegnare manualmente il ruolo NTP primario al nodo. Almeno due nodi in ogni sito dovrebbero avere il ruolo primario per fornire un accesso ridondante al sistema alle fonti di temporizzazione esterne. • Selezionare Client per assegnare manualmente il ruolo Client NTP al nodo.
Servizio ADC (nodi di archiviazione combinati o solo metadati)	Se questo nodo di archiviazione eseguirà il servizio ADC (Administrative Domain Controller). Il servizio ADC tiene traccia della posizione e della disponibilità dei servizi di rete. Almeno tre nodi di archiviazione in ogni sito devono includere il servizio ADC. Non è possibile aggiungere il servizio ADC a un nodo dopo averlo distribuito. • Selezionare Sì se il nodo di archiviazione che si sta sostituendo include il servizio ADC. Poiché non è possibile dismettere un nodo di archiviazione se rimangono troppo pochi servizi ADC, ciò garantisce che un nuovo servizio ADC sia disponibile prima che il vecchio servizio venga rimosso. • Selezionare Automatico per consentire al sistema di determinare se questo nodo richiede il servizio ADC. Scopri di più su "Quorum ADC".
Grado di archiviazione (nodi di archiviazione combinati o solo dati)	Utilizzare il grado di archiviazione Predefinito oppure selezionare il grado di archiviazione personalizzato che si desidera assegnare a questo nuovo nodo. I gradi di archiviazione vengono utilizzati dai pool di archiviazione ILM, pertanto la selezione può influire sugli oggetti che verranno posizionati sul nodo di archiviazione.

d. Se necessario, modificare le impostazioni per la rete Grid, la rete amministrativa e la rete client.

- **Indirizzo IPv4 (CIDR):** l'indirizzo di rete CIDR per l'interfaccia di rete. Ad esempio:
172.16.10.100/24



Se durante l'approvazione dei nodi si scopre che i nodi hanno indirizzi IP duplicati sulla rete Grid, 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 della griglia. Ad esempio: 172.16.10.1
- **Sottoreti (CIDR):** una o più sottoreti per la rete di amministrazione.

e. Seleziona **Salva**.

Il nodo della griglia approvato viene spostato nell'elenco dei nodi approvati.

- Per modificare le proprietà di un nodo della griglia approvato, seleziona il relativo pulsante di scelta e seleziona **Modifica**.
- Per spostare nuovamente un nodo della griglia approvato nell'elenco dei nodi in sospeso, seleziona il relativo pulsante di opzione e seleziona **Reimposta**.
- Per rimuovere definitivamente un nodo di rete approvato, spegnerlo. Quindi, seleziona il pulsante di opzione e seleziona **Rimuovi**.

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



Se possibile, dovresti approvare tutte le note della griglia in sospeso ed eseguire una singola espansione. Se si eseguono più piccole espansioni, sarà necessario più tempo.

7. Dopo aver approvato tutti i nodi della griglia, immettere la **Passphrase di provisioning** e selezionare **Espandi**.

Dopo alcuni minuti, questa pagina si aggiorna per visualizzare lo stato della procedura di espansione. Quando sono in corso attività che interessano singoli nodi della griglia, la sezione Stato nodo griglia elenca lo stato corrente di ciascun nodo della griglia.



Durante la fase di "Installazione dei nodi della griglia" per una nuova appliance, StorageGRID Appliance Installer mostra il passaggio dell'installazione dalla Fase 3 alla Fase 4, Finalizzazione dell'installazione. Una volta completata la Fase 4, il controller viene riavviato.

Expansion Progress

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

1. Installing grid nodes

In Progress

Grid Node Status

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

Search



Name	Site	Grid Network IPv4 Address	Progress	Stage
rleo-010-096-106-151	Data Center 1	10.96.106.151/22		Waiting for Dynamic IP Service peers
rleo-010-096-106-156	Data Center 1	10.96.106.156/22		Waiting for NTP to synchronize

2. Initial configuration

Pending

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

Pending

4. Assigning Storage Nodes to storage grade

Pending

5. Starting services on the new grid nodes

Pending

6. Starting background process to clean up unused Cassandra keys

Pending



L'espansione di un sito include un'attività aggiuntiva per configurare Cassandra per il nuovo sito.

8. Non appena appare il link **Scarica pacchetto di ripristino**, scarica il file del pacchetto di ripristino.

Dopo aver apportato modifiche alla topologia della griglia nel sistema StorageGRID, è necessario scaricare una copia aggiornata del file del pacchetto di ripristino il prima possibile. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

- Seleziona il link per il download.
- Immettere la passphrase di provisioning e selezionare **Avvia download**.
- Una volta completato il download, apri il .zip file e confermare che è possibile accedere al contenuto, incluso il `Passwords.txt` file.
- Copia il file del pacchetto di ripristino scaricato(.zip) in due luoghi sicuri, protetti e separati.



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 archiviazione 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 della griglia.



Non riavviare alcun nodo di archiviazione durante le fasi "Espansione del cluster Cassandra" o "Avvio di Cassandra e streaming dei dati". Il completamento di queste fasi potrebbe richiedere molte ore per ogni nuovo nodo di archiviazione, soprattutto se i nodi di archiviazione esistenti contengono una grande quantità di metadati di oggetti.

Aggiunta di nodi di archiviazione

Se si aggiungono nodi di archiviazione a un sito esistente, verificare la percentuale visualizzata nel messaggio di stato "Avvio di Cassandra e streaming dei dati".

5. Starting services on the new grid nodes

In Progress

Grid Node Status

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

⚠ Do not reboot any Storage Nodes during Step 4. The "Starting Cassandra and streaming data" stage might take hours, especially if existing Storage Nodes contain a large amount of object metadata.

Name	Site	Grid Network IPv4 Address	Progress	Stage
rleo-010-096-106-151	Data Center 1	10.96.106.151/22		Starting Cassandra and streaming data (20.4% streamed)
rleo-010-096-106-156	Data Center 1	10.96.106.156/22		Starting services

Questa percentuale stima il livello di completezza dell'operazione di streaming di Cassandra, in base alla quantità totale di dati Cassandra disponibili e alla quantità già scritta sul nuovo nodo.

Aggiunta del sito

Se stai aggiungendo un nuovo sito, usa `nodetool status` per monitorare l'avanzamento dello streaming di Cassandra e per vedere quanti metadati sono stati copiati sul nuovo sito durante la fase di "Espansione del cluster Cassandra". Il carico dati totale sul nuovo sito dovrebbe essere pari a circa il 20% del carico totale di un sito attuale.

10. Continuare a monitorare l'espansione finché tutte le attività non saranno completate e il pulsante **Configura espansione** non riapparirà.

Dopo aver finito

A seconda dei tipi di nodi della griglia aggiunti, eseguire ulteriori passaggi di integrazione e configurazione. Vedere ["Fasi di configurazione dopo l'espansione"](#).

Configurare il sistema espanso

Fasi di configurazione dopo l'espansione

Dopo aver completato un'espansione, è necessario eseguire ulteriori passaggi di integrazione e configurazione.

Informazioni su questo compito

È necessario completare le attività di configurazione elencate di seguito per i nodi o i siti della griglia che si desidera aggiungere 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.

Passi

1. Se hai aggiunto un sito:

- ["Creare un pool di archiviazione"](#) per il sito e per ogni livello di archiviazione selezionato per i nuovi nodi di archiviazione.
- Verificare che la politica ILM soddisfi i nuovi requisiti. Se sono necessarie modifiche alle regole, ["creare nuove regole"](#) E ["aggiornare la politica ILM"](#) . Se le regole sono già corrette, ["attivare una nuova politica"](#) senza modifiche alle regole per garantire che StorageGRID utilizzi i nuovi nodi.
- Verificare che i server NTP (Network Time Protocol) siano accessibili da quel sito. Vedere ["Gestire i server NTP"](#) .



Assicurarsi che almeno due nodi in ogni sito possano accedere ad almeno quattro fonti NTP esterne. Se solo un nodo in un sito riesce a raggiungere le sorgenti NTP, si verificheranno problemi di temporizzazione se quel nodo non funziona. Inoltre, la designazione di due nodi per sito come fonti NTP primarie garantisce una temporizzazione accurata se un sito è isolato dal resto della griglia.

2. Se hai aggiunto uno o più nodi di archiviazione a un sito esistente:

- ["Visualizza i dettagli del pool di archiviazione"](#) per confermare che ogni nodo aggiunto sia incluso nel pool di archiviazione previsti e utilizzato nelle regole ILM previste.
- Verificare che la politica ILM soddisfi i nuovi requisiti. Se sono necessarie modifiche alle regole, ["creare nuove regole"](#) E ["aggiornare la politica ILM"](#) . Se le regole sono già corrette, ["attivare una nuova politica"](#) senza modifiche alle regole per garantire che StorageGRID utilizzi i nuovi nodi.
- ["Verificare che il nodo di archiviazione sia attivo"](#) e in grado di ingerire oggetti.
- Se non è stato possibile aggiungere il numero consigliato di nodi di archiviazione, ribilanciare i dati con codice di cancellazione. Vedere ["Ribilancia i dati codificati tramite cancellazione dopo l'aggiunta di nodi di archiviazione"](#) .

3. Se hai aggiunto un nodo gateway:

- Se per le connessioni client vengono utilizzati gruppi ad alta disponibilità (HA), è possibile aggiungere facoltativamente il nodo gateway a un gruppo HA. Selezionare **CONFIGURAZIONE > Rete > Gruppi ad alta disponibilità** per rivedere l'elenco dei gruppi HA esistenti e aggiungere il nuovo nodo. Vedere ["Configurare gruppi ad alta disponibilità"](#) .

4. Se hai aggiunto un nodo di amministrazione:

- a. Se per il sistema StorageGRID è abilitato l'accesso singolo (SSO), creare un trust della relying party per il nuovo nodo di amministrazione. Non è possibile accedere al nodo finché non si crea questo trust della relying party. Vedere ["Configurare l'accesso singolo"](#) .
- b. Se si prevede di utilizzare il servizio Load Balancer sui nodi amministrativi, è possibile aggiungere facoltativamente il nuovo nodo amministrativo a un gruppo HA. Selezionare **CONFIGURAZIONE > Rete > Gruppi ad alta disponibilità** per rivedere l'elenco dei gruppi HA esistenti e aggiungere il nuovo nodo. Vedere ["Configurare gruppi ad alta disponibilità"](#) .
- c. Facoltativamente, copiare il database del nodo amministrativo dal nodo amministrativo primario al nodo amministrativo di espansione se si desidera mantenere coerenti le informazioni sugli attributi e sugli audit su ciascun nodo amministrativo. Vedere ["Copia il database del nodo di amministrazione"](#) .
- d. Facoltativamente, copiare il database Prometheus dal nodo di amministrazione primario al nodo di amministrazione di espansione se si desidera mantenere coerenti le metriche storiche su ciascun nodo di amministrazione. Vedere ["Copia le metriche di Prometheus"](#) .
- e. Facoltativamente, copiare i registri di controllo esistenti dal nodo di amministrazione primario al nodo di amministrazione di espansione se si desidera mantenere coerenti le informazioni del registro storico su

ciascun nodo di amministrazione. Vedere ["Copia i registri di controllo"](#) .

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 attendibile o meno, andare su **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 tramite un endpoint di bilanciamento del carico. Vedere ["Configurare gli endpoint del bilanciatore del carico"](#) E ["Gestire i controlli del firewall"](#) .

6. Configurare il DNS.

Se hai specificato le impostazioni DNS separatamente per ogni nodo della griglia, devi aggiungere impostazioni DNS personalizzate per ogni nodo per i nuovi nodi. Vedere ["Modifica la configurazione DNS per un singolo nodo della griglia"](#) .

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

Se possibile, utilizzare server DNS a cui ogni sito possa accedere localmente per garantire che un sito isolato possa risolvere gli FQDN per le destinazioni esterne.

Verificare che il nodo di archiviazione sia attivo

Dopo il completamento di un'operazione di espansione che aggiunge nuovi nodi di archiviazione, il sistema StorageGRID dovrebbe avviarsi automaticamente utilizzando i nuovi nodi di archiviazione. È necessario utilizzare il sistema StorageGRID per verificare che il nuovo nodo di archiviazione sia attivo.

Passi

1. Sign in a Grid Manager utilizzando un ["browser web supportato"](#) .
2. Selezionare **NODI > Nodo di archiviazione di espansione > Archiviazione**.
3. Posiziona il cursore sul grafico **Spazio di archiviazione utilizzato - Dati oggetto** per visualizzare il valore di **Utilizzato**, ovvero la quantità di spazio utilizzabile totale che è stata utilizzata per i dati oggetto.
4. Verifica che il valore di **Usato** aumenti spostando il cursore verso destra sul grafico.

Copia il database del nodo di amministrazione

Quando si aggiungono nodi amministrativi tramite una procedura di espansione, è possibile copiare facoltativamente il database dal nodo amministrativo primario al nuovo nodo amministrativo. La copia del database consente di conservare informazioni storiche su attributi, avvisi e notifiche.

Prima di iniziare

- Hai completato i passaggi di espansione richiesti per aggiungere un nodo di amministrazione.
- Tu hai il `Passwords.txt` file.
- Hai la passphrase di provisioning.

Informazioni su questo compito

Il processo di attivazione del software StorageGRID crea un database vuoto per il servizio NMS sul nodo di amministrazione di espansione. Quando il servizio NMS viene avviato sul nodo di amministrazione di espansione, registra le informazioni sui server e sui servizi che fanno attualmente parte del sistema o che verranno aggiunti in seguito. Questo database del nodo di amministrazione include le seguenti informazioni:

- Cronologia degli avvisi
- Dati degli attributi storici, utilizzati nei grafici in stile legacy nella pagina Nodi

Per garantire che il database del nodo amministrativo sia coerente tra i nodi, è possibile copiare il database dal nodo amministrativo primario al nodo amministrativo di espansione.



La copia del database dal nodo amministrativo primario (*il nodo amministrativo di origine*) a un nodo amministrativo di espansione può richiedere diverse ore. Durante questo periodo, il Grid Manager non è accessibile.

Utilizzare questi passaggi per arrestare il servizio MI e il servizio Management API sia sul nodo di amministrazione primario che sul nodo di amministrazione di espansione prima di copiare il database.

Passi

1. Completare i seguenti passaggi sul nodo di amministrazione primario:
 - a. Accedi al nodo di amministrazione:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla root: `su -`
 - iv. Inserisci la password elencata nel `Passwords.txt` file.
 - b. Eseguire il seguente comando: `recover-access-points`
 - c. Immettere 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 di espansione:
 - a. Accedi al nodo di amministrazione dell'espansione:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla root: `su -`
 - iv. Inserisci la password elencata nel `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. Inserisci: `ssh-add`
 - e. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.

f. Copiare il database dal nodo di amministrazione di origine al nodo di amministrazione 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 sul nodo di amministrazione di espansione.

Il database e i suoi dati storici vengono copiati nel nodo di amministrazione di espansione. Una volta completata l'operazione di copia, lo script avvia il nodo di amministrazione di espansione.

h. Quando non è più necessario l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserisci: `ssh-add -D`

3. Riavviare i servizi sul nodo di amministrazione primario: `service servermanager start`

Copia le metriche di 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 Admin Node è installato e funzionante.
- Tu hai il `Passwords.txt` file.
- Hai la passphrase di provisioning.

Informazioni su questo compito

Quando si aggiunge un Admin Node, il processo di installazione del software crea un nuovo database Prometheus. È possibile mantenere coerenti le metriche storiche tra i nodi copiando il database Prometheus dal nodo di amministrazione primario (il *nodo di amministrazione sorgente*) 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 sono interrotti sul nodo di amministrazione di origine.

Passi

1. Accedi al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.
2. Dal nodo di amministrazione di origine, arrestare il servizio Prometheus: `service prometheus stop`
3. Completare i seguenti passaggi sul nuovo nodo di amministrazione:
 - a. Accedi al nuovo nodo di amministrazione:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password elencata nel `Passwords.txt` file.

- iii. Immettere il seguente comando per passare alla root: `su -`
- iv. Inserisci la password elencata nel `Passwords.txt` file.
- b. Interrompere il servizio Prometheus: `service prometheus stop`
- c. Aggiungere la chiave privata SSH all'agente SSH. Inserisci: `ssh-add`
- d. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.
- e. Copia il database Prometheus dal nodo di amministrazione di origine al nuovo nodo di amministrazione: `/usr/local/prometheus/bin/prometheus-clone-db.sh`
`Source_Admin_Node_IP`
- f. Quando richiesto, premere **Invio** per confermare che si desidera eliminare il nuovo database Prometheus sul nuovo nodo di amministrazione.

Il database Prometheus originale e i suoi dati storici vengono copiati nel nuovo nodo di amministrazione. Una volta completata l'operazione di copia, lo script avvia il nuovo nodo di amministrazione. Viene visualizzato il seguente stato:

```
Database cloned, starting services
```

- a. Quando non è più necessario l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserisci:

```
ssh-add -D
```

- 4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.

```
service prometheus start
```

Copia i registri di controllo

Quando si aggiunge un nuovo nodo amministrativo tramite una procedura di espansione, il suo servizio AMS registra solo gli eventi e le azioni che si verificano dopo l'adesione al sistema. Se necessario, è possibile copiare i registri di controllo da un nodo di amministrazione installato in precedenza al nuovo nodo di amministrazione di espansione, in modo che sia sincronizzato con il resto del sistema StorageGRID .

Prima di iniziare

- Hai completato i passaggi di espansione richiesti per aggiungere un nodo di amministrazione.
- Tu hai il `Passwords.txt` file.

Informazioni su questo compito

Per rendere disponibili i messaggi di controllo storici su un nuovo nodo di amministrazione, è necessario copiare manualmente i file di registro di controllo da un nodo di amministrazione esistente al nodo di amministrazione di 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:



- Hai configurato un server syslog esterno e i log di controllo vengono ora inviati al server syslog anziché ai nodi di amministrazione.
- Hai specificato esplicitamente che i messaggi di controllo devono essere salvati solo sui nodi locali che li hanno generati.

Vedere "[Configurare i messaggi di controllo e le destinazioni dei registri](#)" per i dettagli.

Passi

1. Accedi al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@_primary_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Arrestare il servizio AMS per impedire che crei un nuovo file: `service ams stop`

3. Passare alla directory di esportazione dell'audit:

```
cd /var/local/log
```

4. Rinomina la fonte `audit.log` file per garantire che non sovrascriva il file sul nodo di amministrazione di espansione in cui lo stai 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 primario elencato in `Passwords.txt` file.

7. Ripristina 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. Accedi al nodo di amministrazione dell'espansione:

- a. Immettere il seguente comando: `ssh admin@expansion_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

11. Aggiornare le impostazioni utente e gruppo per i file di registro di controllo:

```
cd /var/local/log  
  
chown ams-user:bycast *
```

12. Disconnettersi dal server:

```
exit
```

Ribilancia i dati codificati tramite cancellazione dopo l'aggiunta di nodi di archiviazione

Dopo aver aggiunto i nodi di archiviazione, è possibile utilizzare la procedura di ribilanciamento della codifica di cancellazione (EC) per ridistribuire i frammenti codificati tramite codifica di cancellazione tra i nodi di archiviazione esistenti e quelli nuovi.

Prima di iniziare

- Sono stati completati i passaggi di espansione per aggiungere i nuovi nodi di archiviazione.
- Hai esaminato il ["considerazioni per il ribilanciamento dei dati codificati con cancellazione"](#).
- L'utente è consapevole che i dati degli oggetti replicati non verranno spostati da questa procedura e che la procedura di ribilanciamento EC non considera l'utilizzo dei dati replicati su ciascun nodo di archiviazione quando determina dove spostare i dati con codice di cancellazione.
- Tu hai il `Passwords.txt` file.

Cosa succede quando viene eseguita questa procedura

Prima di iniziare la procedura, tenere presente quanto segue:

- La procedura di ribilanciamento EC non verrà avviata se uno o più volumi sono offline (smontati) o se sono online (montati) ma in stato di errore.
- La procedura di riequilibrio della CE riserva temporaneamente una grande quantità di stoccaggio. Potrebbero essere attivati avvisi di archiviazione, ma verranno risolti al termine del ribilanciamento. Se non c'è abbastanza spazio per la prenotazione, la procedura di ribilanciamento EC fallirà. Le prenotazioni di archiviazione vengono rilasciate al termine della procedura di ribilanciamento EC, indipendentemente dal fatto che la procedura sia fallita o riuscita.
- Se un volume va offline mentre è in corso la procedura di ribilanciamento EC, la procedura di ribilanciamento verrà terminata. Tutti i frammenti di dati già spostati rimarranno nelle nuove posizioni e

nessun dato andrà perso.

È possibile eseguire nuovamente la procedura dopo che tutti i volumi saranno di nuovo online.

- Quando è in esecuzione la procedura di ribilanciamento EC, le prestazioni delle operazioni ILM e delle operazioni client S3 potrebbero essere compromesse.



Le operazioni API S3 per caricare oggetti (o parti di oggetti) potrebbero non riuscire durante la procedura di ribilanciamento EC se richiedono più di 24 ore per essere completate. Le operazioni PUT di lunga durata non riusciranno se la regola ILM applicabile utilizza il posizionamento Bilanciato o Rigoroso durante l'acquisizione. Verrà segnalato il seguente errore: 500 Internal Server Error.

- Durante questa procedura tutti i nodi hanno un limite di capacità di archiviazione dell'80%. I nodi che superano questo limite, ma che comunque memorizzano dati al di sotto della partizione di destinazione, sono esclusi da:
 - Il valore dello squilibrio del sito
 - Eventuali condizioni 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.** La procedura di ribilanciamento della CE è considerata completa quando si verifica una delle seguenti condizioni:
 - Non è più possibile spostare dati con codice di cancellazione.
 - I dati in tutti i nodi rientrano in una deviazione del 5% rispetto alla partizione dati di destinazione.
 - La procedura è in corso da 30 giorni.

Passi

1. Esamina i dettagli attuali dell'archiviazione degli oggetti per il sito che intendi ribilanciare.
 - a. Selezionare **NODES**.
 - b. Selezionare il primo nodo di archiviazione nel sito.
 - c. Selezionare la scheda **Archiviazione**.
 - d. Posiziona il cursore sul grafico Spazio di archiviazione utilizzato - Dati oggetto per visualizzare la quantità corrente di dati replicati e dati con codice di cancellazione sul nodo di archiviazione.
 - e. Ripetere questi passaggi per visualizzare gli altri nodi di archiviazione nel sito.
2. Accedi al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

3. Avviare la procedura:

```
`rebalance-data start --site "nome-sito"
```

Per "*site-name*", specificare il primo sito in cui sono stati aggiunti nuovi nodi di archiviazione. Allegare *site-name* tra virgolette.

Viene avviata la procedura di ribilanciamento EC e viene restituito un ID processo.

4. Copia l'ID del lavoro.

5. Monitorare lo stato della procedura di riequilibrio della 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 quando è stata avviata la procedura.

- Per visualizzare lo stato della procedura di ribilanciamento EC in corso e di tutte le procedure completate in precedenza:

```
rebalance-data status
```



Per ottenere assistenza sul comando rebalance-data:

```
rebalance-data --help
```

6. Eseguire passaggi aggiuntivi, in base allo stato restituito:

- Se State È In progress, l'operazione di riequilibrio della CE è ancora in corso. È necessario monitorare periodicamente la procedura fino al suo completamento.

Utilizzare il Site Imbalance valore per valutare quanto sia sbilanciato l'utilizzo dei dati del codice di cancellazione tra i nodi di archiviazione del sito. Questo valore può variare da 1,0 a 0, dove 0 indica che l'utilizzo dei dati di codifica di cancellazione è completamente bilanciato su tutti i nodi di archiviazione del sito.

Il processo di ribilanciamento EC è considerato completo e si interromperà quando i dati in tutti i nodi si troveranno entro una deviazione del 5% dalla partizione dati di destinazione.

- Se State È Success, facoltativamente [rivedere l'archiviazione degli oggetti](#) per vedere i dettagli aggiornati del sito.

I dati con codice di cancellazione dovrebbero ora essere più bilanciati tra i nodi di archiviazione del sito.

- Se State È Failure:

- i. Verificare che tutti i nodi di archiviazione del sito siano collegati alla rete.
- ii. Verificare e risolvere eventuali avvisi che potrebbero interessare questi nodi di archiviazione.
- iii. Riavviare la procedura di ribilanciamento della CE:

```
rebalance-data start --job-id job-id
```

- iv. [Visualizza lo stato](#) della nuova procedura. Se State è ancora Failure, contattare l'assistenza

tecnica.

7. Se la procedura di ribilanciamento EC genera un carico eccessivo (ad esempio, sono interessate le operazioni di acquisizione), mettere in pausa la procedura.

```
rebalance-data pause --job-id job-id
```

8. Se è necessario terminare la procedura di ribilanciamento EC (ad esempio, per poter eseguire un aggiornamento del software StorageGRID), immettere quanto segue:

```
rebalance-data terminate --job-id job-id
```



Quando si termina una procedura di ribilanciamento EC, tutti i frammenti di dati già spostati rimangono nelle loro nuove posizioni. I dati non vengono spostati nella posizione originale.

9. Se si utilizza la codifica di cancellazione in più di un sito, eseguire questa procedura per tutti gli altri siti interessati.

Risoluzione dei problemi di espansione

Se durante il processo di espansione della griglia si verificano errori che non si riescono a risolvere o se un'attività della griglia non riesce, raccogliere i file di registro e contattare l'assistenza tecnica.

Prima di contattare l'assistenza tecnica, raccogliere i file di registro necessari per facilitare la risoluzione dei problemi.

Passi

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 del contenitore che esegue StorageGRID.

- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Dopo aver effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. A seconda della fase raggiunta dall'installazione, recupera uno dei seguenti log disponibili sul nodo della griglia:

Piattaforma	Registri
VMware	• <code>/var/log/daemon.log</code> • <code>/var/log/storagegrid/daemon.log</code> • <code>/var/log/storagegrid/nodes/<node-name>.log</code>

Piattaforma	Registri
Linux	• /var/log/storagegrid/daemon.log • /etc/storagegrid/nodes/<node-name>.conf(per ogni nodo fallito) • /var/log/storagegrid/nodes/<node-name>.log(per ogni nodo non riuscito; potrebbe non esistere)

Mantenere un sistema StorageGRID

Manutenzione della rete

Le attività di manutenzione della rete includono la dismissione di un nodo o di un sito, la ridenominazione di una rete, di un nodo o di un sito e la manutenzione delle reti. È inoltre possibile eseguire procedure host e middleware e procedure del nodo della griglia.



In queste istruzioni, "Linux" si riferisce a una distribuzione Red Hat® Enterprise Linux®, Ubuntu® o Debian®. Per un elenco delle versioni supportate, vedere ["Strumento matrice di interoperabilità NetApp"](#).

Prima di iniziare

- Hai una conoscenza approfondita del sistema StorageGRID.
- Hai esaminato la topologia del tuo sistema StorageGRID e hai compreso la configurazione della griglia.
- L'utente è consapevole che è necessario seguire scrupolosamente tutte le istruzioni e prestare attenzione a tutti gli avvertimenti.
- L'utente è consapevole che le procedure di manutenzione non descritte non sono supportate né richiedono un impegno di servizi.

Procedure di manutenzione per gli elettrodomestici

Per le procedure hardware, vedere ["istruzioni di manutenzione per il tuo dispositivo StorageGRID"](#).

Scarica il pacchetto di ripristino

Il file Recovery Package consente di ripristinare il sistema StorageGRID in caso di errore.

Prima di iniziare

- Dal nodo di amministrazione primario, si accede al Grid Manager utilizzando un ["browser web supportato"](#).
- Hai la passphrase di provisioning.
- Hai ["autorizzazioni di accesso specifiche"](#).

Scaricare il file del pacchetto di ripristino corrente prima di apportare modifiche alla topologia della griglia nel sistema StorageGRID o prima di aggiornare il software. Quindi, dopo aver apportato modifiche alla topologia della griglia o dopo aver aggiornato il software, scaricare una nuova copia del pacchetto di ripristino.

Passi

1. Selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino**.
2. Inserisci la passphrase di provisioning e seleziona **Avvia download**.

Il download inizia immediatamente.

3. Una volta completato il download, apri il .zip file e confermare che è possibile accedere al contenuto, incluso il `Passwords.txt` file.

4. Copia il file del pacchetto di ripristino scaricato(. zip) in due luoghi sicuri, protetti e separati.



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 .

Disattivare nodi o siti

Dismettere il nodo o il sito

È possibile eseguire una procedura di dismissione per rimuovere definitivamente 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 dismissione:

- Eseguire un ["dismissione del nodo della griglia"](#) 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 un ["dismissione del sito"](#) per rimuovere un sito. Si esegue una **decommissionazione del sito connesso** se tutti i nodi sono connessi a StorageGRID. Si esegue una **decommissionazione del sito disconnesso** se tutti i nodi sono disconnessi da StorageGRID. Se il sito contiene un mix di nodi connessi e disconnessi, è necessario riportare online tutti i nodi offline.



Prima di procedere alla dismissione di un sito disconnesso, contattare il rappresentante dell'account NetApp . NetApp esaminerà i tuoi requisiti prima di abilitare tutti i passaggi della procedura guidata di dismissione del sito. Non tentare di disattivare un sito disconnesso se ritieni che sia possibile ripristinarlo o recuperare i dati degli oggetti dal sito.

Nodi dismessi

Disattivazione del nodo della rete

È possibile utilizzare la procedura di dismissione dei nodi per rimuovere uno o più nodi della griglia in uno o più siti. Non è possibile disattivare il nodo di amministrazione primario.

Quando dismettere un nodo

Utilizzare la procedura di dismissione del nodo quando si verifica una delle seguenti condizioni:

- Hai aggiunto un nodo di archiviazione più grande in un'espansione e vuoi rimuovere uno o più nodi di archiviazione più piccoli, preservando allo stesso tempo gli oggetti.



Se vuoi sostituire un elettrodomestico vecchio con uno più nuovo, considera ["clonazione del nodo dell'appliance"](#) invece di aggiungere un nuovo elettrodomestico in un'espansione e poi dismettere quello vecchio.

- Hai bisogno di meno spazio di archiviazione totale.
- Non hai più bisogno di un Gateway Node.

- Non è più necessario un nodo di amministrazione non primario.
- La tua rete include un nodo disconnesso che non puoi recuperare o rimettere online.
- La tua griglia include un nodo archivio.

Come dismettere un nodo

È possibile disattivare i nodi della rete connessi o disconnessi.

Disattivare i nodi connessi

In generale, è opportuno disattivare i nodi della griglia solo quando sono connessi al sistema StorageGRID e solo quando tutti i nodi sono in condizioni normali (sono presenti icone verdi nelle pagine **NODI** e nella pagina **Disattivazione nodi**).

Per le istruzioni, vedere ["Disattivare i nodi della rete connessi"](#) .

Disattivare i nodi disconnessi

In alcuni casi, potrebbe essere necessario dismettere un nodo della rete che non è attualmente connesso alla rete (uno il cui stato è sconosciuto o amministrativamente inattivo).

Per le istruzioni, vedere ["Disattivare i nodi della rete disconnessi"](#) .

Cosa considerare prima di dismettere un nodo

Prima di eseguire una delle due procedure, rivedere le considerazioni per ciascun tipo di nodo:

- ["Considerazioni per la dismissione del nodo di amministrazione o gateway"](#)
- ["Considerazioni per la dismissione del nodo di archiviazione"](#)

Considerazioni sulla dismissione dei nodi di amministrazione o gateway

Esaminare le considerazioni per la dismissione di un nodo amministrativo o di un nodo gateway.

Considerazioni per il nodo di amministrazione

- Non è possibile disattivare il nodo di amministrazione primario.
- Non è possibile dismettere un nodo amministrativo se una delle sue interfacce di rete fa parte di un gruppo ad alta disponibilità (HA). Per prima cosa è necessario rimuovere le interfacce di rete dal gruppo HA. Vedi le istruzioni per ["gestione dei gruppi HA"](#) .
- Se necessario, è possibile modificare in modo sicuro i criteri ILM durante la dismissione di un nodo amministrativo.
- Se si dismette un nodo di amministrazione e per il sistema StorageGRID è abilitato l'accesso singolo (SSO), è necessario ricordarsi di rimuovere il trust della parte affidabile del nodo da Active Directory Federation Services (AD FS).
- Se usi ["federazione di rete"](#) , assicurarsi che l'indirizzo IP del nodo che si sta dismettendo non sia stato specificato per una connessione di federazione di griglia.
- Quando si dismette un nodo amministrativo disconnesso, si perdono i registri di controllo di quel nodo; tuttavia, questi registri dovrebbero essere presenti anche sul nodo amministrativo primario.

Considerazioni per il nodo gateway

- Non è possibile dismettere un Gateway Node se una delle sue interfacce di rete fa parte di un gruppo ad alta disponibilità (HA). Per prima cosa è necessario rimuovere le interfacce di rete dal gruppo HA. Vedi le istruzioni per ["gestione dei gruppi HA"](#) .
- Se necessario, è possibile modificare in modo sicuro i criteri ILM durante la dismissione di un nodo gateway.
- Se usi ["federazione di rete"](#) , assicurarsi che l'indirizzo IP del nodo che si sta dismettendo non sia stato specificato per una connessione di federazione di griglia.
- È possibile disattivare in tutta sicurezza un Gateway Node mentre è disconnesso.

Considerazioni sui nodi di archiviazione

Considerazioni per la dismissione dei nodi di archiviazione

Prima di dismettere un nodo di archiviazione, valuta se è possibile clonarlo. Quindi, se si decide di dismettere il nodo, verificare come StorageGRID gestisce gli oggetti e i metadati durante la procedura di dismissione.

Quando clonare un nodo invece di dismetterlo

Se si desidera sostituire un vecchio nodo di archiviazione con un dispositivo più nuovo o più grande, si consiglia di clonare il nodo del dispositivo anziché aggiungere un nuovo dispositivo in un'espansione e quindi dismettere il vecchio dispositivo.

La clonazione del nodo appliance consente di sostituire facilmente un nodo appliance esistente con un appliance compatibile nello stesso sito StorageGRID . Il processo di clonazione trasferisce tutti i dati al nuovo dispositivo, lo mette in servizio e lascia il vecchio dispositivo in uno stato di preinstallazione.

È possibile clonare un nodo appliance se è necessario:

- Sostituisci un elettrodomestico che sta per raggiungere la fine del suo ciclo di vita.
- Aggiorna un nodo esistente per sfruttare i vantaggi della tecnologia avanzata degli elettrodomestici.
- Aumenta la capacità di archiviazione della griglia senza modificare il numero di nodi di archiviazione nel tuo sistema StorageGRID .
- Migliorare l'efficienza di archiviazione, ad esempio modificando la modalità RAID.

Vedere ["Clonazione del nodo dell'appliance"](#) per i dettagli.

Considerazioni sui nodi di archiviazione connessi

Esaminare le considerazioni per la dismissione di un nodo di archiviazione connesso.

- Non dovresti dismettere più di 10 nodi di archiviazione in un'unica procedura di dismissione del nodo.
- Il sistema deve, in ogni momento, includere un numero sufficiente di nodi di archiviazione per soddisfare i requisiti operativi, tra cui ["Quorum ADC"](#) e l'attivo ["Politica ILM"](#) . Per soddisfare questa restrizione, potrebbe essere necessario aggiungere un nuovo nodo di archiviazione in un'operazione di espansione prima di poter dismettere un nodo di archiviazione esistente.

Prestare attenzione quando si dismettono nodi di archiviazione in una griglia contenente nodi basati solo su software. Se si dismettono tutti i nodi configurati per archiviare sia oggetti che metadati, la possibilità di

archiviare oggetti viene rimossa dalla griglia. Vedere ["Tipi di nodi di archiviazione"](#) per ulteriori informazioni sui nodi di archiviazione solo metadati.

- Quando si rimuove un nodo di archiviazione, grandi volumi di dati di oggetti vengono trasferiti sulla rete. Sebbene questi trasferimenti non dovrebbero influire sul normale funzionamento del sistema, possono influire sulla quantità totale di larghezza di banda di rete consumata dal sistema StorageGRID .
- Alle attività associate alla dismissione del nodo di archiviazione viene assegnata una priorità inferiore rispetto alle attività associate alle normali operazioni di sistema. Ciò significa che la dismissione non interferisce con le normali operazioni del sistema StorageGRID e non deve essere programmata per un periodo di inattività del sistema. Poiché la dismissione viene eseguita in background, è difficile stimare quanto tempo ci vorrà per completarla. In generale, la dismissione viene completata più rapidamente quando il sistema è inattivo o se viene rimosso un solo nodo di archiviazione alla volta.
- Potrebbero essere necessari giorni o settimane per dismettere un nodo di archiviazione. Pianificare questa procedura di conseguenza. Sebbene il processo di dismissione sia concepito per non influire sulle operazioni del sistema, può limitare altre procedure. In generale, è opportuno eseguire eventuali aggiornamenti o espansioni pianificati del sistema prima di rimuovere i nodi della griglia.
- Se è necessario eseguire un'altra procedura di manutenzione mentre i nodi di archiviazione vengono rimossi, è possibile ["sospendere la procedura di dismissione"](#) e riprenderla dopo aver completato l'altra procedura.



Il pulsante **Pausa** è abilitato solo quando vengono raggiunte le fasi di valutazione ILM o di disattivazione dei dati codificati in cancellazione; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background.

- Non è possibile eseguire operazioni di riparazione dei dati su alcun nodo della griglia quando è in esecuzione un'attività di dismissione.
- Non apportare modifiche a una policy ILM mentre un nodo di archiviazione è in fase di dismissione.
- Per rimuovere i dati in modo permanente e sicuro, è necessario cancellare le unità del nodo di archiviazione una volta completata la procedura di dismissione.

Considerazioni sui nodi di archiviazione disconnessi

Esaminare le considerazioni per la dismissione di un nodo di archiviazione disconnesso.

- Non disattivare mai un nodo disconnesso a meno che non si sia certi che non possa essere riattivato o ripristinato.



Non eseguire questa procedura se ritieni che sia possibile recuperare i dati dell'oggetto dal nodo. Contattare invece l'assistenza tecnica per verificare se è possibile il ripristino del nodo.

- Quando si dismette un nodo di archiviazione disconnesso, StorageGRID utilizza i dati di altri nodi di archiviazione per ricostruire i dati e i metadati degli oggetti presenti sul nodo disconnesso.
- Potrebbe verificarsi una perdita di dati se si dismette più di un nodo di archiviazione disconnesso. Il sistema potrebbe non essere in grado di ricostruire i dati se non sono disponibili sufficienti copie di oggetti, frammenti con codice di cancellazione o metadati di oggetti. Quando si dismettono i nodi di archiviazione in una griglia con nodi basati solo su software, la dismissione di tutti i nodi configurati per archiviare sia oggetti che metadati rimuove tutto lo storage degli oggetti dalla griglia. Vedere ["Tipi di nodi di archiviazione"](#) per ulteriori informazioni sui nodi di archiviazione solo metadati.



Se hai più di un nodo di archiviazione disconnesso che non riesci a ripristinare, contatta l'assistenza tecnica per determinare la soluzione migliore.

- Quando si dismette un nodo di archiviazione disconnesso, StorageGRID avvia i processi di riparazione dei dati al termine del processo di dismissione. Questi lavori tentano di ricostruire i dati e i metadati dell'oggetto archiviati sul nodo disconnesso.
- Quando si dismette un nodo di archiviazione disconnesso, la procedura di dismissione si completa in tempi relativamente rapidi. Tuttavia, i lavori di riparazione dei dati possono richiedere giorni o settimane e non vengono monitorati dalla procedura di disattivazione. È necessario monitorare manualmente questi lavori e riavviarli quando necessario. Vedere ["Controlla i lavori di riparazione dei dati"](#).
- Se si dismette un nodo di archiviazione disconnesso che contiene l'unica copia di un oggetto, l'oggetto andrà perso. I processi di riparazione dei dati possono ricostruire e recuperare oggetti solo se sui nodi di archiviazione attualmente connessi è presente almeno una copia replicata o un numero sufficiente di frammenti con codice di cancellazione.

Qual è il quorum dell'ADC?

Potrebbe non essere possibile dismettere determinati nodi di archiviazione in un sito se dopo la dismissione rimangono troppo pochi servizi di controller di dominio amministrativo (ADC).

Il servizio ADC, presente su alcuni nodi di archiviazione, gestisce le informazioni sulla topologia della griglia e fornisce servizi di configurazione alla griglia. Il sistema StorageGRID richiede che un quorum di servizi ADC sia disponibile in ogni sito e in ogni momento.

Non è possibile dismettere un nodo di archiviazione se la rimozione del nodo impedirebbe il raggiungimento del quorum ADC. Per soddisfare il quorum ADC durante una dismissione, almeno tre nodi di archiviazione in ogni sito devono disporre del servizio ADC. Se un sito ha più di tre nodi di archiviazione con il servizio ADC, la maggioranza semplice di tali nodi deve rimanere disponibile dopo la dismissione: $((0.5 * \text{Storage Nodes with ADC}) + 1)$



Prestare attenzione quando si dismettono nodi di archiviazione in una griglia contenente nodi basati solo su software. Se si dismettono tutti i nodi configurati per archiviare sia oggetti che metadati, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere ["Tipi di nodi di archiviazione"](#) per ulteriori informazioni sui nodi di archiviazione solo metadati.

Ad esempio, supponiamo che un sito includa attualmente sei nodi di archiviazione con servizi ADC e che si desideri dismettere tre nodi di archiviazione. A causa del requisito del quorum ADC, è necessario completare due procedure di dismissione, come segue:

- Nella prima procedura di dismissione, è necessario assicurarsi che rimangano disponibili quattro nodi di archiviazione con servizi ADC: $((0.5 * 6) + 1)$. Ciò significa che inizialmente è possibile dismettere solo due nodi di archiviazione.
- Nella seconda procedura di dismissione, è possibile rimuovere il terzo nodo di archiviazione perché il quorum ADC richiede ora che rimangano disponibili solo tre servizi ADC: $((0.5 * 4) + 1)$.

Se è necessario dismettere un nodo di archiviazione ma non è possibile a causa del requisito di quorum ADC, aggiungere un nuovo nodo di archiviazione in un'"[espansione](#)" e specificare che dovrebbe avere un servizio ADC. Quindi, dismettere il nodo di archiviazione esistente.

Se si prevede di dismettere un nodo di archiviazione, è necessario rivedere la policy ILM del sistema StorageGRID prima di avviare il processo di dismissione.

Durante la dismissione, tutti i dati degli oggetti vengono migrati dal nodo di archiviazione dismesso ad altri nodi di archiviazione.



La politica ILM in vigore *durante* la dismissione sarà quella utilizzata *dopo* la dismissione. È necessario assicurarsi che questa policy soddisfi i requisiti dei dati sia prima di iniziare la dismissione sia dopo il suo completamento.

Dovresti rivedere le regole in ogni "[politica ILM attiva](#)" per garantire che il sistema StorageGRID continui ad avere una capacità sufficiente del tipo corretto e nelle posizioni corrette per gestire la dismissione di un nodo di archiviazione.

Considera quanto segue:

- Sarà possibile per i servizi di valutazione ILM 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 dismissione? È possibile effettuare copie aggiuntive in un luogo alternativo?
- In che modo il processo di dismissione influirà sulla distribuzione finale dei contenuti? Come descritto in "[Consolidamento dei nodi di archiviazione](#)", dovresti "[aggiungere nuovi nodi di archiviazione](#)" prima di smantellare quelli vecchi. Se si aggiunge un nodo di archiviazione sostitutivo più grande dopo aver dismesso un nodo di archiviazione più piccolo, i vecchi nodi di archiviazione potrebbero essere prossimi alla capacità massima e il nuovo nodo di archiviazione potrebbe non avere quasi alcun contenuto. La maggior parte delle operazioni di scrittura per i nuovi dati oggetto verrebbero quindi indirizzate al nuovo nodo di archiviazione, riducendo l'efficienza complessiva delle operazioni di sistema.
- Il sistema includerà sempre un numero sufficiente di nodi di archiviazione per soddisfare le policy ILM attive?



Una policy ILM che non può essere soddisfatta causerà arretrati e avvisi e potrebbe interrompere il funzionamento del sistema StorageGRID .

Verificare che la topologia proposta che risulterà dal processo di dismissione soddisfi la politica ILM valutando le aree elencate nella tabella.

Area da valutare	Cosa considerare
Capacità disponibile	Ci sarà sufficiente capacità di archiviazione per contenere tutti i dati degli oggetti archiviati nel sistema StorageGRID , comprese le copie permanenti dei dati degli oggetti attualmente archiviati sul nodo di archiviazione da dismettere? Ci sarà capacità sufficiente per gestire la crescita prevista dei dati degli oggetti archiviati per un intervallo di tempo ragionevole dopo il completamento della dismissione?

Area da valutare	Cosa considerare
Luogo di stoccaggio	Se nel sistema StorageGRID nel suo complesso rimane una capacità sufficiente, la capacità è nelle posizioni giuste per soddisfare le regole aziendali del sistema StorageGRID ?
Tipo di archiviazione	Una volta completata la dismissione, ci sarà abbastanza spazio di stoccaggio del tipo appropriato? Ad esempio, le regole ILM potrebbero spostare i contenuti da un tipo di archiviazione a un altro man mano che i contenuti invecchiano. In questo caso, è necessario assicurarsi che nella configurazione finale del sistema StorageGRID sia disponibile spazio di archiviazione sufficiente del tipo appropriato.

Consolidamento dei nodi di archiviazione

È possibile consolidare i nodi di archiviazione per ridurre il numero di nodi di archiviazione per un sito o una distribuzione, aumentando al contempo la capacità di archiviazione.

Quando si consolidano i nodi di archiviazione, ["espandere il sistema StorageGRID"](#) aggiungendo nuovi nodi di archiviazione con capacità maggiore e quindi dismettendo i vecchi nodi di archiviazione con capacità inferiore. Durante la procedura di dismissione, gli oggetti vengono migrati dai vecchi nodi di archiviazione ai nuovi nodi di archiviazione.



Se stai consolidando elettrodomestici più vecchi e più piccoli con nuovi modelli o elettrodomestici di maggiore capacità, considera ["clonazione del nodo dell'appliance"](#) (oppure utilizzare la clonazione del nodo dell'appliance e la procedura di dismissione se non si sta eseguendo una sostituzione uno a uno).

Ad esempio, potresti aggiungere due nuovi nodi di archiviazione con capacità maggiore per sostituire tre nodi di archiviazione più vecchi. Per prima cosa, dovresti utilizzare la procedura di espansione per aggiungere i due nuovi nodi di archiviazione più grandi, quindi utilizzare la procedura di dismissione per rimuovere i tre vecchi nodi di archiviazione di capacità inferiore.

Aggiungendo nuova capacità prima di rimuovere i nodi di archiviazione esistenti, si garantisce una distribuzione più equilibrata dei dati nel sistema StorageGRID . Si riduce inoltre la possibilità che un nodo di archiviazione esistente possa essere spinto oltre il livello di filigrana di archiviazione.

Disattivare più nodi di archiviazione

Se è necessario rimuovere più di un nodo di archiviazione, è possibile dismetterli in sequenza o in parallelo.



Prestare attenzione quando si dismettono nodi di archiviazione in una griglia contenente nodi basati solo su software. Se si dismettono tutti i nodi configurati per archiviare sia oggetti che metadati, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere ["Tipi di nodi di archiviazione"](#) per ulteriori informazioni sui nodi di archiviazione solo metadati.

- Se si dismettono i nodi di archiviazione in sequenza, è necessario attendere che il primo nodo di

archiviazione completi la dismissione prima di iniziare a dismettere il nodo di archiviazione successivo.

- Se si dismettono i nodi di archiviazione in parallelo, i nodi di archiviazione elaborano simultaneamente le attività di dismissione per tutti i nodi di archiviazione in fase di dismissione. Ciò può comportare una situazione in cui tutte le copie permanenti di un file vengono contrassegnate come "di sola lettura", disabilitando temporaneamente l'eliminazione nelle griglie in cui questa funzionalità è abilitata.

Controlla i lavori di riparazione dei dati

Prima di dismettere un nodo della griglia, è necessario confermare che non siano attivi processi di riparazione dei dati. Se una riparazione non ha avuto successo, è necessario riavviarla e lasciarla completare prima di eseguire la procedura di dismissione.

Informazioni su questo compito

Se è necessario dismettere un nodo di archiviazione disconnesso, è necessario completare anche questi passaggi al termine della procedura di dismissione per garantire che il processo di riparazione dei dati sia stato completato correttamente. È necessario assicurarsi che tutti i frammenti con codice di cancellazione presenti sul nodo rimosso siano stati ripristinati correttamente.

Questi passaggi si applicano solo ai sistemi che dispongono di oggetti con codice di cancellazione.

Passi

1. Accedi al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Controllare le riparazioni in corso: `repair-data show-ec-repair-status`

- Se non hai mai eseguito un processo di riparazione dei dati, l'output è `No job found`. Non è necessario riavviare alcun lavoro di riparazione.
- Se il processo di riparazione dei dati è stato eseguito in precedenza o è in esecuzione attualmente, 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



Facoltativamente, è possibile utilizzare Grid Manager per monitorare i processi di ripristino in corso e visualizzare una cronologia dei ripristini. Vedere ["Ripristina i dati degli oggetti utilizzando Grid Manager"](#).

3. Se lo Stato per tutte le riparazioni è `Completed`, non è necessario riavviare alcun processo di riparazione.
4. Se lo Stato per qualsiasi riparazione è `Stopped`, è necessario riavviare la riparazione.
 - a. Ottieni l'ID di riparazione per la riparazione non riuscita dall'output.

b. Esegui il `repair-data start-ec-node-repair` comando.

Utilizzare il `--repair-id` opzione per specificare l'ID di riparazione. Ad esempio, se si desidera riprovare una riparazione con ID di riparazione 949292, eseguire questo comando: `repair-data start-ec-node-repair --repair-id 949292`

c. Continuare a monitorare lo stato delle riparazioni dei dati EC finché lo Stato per tutte le riparazioni non è Completed .

Raccogli i materiali richiesti

Prima di procedere alla dismissione di un nodo della griglia, è necessario ottenere le seguenti informazioni.

Articolo	Note
Pacchetto di recupero .zip file	Devi scaricare il pacchetto di ripristino più recente .zip file(<code>sgws-recovery-package-id-revision.zip</code>). 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.
Frase segreta di provisioning	La passphrase viene creata e documentata quando il sistema StorageGRID viene installato per la prima volta. La passphrase di provisioning non è presente nel <code>Passwords.txt</code> file.
Descrizione della topologia del sistema StorageGRID prima della dismissione	Se disponibile, procurarsi la documentazione che descrive la topologia attuale del sistema.

Informazioni correlate

["Requisiti del browser web"](#)

Accedi alla pagina Nodi di dismissione

Quando si accede alla pagina Decommission Nodes in Grid Manager, è possibile vedere a colpo d'occhio quali nodi possono essere dismessi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#) .



Prestare attenzione quando si dismettono nodi di archiviazione in una griglia contenente nodi basati solo su software. Se si dismettono tutti i nodi configurati per archiviare sia oggetti che metadati, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere ["Tipi di nodi di archiviazione"](#) per ulteriori informazioni sui nodi di archiviazione solo metadati.

Passi

1. Selezionare **MANUTENZIONE > Attività > Dismissione**.

2. Selezionare **Dismissione nodi**.

Viene visualizzata la pagina Nodi dismessi. Da questa pagina puoi:

- Determinare quali nodi della griglia possono essere attualmente dismessi.
- Visualizza lo stato di salute di tutti i nodi della griglia
- Ordina l'elenco in ordine crescente o decrescente per **Nome**, **Sito**, **Tipo** o **Ha ADC**.
- Inserisci i termini di ricerca per trovare rapidamente nodi specifici.

In questo esempio, la colonna Dismissione possibile indica che è possibile dismettere 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 ogni nodo che si desidera dismettere.

Se un nodo della griglia può essere dismesso, questa colonna include un segno di spunta verde e la colonna di sinistra include una casella di controllo. Se un nodo non può essere dismesso, questa colonna descrive il problema. Se esiste più di un motivo per cui un nodo non può essere dismesso, viene mostrato il motivo più critico.

Possibile motivo di disattivazione	Descrizione	Passaggi per risolvere
No, la dismissione del tipo <i>node</i> non è supportata.	Non è possibile disattivare il nodo di amministrazione primario.	Nessuno.

Possibile motivo di disattivazione	Descrizione	Passaggi per risolvere
No, almeno un nodo della griglia è disconnesso. Nota: questo messaggio viene visualizzato solo per i nodi della griglia connessi.	Non è possibile disattivare un nodo della rete connesso se un nodo della rete è disconnesso. La colonna Salute include una di queste icone per i nodi della griglia disconnessi:  (grigio): Amministrativamente inattivo  (blu): Sconosciuto	È necessario riportare online tutti i nodi disconnessi o "dismettere tutti i nodi disconnessi" prima di poter rimuovere un nodo connesso. Nota: se la rete contiene più nodi disconnessi, il software richiede di disattivarli tutti contemporaneamente, il che aumenta il rischio di risultati imprevisti.
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 dismettere un nodo di rete disconnesso se anche uno o più nodi necessari sono disconnessi (ad esempio, un nodo di archiviazione necessario per il quorum ADC).	- Esaminare i messaggi di possibile dismissione per tutti i nodi disconnessi. - Determinare quali nodi non possono essere dismessi perché necessari. - Se lo stato di un nodo richiesto è amministrativamente inattivo, riportare il nodo online. - Se lo stato di un nodo richiesto è sconosciuto, eseguire una procedura di ripristino del nodo per recuperarlo.
No, membro del gruppo/i HA: <i>nome del gruppo</i>. Prima di poter dismettere questo nodo, è necessario rimuoverlo da tutti i gruppi HA.	Non è possibile disattivare un nodo amministrativo o un nodo gateway se un'interfaccia del 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 gruppi ad alta disponibilità".
No, il sito <i>x</i> richiede un minimo di <i>n</i> nodi di archiviazione con servizi ADC.	Solo nodi di archiviazione. Non è possibile dismettere un nodo di archiviazione se nel sito non rimarrebbero nodi sufficienti a supportare i requisiti di quorum ADC.	Eseguire un'espansione. Aggiungere un nuovo nodo di archiviazione al sito e specificare che deve disporre di un servizio ADC. Vedi informazioni su "Quorum ADC".

Possibile motivo di disattivazione	Descrizione	Passaggi per risolvere
No, uno o più profili di codifica di cancellazione necessitano di almeno n nodi di archiviazione. Se il profilo non viene utilizzato in una regola ILM, è possibile disattivarlo.	Solo nodi di archiviazione. Non è possibile dismettere un nodo di archiviazione a meno che non rimangano nodi sufficienti per i profili di codifica di cancellazione esistenti. Ad esempio, se esiste un profilo di codifica di cancellazione per la codifica di cancellazione 4+2, devono rimanere almeno 6 nodi di archiviazione.	Per ciascun profilo di codifica di cancellazione interessato, eseguire uno dei seguenti passaggi, in base al modo in cui viene utilizzato il profilo: • Utilizzato nelle policy ILM attive: Esegue un'espansione. Aggiungere un numero sufficiente di nuovi nodi di archiviazione per consentire la continuazione della codifica di cancellazione. Vedi le istruzioni per "espandere la tua griglia". • Utilizzato in una regola ILM ma non nei criteri ILM attivi: modifica o elimina la regola e quindi disattiva il profilo di codifica di cancellazione. • Non utilizzato in nessuna regola ILM: Disattiva il profilo di codifica di cancellazione. Nota: viene visualizzato un messaggio di errore se si tenta di disattivare un profilo di codifica di cancellazione e i dati dell'oggetto sono ancora associati al profilo. Potrebbe essere necessario attendere diverse settimane prima di provare nuovamente la procedura di disattivazione. Scopri di più "disattivazione di un profilo di codifica di cancellazione".
No, non è possibile disattivare un nodo di archivio a meno che il nodo non sia disconnesso.	Se un nodo archivio è ancora connesso, non è possibile rimuoverlo.	Nota: il supporto per i nodi di archivio è stato rimosso. Se è necessario dismettere un nodo di archivio, vedere "Dismissione del nodo di rete (sito di documentazione StorageGRID 11.8)"

Disattivare i nodi della rete disconnessi

Potrebbe essere necessario dismettere un nodo che al momento non è connesso alla rete (uno il cui stato di integrità è sconosciuto o amministrativamente inattivo).

Prima di iniziare

- Hai compreso le considerazioni per la dismissione "[Nodi di amministrazione e gateway](#)" e le considerazioni per la dismissione "[Nodi di archiviazione](#)".
- Hai ottenuto tutti gli elementi prerequisites.
- Hai verificato che non ci siano processi di riparazione dati attivi. Vedere "[Controlla i lavori di riparazione dei dati](#)".
- Hai confermato che il ripristino del nodo di archiviazione non è in corso in nessuna parte della griglia. In tal caso, è necessario attendere il completamento di qualsiasi ricostruzione di Cassandra eseguita come parte del ripristino. Si può quindi procedere con la dismissione.
- Hai assicurato che non verranno eseguite altre procedure di manutenzione mentre è in esecuzione la procedura di dismissione del nodo, a meno che la procedura di dismissione del nodo non sia in pausa.
- La colonna **Dismissione possibile** per il nodo o i nodi disconnessi che si desidera dismettere include un segno di spunta verde.
- Hai la passphrase di provisioning.

Informazioni su questo compito

È possibile identificare i nodi disconnessi cercando l'icona blu Sconosciuto  o l'icona grigia Amministrativamente in basso  nella colonna **Salute**.

Prima di disattivare un nodo disconnesso, tenere presente quanto segue:

- Questa procedura è pensata principalmente per rimuovere un singolo nodo disconnesso. Se la rete contiene più nodi disconnessi, il software richiede di disattivarli tutti contemporaneamente, aumentando il rischio di risultati imprevisti.



Potrebbe verificarsi una perdita di dati se si dismettono più nodi di archiviazione disconnessi contemporaneamente. Vedere "[Considerazioni sui nodi di archiviazione disconnessi](#)".



Prestare attenzione quando si dismettono nodi di archiviazione in una griglia contenente nodi basati solo su software. Se si dismettono tutti i nodi configurati per archiviare sia oggetti che metadati, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere "[Tipi di nodi di archiviazione](#)" per ulteriori informazioni sui nodi di archiviazione solo metadati.

- Se non è possibile rimuovere un nodo disconnesso (ad esempio, un nodo di archiviazione necessario per il quorum ADC), non è possibile rimuovere nessun altro nodo disconnesso.

Passi

1. A meno che non si stia dismettendo un nodo di archivio (che deve essere disconnesso), provare a riportare online i nodi della griglia disconnessi o a recuperarli.

Vedere "[Procedure di ripristino del nodo della griglia](#)" per istruzioni.

2. Se non è possibile ripristinare un nodo della rete disconnesso e si desidera disattivarlo mentre è disconnesso, selezionare la casella di controllo per quel nodo.



Se la rete contiene più nodi disconnessi, il software richiede di disattivarli tutti contemporaneamente, aumentando il rischio di risultati imprevisti.



Prestare attenzione quando si sceglie di dismettere più di un nodo di rete disconnesso alla volta, soprattutto se si selezionano più nodi di archiviazione disconnessi. Se hai più di un nodo di archiviazione disconnesso che non riesci a ripristinare, contatta l'assistenza tecnica per determinare la soluzione migliore.

3. Immettere la passphrase di provisioning.

Il pulsante **Avvia disattivazione** è abilitato.

4. Fare clic su **Avvia dismissione**.

Viene visualizzato un avviso che indica che è stato selezionato un nodo disconnesso e che i dati dell'oggetto andranno persi se il nodo ha l'unica copia di un oggetto.

5. Esaminare l'elenco dei nodi e fare clic su **OK**.

Viene avviata la procedura di dismissione e per ogni nodo viene visualizzato lo stato di avanzamento. Durante la procedura viene generato un nuovo pacchetto di ripristino contenente la modifica alla 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 Pacchetto di ripristino. Quindi, scarica il .zip file.

Vedi le istruzioni per "[scaricando il pacchetto di ripristino](#)".



Scarica il pacchetto di ripristino il prima possibile per assicurarti di poter ripristinare la tua rete se qualcosa va storto durante la procedura di dismissione.



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 Decommission per assicurarsi che tutti i nodi selezionati vengano dismessi correttamente.

La dismissione dei nodi di archiviazione può richiedere giorni o settimane. Una volta completate tutte le attività, l'elenco di selezione dei nodi viene nuovamente visualizzato con un messaggio di successo. Se hai dismesso un nodo di archiviazione disconnesso, un messaggio informativo indica che i processi di riparazione sono stati avviati.

8. Dopo che i nodi si sono arrestati automaticamente come parte della procedura di dismissione, rimuovere tutte le macchine virtuali rimanenti o altre risorse associate al nodo dismesso.



Non eseguire questo passaggio finché i nodi non si saranno spenti automaticamente.

9. Se si sta dismettendo un nodo di archiviazione, monitorare lo stato dei processi di riparazione dei **dati replicati** e dei **dati con codice di cancellazione (EC)** che vengono avviati automaticamente durante il processo di dismissione.

Dati replicati

- Per ottenere una percentuale stimata di completamento per la riparazione replicata, aggiungere `show-replicated-repair-status` opzione al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Per determinare se le riparazioni sono state completate:
 - a. Selezionare **NODI > Nodo di archiviazione in riparazione > ILM**.
 - b. Esaminare gli attributi nella sezione Valutazione. Una volta completate le riparazioni, l'attributo **In attesa - Tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
 - a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - b. Selezionare **grid > Nodo di archiviazione in riparazione > LDR > Data Store**.
 - c. Utilizzare una combinazione dei seguenti attributi per determinare, nel miglior modo possibile, se le riparazioni replicate sono complete.



Potrebbero essere presenti incongruenze in Cassandra e le riparazioni non riuscite non vengono tracciate.

- **Riparazioni tentate (XRPA)**: utilizzare questo attributo per monitorare l'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di archiviazione tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo più lungo del periodo di scansione corrente (fornito dall'attributo **Periodo di scansione - Stimato**), significa che la scansione ILM non ha trovato oggetti ad alto rischio che necessitano di riparazione su alcun nodo.



Gli oggetti ad alto rischio sono oggetti che rischiano di andare completamente persi. Sono esclusi gli oggetti che non soddisfano la loro configurazione ILM.

- **Periodo di scansione - Stimato (XSCM)**: utilizzare questo attributo per stimare quando una modifica della policy verrà applicata agli oggetti precedentemente acquisiti. Se l'attributo **Riparazioni tentate** non aumenta per un periodo più lungo del periodo di scansione corrente, è probabile che siano state eseguite riparazioni replicate. Si noti che il periodo di scansione può variare. L'attributo **Periodo di scansione - Stimato (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione dei nodi. È possibile interrogare la cronologia degli attributi **Periodo di scansione - Stima** per la griglia per determinare un intervallo di tempo appropriato.

Dati con codice di cancellazione (EC)

Per monitorare la riparazione dei dati codificati in modo da cancellarli e riprovare eventuali richieste non riuscite:

1. Determinare lo stato delle riparazioni dei dati codificati tramite cancellazione:
 - Selezionare **SUPPORTO > Strumenti > Metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, seleziona **Panoramica EC** nella sezione Grafana. Consulta i dashboard **Tempo stimato per il completamento del lavoro EC in griglia** e **Percentuale completata del lavoro EC in griglia**.
 - Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` operazione:

```
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 eseguite in precedenza e attualmente.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

Questo comando riprova una riparazione del nodo non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Questo comando riprova una riparazione del volume non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Dopo aver finito

Non appena i nodi disconnessi sono stati dismessi e tutti i lavori di riparazione dei dati sono stati completati, è possibile dismettere tutti i nodi della griglia connessi, se necessario.

Dopo aver completato la procedura di dismissione, completa questi passaggi:

- Assicurarsi che le unità del nodo di rete dismesso siano state cancellate. Utilizzare uno strumento o un servizio di cancellazione dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dalle unità.
- Se hai dismesso un nodo dell'appliance e i dati sull'appliance erano protetti tramite crittografia del nodo, usa StorageGRID Appliance Installer per cancellare la configurazione del server di gestione delle chiavi (Clear KMS). Se si desidera aggiungere l'appliance a un'altra griglia, è necessario cancellare la configurazione KMS. Per le istruzioni, vedere ["Monitora la crittografia del nodo in modalità di manutenzione"](#).

Disattivare i nodi della rete connessi

È possibile dismettere e rimuovere definitivamente i nodi collegati alla rete.

Prima di iniziare

- Hai compreso le considerazioni per la dismissione ["Nodi di amministrazione e gateway"](#) e le considerazioni per la dismissione ["Nodi di archiviazione"](#).
- Hai raccolto tutto il materiale necessario.
- Hai verificato che non ci siano processi di riparazione dati attivi.
- Hai confermato che il ripristino del nodo di archiviazione non è in corso in nessuna parte della griglia. In tal caso, attendere il completamento di qualsiasi ricostruzione di Cassandra eseguita come parte del ripristino. Si può quindi procedere con la dismissione.
- Hai assicurato che non verranno eseguite altre procedure di manutenzione mentre è in esecuzione la

procedura di dismissione del nodo, a meno che la procedura di dismissione del nodo non sia in pausa.

- Hai la passphrase di provisioning.
- I nodi della griglia sono collegati.
- La colonna **Dismissione possibile** per il nodo o i nodi che si desidera dismettere include un segno di spunta verde.



La dismissione non verrà avviata se uno o più volumi sono offline (smontati) o se sono online (montati) ma in stato di errore.



Se uno o più volumi vanno offline mentre è in corso una dismissione, il processo di dismissione viene completato dopo che i volumi tornano online.

- Tutti i nodi della griglia hanno una salute normale (verde) . Se vedi una di queste icone nella colonna **Salute**, devi provare a risolvere il problema:

Icona	Colore	Gravità
	Giallo	Avviso
	Arancione chiaro	Minore
	Arancione scuro	Maggiore
	Rosso	Critico

- Se in precedenza hai dismesso un nodo di archiviazione disconnesso, tutti i processi di riparazione dei dati sono stati completati correttamente. Vedere "[Controlla i lavori di riparazione dei dati](#)".



Non rimuovere la macchina virtuale o altre risorse di un nodo della griglia finché non ti viene richiesto in questa procedura.



Prestare attenzione quando si dismettono nodi di archiviazione in una griglia contenente nodi basati solo su software. Se si dismettono tutti i nodi configurati per archiviare sia oggetti che metadati, la possibilità di archiviare oggetti viene rimossa dalla griglia. Vedere "[Tipi di nodi di archiviazione](#)" per ulteriori informazioni sui nodi di archiviazione solo metadati.

Informazioni su questo compito

Quando un nodo viene dismesso, i suoi servizi vengono disabilitati e il nodo si spegne automaticamente.

Passi

1. Nella pagina Nodi di dismissione, seleziona la casella di controllo per ogni nodo della griglia che desideri dismettere.
2. Immettere la passphrase di provisioning.

Il pulsante **Avvia disattivazione** è abilitato.

3. Selezionare **Avvia dismissione**.

4. Esaminare l'elenco dei nodi nella finestra di dialogo di conferma e selezionare **OK**.

Viene avviata la procedura di dismissione del nodo e per ogni nodo viene visualizzato lo stato di avanzamento.



Non mettere offline un nodo di archiviazione dopo l'avvio della procedura di dismissione. La modifica dello stato potrebbe comportare la mancata copia di alcuni contenuti in altre posizioni.

5. Non appena il nuovo Pacchetto di ripristino è disponibile, seleziona il collegamento Pacchetto di ripristino nel banner oppure seleziona **MANUTENZIONE > Sistema > Pacchetto di ripristino** per accedere alla pagina Pacchetto di ripristino. Quindi, scarica il .zip file.

Vedere "[scaricando il pacchetto di ripristino](#)".



Scarica il pacchetto di ripristino il prima possibile per assicurarti di poter ripristinare la tua rete se qualcosa va storto durante la procedura di dismissione.

6. Monitorare periodicamente la pagina Nodi dismessi per assicurarsi che tutti i nodi selezionati vengano dismessi correttamente.



La dismissione dei nodi di archiviazione può richiedere giorni o settimane.

Una volta completate tutte le attività, l'elenco di selezione dei nodi viene nuovamente visualizzato con un messaggio di successo.

Dopo aver finito

Completare questi passaggi dopo aver completato la procedura di dismissione del nodo:

1. Segui i passaggi appropriati per la tua piattaforma. Per esempio:
 - **Linux:** Potresti voler staccare i volumi ed eliminare i file di configurazione del nodo creati durante l'installazione. Vedere "[Installa StorageGRID su Red Hat Enterprise Linux](#)" E "[Installa StorageGRID su Ubuntu o Debian](#)".
 - **VMware:** Potresti voler utilizzare l'opzione "Elimina dal disco" di vCenter per eliminare la macchina virtuale. Potrebbe anche essere necessario eliminare eventuali dischi dati indipendenti dalla macchina virtuale.
 - * Appliance StorageGRID *: il nodo dell'appliance torna automaticamente a uno stato non distribuito in cui 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 le unità del nodo di rete dismesso siano state cancellate. Utilizzare uno strumento o un servizio di cancellazione dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dalle unità.
3. Se hai dismesso un nodo dell'appliance e i dati sull'appliance erano protetti tramite crittografia del nodo, usa StorageGRID Appliance Installer per cancellare la configurazione del server di gestione delle chiavi (Clear KMS). Se si desidera aggiungere l'appliance a un'altra griglia, è necessario cancellare la configurazione KMS. Per le istruzioni, vedere "[Monitora la crittografia del nodo in modalità di manutenzione](#)".

Sospendi e riprendi il processo di dismissione per i nodi di archiviazione

Se è necessario eseguire una seconda procedura di manutenzione, è possibile sospendere la procedura di dismissione di un nodo di archiviazione durante determinate fasi. Una volta completata l'altra procedura, è possibile riprendere la dismissione.



Il pulsante **Pausa** è abilitato solo quando vengono raggiunte le fasi di valutazione ILM o di disattivazione dei dati codificati in cancellazione; 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"](#).
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).

Passi

1. Selezionare **MANUTENZIONE** > **Attività** > **Dismissione**.

Viene visualizzata la pagina Disattivazione.

2. Selezionare **Dismissione nodi**.

Viene visualizzata la pagina Nodi dismessi. Quando la procedura di disattivazione raggiunge una delle seguenti fasi, il pulsante **Pausa** viene abilitato.

- Valutazione dell'ILM
- Dismissione dei dati codificati tramite cancellazione

3. Selezionare **Pausa** per sospendere la procedura.

La fase corrente è in pausa e il pulsante **Riprendi** è abilitato.

Decommission Nodes

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

Decommissioning procedure has been paused. Click 'Resume' to resume the procedure.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Search				
Name	Type	Progress	Stage	
DC1-S5	Storage Node		Evaluating ILM	

Pause Resume

4. Una volta completata l'altra procedura di manutenzione, selezionare **Riprendi** per procedere con la dismissione.

Sito di dismissione

Considerazioni sulla rimozione di un sito

Prima di utilizzare la procedura di dismissione del sito per rimuovere un sito, è necessario esaminare le considerazioni.

Cosa succede quando si dismette un sito

Quando si dismette un sito, StorageGRID rimuove definitivamente tutti i nodi del sito e il sito stesso dal sistema StorageGRID .

Una volta completata la procedura di dismissione del sito:

- Non è più possibile utilizzare StorageGRID per visualizzare o accedere al sito o a uno qualsiasi dei nodi del sito.
- Non è più possibile utilizzare alcun pool di archiviazione o profilo di codifica di cancellazione che faccia riferimento al sito. Quando StorageGRID dismette un sito, rimuove automaticamente questi pool di archiviazione e disattiva questi profili di codifica di cancellazione.

Differenze tra le procedure di dismissione dei siti connessi e dei siti disconnessi

È possibile utilizzare la procedura di dismissione del sito per rimuovere un sito in cui tutti i nodi sono connessi a StorageGRID (definita dismissione del sito connesso) oppure per rimuovere un sito in cui tutti i nodi sono disconnessi da StorageGRID (definita dismissione del sito disconnesso). Prima di iniziare, è necessario comprendere le differenze tra queste procedure.



Se un sito contiene una miscela di elementi connessi () e nodi disconnessi ( o ), è necessario riportare online tutti i nodi offline.

- La dismissione di un sito connesso consente di rimuovere un sito operativo dal sistema StorageGRID . Ad esempio, è possibile eseguire la dismissione 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 degli oggetti nel sito. Prima di poter avviare la dismissione 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 verificarsi contemporaneamente, ma la procedura consigliata è quella di attendere il completamento dei passaggi ILM prima di avviare la procedura di dismissione effettiva.
- La dismissione di un sito disconnesso consente di rimuovere un sito non funzionante dal sistema StorageGRID . Ad esempio, è possibile eseguire la dismissione di un sito disconnesso per rimuovere un sito distrutto da un incendio o da un'alluvione.

Quando StorageGRID rimuove un sito disconnesso, considera tutti i nodi irrecuperabili e non tenta in alcun modo di preservare i dati. Tuttavia, prima di poter avviare la dismissione di un sito disconnesso, è necessario rimuovere il sito da tutte le regole ILM e attivare una nuova policy ILM.



Prima di eseguire una procedura di dismissione di un sito disconnesso, è necessario contattare il rappresentante dell'account NetApp . NetApp esaminerà i tuoi requisiti prima di abilitare tutti i passaggi della procedura guidata di dismissione del sito. Non tentare di disattivare un sito disconnesso se ritieni che sia possibile ripristinarlo o recuperare 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 essere a conoscenza dei seguenti requisiti:

- Non è possibile dismettere un sito che include il nodo di amministrazione primario.
- Non è possibile dismettere un sito se uno qualsiasi dei nodi ha un'interfaccia che appartiene a un gruppo ad alta disponibilità (HA). È necessario modificare il gruppo HA per rimuovere l'interfaccia del nodo oppure rimuovere l'intero gruppo HA.
- Non è possibile dismettere un sito se contiene una combinazione di elementi connessi () e disconnesso ( O ) nodi.
- Non è possibile dismettere un sito se un nodo in un altro sito è disconnesso ( O ).
- Non è possibile avviare la procedura di dismissione del sito se è in corso un'operazione di riparazione ec-node. Vedere ["Controlla i lavori di riparazione dei dati"](#) per monitorare le riparazioni dei dati codificati in modo da essere cancellati.
- Mentre è in corso la procedura di dismissione del sito:
 - Non è possibile creare regole ILM che facciano riferimento al sito in fase di dismissione. Non è inoltre possibile modificare una regola ILM esistente per fare riferimento al sito.
 - Non è possibile eseguire altre procedure di manutenzione, come l'espansione o l'aggiornamento.



Se è necessario eseguire un'altra procedura di manutenzione durante la dismissione di un sito connesso, è possibile ["mettere in pausa la procedura mentre i nodi di archiviazione vengono rimossi"](#). Il pulsante **Pausa** è abilitato solo quando vengono raggiunte le fasi di valutazione ILM o di disattivazione dei dati codificati in cancellazione; 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 dismissione.

- Se è necessario ripristinare un nodo dopo aver avviato la procedura di dismissione del sito, è necessario contattare l'assistenza.
- Non è possibile dismettere più di un sito alla volta.
- Se il sito include uno o più nodi amministrativi e l'accesso Single Sign-On (SSO) è abilitato per il sistema StorageGRID, è necessario rimuovere tutti i trust delle parti affidabili per il sito da Active Directory Federation Services (AD FS).

Requisiti per la gestione del ciclo di vita delle informazioni (ILM)

Per rimuovere un sito, è necessario aggiornare la configurazione ILM. La procedura guidata Decommission Site ti guida attraverso una serie di passaggi preliminari per garantire quanto segue:

- Il sito non è menzionato in alcuna policy ILM. In tal caso, è necessario modificare le policy oppure creare e attivare policy con nuove regole ILM.
- Nessuna regola ILM fa riferimento al sito, anche se tali regole non sono utilizzate in alcuna policy. È necessario eliminare o modificare tutte le regole che fanno riferimento al sito.

Quando StorageGRID dismette il sito, disattiverà automaticamente tutti i profili di codifica di cancellazione inutilizzati che fanno riferimento al sito ed eliminerà automaticamente tutti i pool di archiviazione inutilizzati che fanno riferimento al sito. Se esiste il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti), viene rimosso perché utilizza tutti i siti.



Prima di poter rimuovere un sito, potrebbe essere necessario creare nuove regole ILM e attivare un nuovo criterio ILM. Queste istruzioni presuppongono che tu abbia una buona conoscenza del funzionamento di ILM e che tu abbia familiarità con la creazione di pool di archiviazione, profili di codifica di cancellazione, regole ILM e simulazione e attivazione di una policy ILM. Vedere ["Gestire gli oggetti con ILM"](#).

Considerazioni sui dati degli oggetti in un sito connesso

Se si sta eseguendo la dismissione di un sito connesso, è necessario decidere cosa fare con i dati degli oggetti esistenti nel sito quando si creano nuove regole ILM e un nuovo criterio ILM. Puoi fare una o entrambe le cose seguenti:

- Sposta i dati degli oggetti dal sito selezionato a uno o più altri siti nella griglia.

Esempio per lo spostamento dei dati: supponiamo che tu voglia dismettere un sito a Raleigh perché hai aggiunto un nuovo sito a Sunnyvale. In questo esempio, si desidera spostare tutti i dati degli oggetti dal vecchio sito al nuovo sito. Prima di aggiornare le regole e le policy ILM, è necessario verificare la capacità di entrambi i siti. È necessario assicurarsi che il sito di Sunnyvale abbia una capacità sufficiente per ospitare i dati degli oggetti provenienti dal sito di Raleigh e che a Sunnyvale rimanga una capacità adeguata per la crescita futura.



Per garantire che sia disponibile una capacità adeguata, potrebbe essere necessario ["espandere una griglia"](#) aggiungendo volumi di archiviazione o nodi di archiviazione a un sito esistente o aggiungendo un nuovo sito prima di eseguire questa procedura.

- Elimina le copie degli oggetti dal sito selezionato.

Esempio di eliminazione dei dati: supponiamo che tu stia attualmente utilizzando una regola ILM a 3 copie per replicare i dati degli oggetti su tre siti. Prima di dismettere un sito, è possibile creare una regola ILM a 2 copie equivalente per archiviare i dati solo in due siti. Quando si attiva un nuovo criterio ILM che utilizza la regola delle 2 copie, StorageGRID elimina le copie dal terzo sito perché non soddisfano più i requisiti ILM. Tuttavia, i dati dell'oggetto saranno comunque protetti e la capacità dei due siti rimanenti rimarrà invariata.



Non creare mai una regola ILM a copia singola per gestire la rimozione di un sito. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Requisiti aggiuntivi per la dismissione di un sito connesso

Prima che StorageGRID possa rimuovere un sito connesso, è necessario verificare quanto segue:

- Tutti i nodi nel sistema StorageGRID devono avere uno stato di connessione **Connesso** (); tuttavia, i nodi possono avere avvisi attivi.



È possibile completare i passaggi da 1 a 4 della procedura guidata Decommission Site se uno o più nodi sono disconnessi. Tuttavia, non è possibile completare il passaggio 5 della procedura guidata, che avvia il processo di dismissione, a meno che tutti i nodi non siano connessi.

- Se il sito che intendi rimuovere contiene un nodo gateway o un nodo amministrativo 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 dismissione del sito.
- Se il sito che intendi rimuovere contiene nodi gateway o nodi amministrativi che si trovano in un gruppo ad alta disponibilità (HA), puoi completare i passaggi da 1 a 4 della procedura guidata di dismissione del sito. Tuttavia, non è possibile completare il passaggio 5 della procedura guidata, che avvia il processo di dismissione, finché non si rimuovono questi nodi da tutti i gruppi HA. Se i client esistenti si connettono a un gruppo HA che include nodi del 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 archiviazione nel sito che si intende rimuovere, è necessario assicurarsi che possano connettersi ai nodi di archiviazione in altri siti prima di avviare la procedura di dismissione del sito.
- È necessario fornire spazio sufficiente sui siti rimanenti per contenere tutti 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 archiviazione, volumi di archiviazione o nuovi siti prima di poter completare la dismissione di un sito connesso.
- È necessario prevedere un tempo adeguato per il completamento della procedura di disattivazione. I processi StorageGRID ILM potrebbero richiedere giorni, settimane o persino mesi per spostare o eliminare i dati degli oggetti dal sito prima che il sito possa essere dismesso.



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 presenti nel sito, del carico sul sistema, delle latenze di rete e della natura delle modifiche ILM richieste.

- Se possibile, dovresti completare i passaggi da 1 a 4 della procedura guidata di dismissione del sito il prima possibile. La procedura di dismissione verrà completata più rapidamente e con meno interruzioni e impatti sulle prestazioni se si consente lo spostamento dei dati dal sito prima di avviare la procedura di dismissione effettiva (selezionando **Avvia dismissione** nel passaggio 5 della procedura guidata).

Requisiti aggiuntivi per la dismissione di un sito disconnesso

Prima che StorageGRID possa rimuovere un sito disconnesso, è necessario verificare quanto segue:

- Hai contattato il rappresentante del tuo account NetApp . NetApp esaminerà i tuoi requisiti prima di abilitare tutti i passaggi della procedura guidata di dismissione del sito.



Non tentare di disattivare un sito disconnesso se ritieni che sia possibile ripristinarlo o recuperare dati di oggetti dal sito. Vedere ["Come il supporto tecnico recupera un sito"](#) .

- Tutti i nodi del sito devono avere uno stato di connessione tra i seguenti:
 - **Sconosciuto** (): Per un motivo sconosciuto, un nodo è disconnesso oppure i servizi sul nodo sono inaspettatamente inattivi. Ad esempio, un servizio sul nodo potrebbe essere interrotto oppure il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione di corrente o di un'interruzione imprevista.

◦ **Amministrativamente inattivo** (🌙): Il nodo non è connesso alla rete per un motivo prevedibile. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente.

- Tutti i nodi in tutti gli altri siti devono avere uno stato di connessione di **Connesso** (✅); tuttavia, questi altri nodi possono avere avvisi attivi.
- Devi comprendere che non potrai più utilizzare StorageGRID per visualizzare o recuperare i dati degli oggetti archiviati nel sito. Quando StorageGRID esegue questa procedura, non tenta in alcun modo di preservare i dati del sito disconnesso.



Se le regole e i criteri ILM sono stati concepiti per proteggere dalla perdita di un singolo sito, copie degli oggetti saranno comunque presenti sui siti rimanenti.

- È necessario comprendere che se il sito conteneva l'unica copia di un oggetto, l'oggetto è andato perso e non può essere recuperato.

Considerazioni sulla coerenza quando si rimuove un sito

La coerenza di un bucket S3 determina se StorageGRID replica completamente i metadati degli oggetti su tutti i nodi e siti prima di comunicare al client che l'acquisizione dell'oggetto è avvenuta correttamente. La coerenza fornisce un equilibrio tra la disponibilità degli oggetti e la coerenza di tali oggetti tra diversi nodi di archiviazione e siti.

Quando StorageGRID rimuove un sito, deve assicurarsi che nessun dato venga scritto sul sito da rimuovere. Di conseguenza, sostituisce temporaneamente la coerenza per ogni bucket o contenitore. Dopo aver avviato il processo di dismissione del sito, StorageGRID utilizza temporaneamente la coerenza del sito per impedire che i metadati degli oggetti vengano scritti sul sito da rimuovere.

Come risultato di questa sostituzione temporanea, tieni presente che tutte le operazioni di scrittura, aggiornamento ed eliminazione del client che si verificano durante la dismissione di un sito potrebbero non riuscire se più nodi diventano non disponibili nei siti rimanenti.

Raccogli i materiali richiesti

Prima di smantellare un sito, è necessario procurarsi i seguenti materiali.

Articolo	Note
Pacchetto di recupero .zip file	Devi 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. "Scarica 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.
Frase segreta di provisioning	La passphrase viene creata e documentata quando il sistema StorageGRID viene installato per la prima volta. La passphrase di provisioning non è presente nel Passwords.txt file.

Articolo	Note
Descrizione della topologia del sistema StorageGRID prima della dismissione	Se disponibile, procurarsi la documentazione che descrive la topologia attuale del sistema.

Informazioni correlate

["Requisiti del browser web"](#)

Passaggio 1: seleziona il sito

Per determinare se un sito può essere dismesso, iniziare accedendo alla procedura guidata Dismissione sito.

Prima di iniziare

- Hai ottenuto tutto il materiale richiesto.
- Hai esaminato le considerazioni per la rimozione di un sito.
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso root o autorizzazioni di manutenzione e ILM"](#).

Passi

1. Selezionare **MANUTENZIONE** > **Attività** > **Dismissione**.
2. Selezionare **Dismissione sito**.

Viene visualizzato il passaggio 1 (Seleziona sito) della procedura guidata Dismissione sito. Questo passaggio include un elenco alfabetico dei siti nel sistema StorageGRID.

Decommission Site

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

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

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

Sites

	Site Name	Used Storage Capacity ?	Decommission Possible
☐	Raleigh	3.93 MB	✓
☐	Sunnyvale	3.97 MB	✓
☐	Vancouver	3.90 MB	No. This site contains the primary Admin Node.

Next

3. Visualizza i valori nella colonna **Capacità di archiviazione utilizzata** per determinare la quantità di spazio di archiviazione attualmente utilizzata per i dati degli oggetti in ciascun sito.

La capacità di archiviazione utilizzata è una stima. Se i nodi sono offline, la capacità di archiviazione utilizzata è l'ultimo valore noto per il sito.

- Per la dismissione di un sito connesso, questo valore rappresenta la quantità di dati oggetto che dovranno essere spostati in altri siti o eliminati da ILM prima di poter dismettere in sicurezza il sito.
- Per la dismissione di un sito disconnesso, questo valore rappresenta la quantità di spazio di archiviazione dati del sistema che diventerà inaccessibile quando si dismette il sito.



Se la tua policy ILM è stata progettata per proteggere dalla perdita di un singolo sito, copie dei dati dell'oggetto dovrebbero comunque esistere sui siti rimanenti.

4. Esaminare i motivi nella colonna **Dismissione possibile** per determinare quali siti possono essere dismessi al momento.



Se sussistono più motivi per cui un sito non può essere dismesso, viene visualizzato il motivo più critico.

Possibile motivo di disattivazione	Descrizione	Passo successivo
Segno di spunta verde (✓)	Puoi disattivare questo sito.	Vai al passo successivo .
No. Questo sito contiene il nodo di amministrazione principale.	Non è possibile dismettere un sito contenente il nodo di amministrazione primario.	Nessuno. Non è possibile eseguire questa procedura.
No. Questo sito contiene uno o più nodi di archivio.	Non è possibile dismettere un sito contenente un nodo archivio.	Nessuno. Non è possibile eseguire questa procedura.
No. Tutti i nodi di questo sito sono disconnessi. Contatta il tuo rappresentante NetApp.	Non è possibile eseguire la dismissione di un sito connesso a meno che ogni nodo del sito non sia connesso (✓).	Se si desidera eseguire la dismissione di un sito disconnesso, è necessario contattare il rappresentante dell'account NetApp, che esaminerà i requisiti e abiliterà il resto della procedura guidata di dismissione del sito. IMPORTANTE: Non disattivare mai i nodi online per poter rimuovere un sito. Perderai dati.

L'esempio mostra un sistema StorageGRID con tre siti. Il segno di spunta verde (✓) per i siti di Raleigh e Sunnyvale indica che è possibile dismettere tali siti. Tuttavia, non è possibile dismettere il sito di Vancouver perché contiene il nodo di amministrazione principale.

1. Se è possibile la dismissione, selezionare il pulsante di opzione per il sito.

Il pulsante **Avanti** è abilitato.

2. Selezionare **Avanti**.

Viene visualizzato il passaggio 2 (Visualizza dettagli).

Passaggio 2: Visualizza i dettagli

Dal passaggio 2 (Visualizza dettagli) della procedura guidata Dismissione sito, è possibile esaminare quali nodi sono inclusi nel sito, vedere quanto spazio è stato utilizzato su ciascun nodo di archiviazione e valutare quanto spazio libero è disponibile negli altri siti nella griglia.

Prima di iniziare

Prima di dismettere un sito, è necessario verificare la quantità di dati degli oggetti presenti nel sito.

- Se si sta eseguendo la dismissione di un sito connesso, è necessario comprendere quanti dati oggetto sono 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.
- Se possibile, eseguire tutte le espansioni necessarie del nodo di archiviazione prima di avviare la procedura di dismissione.
- Se si esegue la dismissione di un sito disconnesso, è necessario comprendere quanti dati degli oggetti diventeranno permanentemente inaccessibili quando si rimuove il sito.

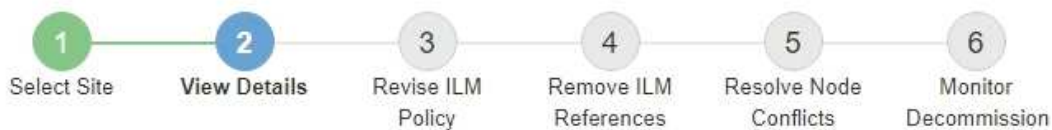


Se si esegue la dismissione di un sito disconnesso, ILM non può spostare o eliminare i dati degli oggetti. Tutti i dati rimasti sul sito andranno persi. Tuttavia, se la tua policy ILM è stata progettata per proteggere dalla perdita di un singolo sito, copie dei dati dell'oggetto saranno comunque presenti sui siti rimanenti. Vedere ["Abilita la protezione contro la perdita del sito"](#).

Passi

1. Dal passaggio 2 (Visualizza dettagli), esamina tutti gli avvisi relativi al sito che hai selezionato per la rimozione.

Decommission Site



Data Center 2 Details

⚠ This site includes a Gateway Node. If clients are currently connecting to this node, you must configure an equivalent node at another site. Be sure clients can connect to the replacement node before starting the decommission procedure.

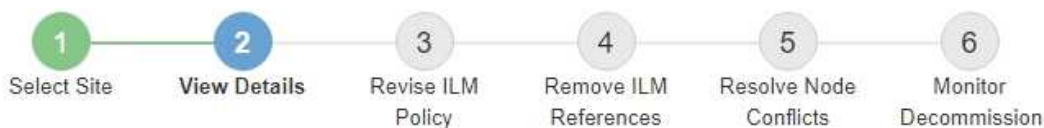
⚠ This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

In questi casi viene visualizzato un avviso:

- Il sito include un Gateway Node. Se i client S3 si stanno attualmente connettendo a questo nodo, è necessario configurare un nodo equivalente in un altro sito. Prima di procedere con la procedura di dismissione, assicurarsi che i client possano connettersi al nodo sostitutivo.
- Il sito contiene una miscela di elementi connessi (✓) e nodi disconnessi (☾ o ⚙). Prima di poter rimuovere questo sito, è necessario riportare online tutti i nodi offline.

2. Esamina i dettagli sul sito che hai scelto di rimuovere.

Decommission Site



Raleigh Details

Number of Nodes: 3
Used Space: 3.93 MB

Free Space: 475.38 GB
Site Capacity: 475.38 GB

Node Name	Node Type	Connection State	Details
RAL-S1-101-196	Storage Node	✓	1.30 MB used space
RAL-S2-101-197	Storage Node	✓	1.30 MB used space
RAL-S3-101-198	Storage Node	✓	1.34 MB used space

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space ?	Used Space ?	Site Capacity ?
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

[Previous](#)[Next](#)

Per il sito selezionato sono incluse le seguenti informazioni:

- Numero di nodi
- Lo spazio totale utilizzato, lo spazio libero e la capacità di tutti i nodi di archiviazione nel sito.
 - Per la dismissione di un sito connesso, il valore **Spazio utilizzato** rappresenta la quantità di dati oggetto che devono essere spostati in altri siti o eliminati con ILM.
 - Per la dismissione di un sito disconnesso, il valore **Spazio utilizzato** indica la quantità di dati dell'oggetto che diventerà inaccessibile quando si rimuove il sito.
- Nomi dei nodi, tipi e stati di connessione:
 -  (Collegato)
 -  (Amministrativamente inattivo)
 -  (Sconosciuto)
- Dettagli su ciascun nodo:
 - Per ogni nodo di archiviazione, la quantità di spazio utilizzata per i dati degli oggetti.

- Per i nodi amministrativi e i nodi gateway, se il nodo è attualmente utilizzato in un gruppo ad alta disponibilità (HA). Non è possibile disattivare un nodo amministrativo o un nodo gateway utilizzato in un gruppo HA. Prima di iniziare la dismissione, modificare i gruppi HA per rimuovere tutti i nodi nel sito oppure rimuovere il gruppo HA se include solo nodi da questo sito. Per le istruzioni, vedere ["Gestire gruppi ad alta disponibilità \(HA\)"](#).

3. Nella sezione Dettagli per altri siti della pagina, valuta quanto spazio è disponibile negli altri siti nella tua griglia.

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB

Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space ?	Used Space ?	Site Capacity ?
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Se si sta eseguendo la dismissione di un sito connesso e si prevede di utilizzare ILM per spostare i dati degli oggetti dal sito selezionato (anziché semplicemente eliminarli), è necessario assicurarsi che gli altri siti abbiano 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** per il sito che si desidera rimuovere è maggiore dello **Spazio libero totale per altri siti**. Per garantire che sia disponibile una capacità di archiviazione adeguata dopo la rimozione del sito, potrebbe essere necessario eseguire un'espansione prima di eseguire questa procedura.

4. Selezionare **Avanti**.

Viene visualizzato il passaggio 3 (Revisione della politica ILM).

Fase 3: rivedere le politiche ILM

Dal passaggio 3 (Revisione criteri ILM) della procedura guidata Dismissione sito, è possibile determinare se il sito è a cui fa riferimento un criterio ILM.

Prima di iniziare

Hai una buona comprensione di come ["gestire gli oggetti con ILM"](#). Hai familiarità con la creazione di pool di archiviazione e regole ILM e con la simulazione e l'attivazione di una policy ILM.

Informazioni su questo compito

StorageGRID non può dismettere un sito se una qualsiasi regola ILM in una policy (attiva o inattiva) fa riferimento a tale sito.

Se una qualsiasi policy ILM fa riferimento al sito che si desidera dismettere, è necessario rimuovere tali policy o modificarle in modo che soddisfino i seguenti requisiti:

- Proteggere completamente tutti i dati degli oggetti.

- Non fare riferimento al sito che stai dismettendo.
- Non utilizzare pool di archiviazione che fanno riferimento al sito né utilizzare l'opzione Tutti i siti.
- Non utilizzare profili di codifica di cancellazione che fanno riferimento al sito.
- Non utilizzare la regola Crea 2 copie di StorageGRID 11.6 o installazioni precedenti.



Non creare mai una regola ILM a copia singola per gestire la rimozione di un sito. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.



Se si sta eseguendo la *decommissionazione di un sito connesso*, è necessario considerare come StorageGRID deve gestire i dati degli oggetti attualmente presenti nel sito che si desidera rimuovere. A seconda dei requisiti di protezione dei dati, le nuove regole possono spostare i dati degli oggetti esistenti in siti diversi oppure eliminare eventuali copie extra degli oggetti che non sono più necessarie.

Contatta il supporto tecnico se hai bisogno di assistenza per progettare una nuova policy.

Passi

1. Dal passaggio 3 (Revisione delle policy ILM), determinare se alcune policy ILM fanno riferimento al sito selezionato per la dismissione.
2. Se non sono elencate policy, selezionare **Avanti** per andare a ["Passaggio 4: rimuovere i riferimenti ILM"](#).
3. Se sono elencati uno o più criteri ILM *attivi*, clonare ciascun criterio esistente o creare nuovi criteri che non facciano riferimento al sito che viene dismesso:
 - a. Selezionare il collegamento per la policy nella colonna Nome policy.

La pagina dei dettagli della policy ILM viene visualizzata in una nuova scheda del browser. La pagina Sito di dismissione rimarrà aperta nell'altra scheda.

- b. Seguire queste linee guida e istruzioni secondo necessità:

- Lavora con le regole ILM:
 - ["Creare uno o più pool di archiviazione"](#) che non fanno riferimento al sito.
 - ["Modifica o sostituisci le regole"](#) che si riferiscono al sito.



Non selezionare la regola **Crea 2 copie** perché tale regola utilizza il pool di archiviazione **Tutti i nodi di archiviazione**, che non è consentito.

- Lavorare con le politiche ILM:
 - ["Clona una policy ILM esistente"](#) o ["creare una nuova politica ILM"](#).
 - Assicurarsi che la regola predefinita e le altre regole non facciano riferimento al sito.



È necessario confermare che le regole ILM siano nell'ordine corretto. Quando la policy viene attivata, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'alto.

c. Inserire oggetti di prova e simulare la policy per garantire che vengano applicate le regole corrette.



Gli errori in una policy 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 una nuova policy ILM, StorageGRID la utilizza per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Prima di attivare una nuova policy ILM, rivedere tutte le modifiche apportate al posizionamento degli oggetti replicati e con codice di cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

d. Attivare le nuove policy e assicurarsi che le vecchie policy siano ora inattive.

Se vuoi attivare più policy, ["segui i passaggi per creare tag di policy ILM"](#) .

Se si esegue la dismissione di un sito connesso, StorageGRID inizia a rimuovere i dati degli oggetti dal sito selezionato non appena si attiva il nuovo criterio ILM. Lo spostamento o l'eliminazione di tutte le copie degli oggetti potrebbero richiedere settimane. Sebbene sia possibile avviare in sicurezza la dismissione di un sito mentre i dati degli oggetti sono ancora presenti nel sito, la procedura di dismissione verrà completata più rapidamente e con meno interruzioni e impatti sulle prestazioni se si consente lo spostamento dei dati dal sito prima di avviare la procedura di dismissione effettiva (selezionando **Avvia dismissione** nel passaggio 5 della procedura guidata).

4. Per ogni policy *inattiva*, modificarla o rimuoverla selezionando prima il collegamento per ogni policy come descritto nei passaggi precedenti.
 - ["Modifica la politica"](#) quindi non si riferisce al sito da dismettere.
 - ["Rimuovere una policy"](#) .
5. Una volta completate le modifiche alle regole e alle policy ILM, non dovrebbero esserci più policy elencate nel passaggio 3 (Revisione delle policy ILM). Selezionare **Avanti**.

Viene visualizzato il passaggio 4 (Rimuovi riferimenti ILM).

Passaggio 4: rimuovere i riferimenti ILM

Dal passaggio 4 (Rimuovi riferimenti ILM) della procedura guidata Dismissione sito, è necessario eliminare o modificare tutte le regole ILM non utilizzate che fanno riferimento al sito, anche se le regole non sono utilizzate in alcun criterio ILM.

Passi

1. Determinare se le regole ILM non utilizzate fanno riferimento al sito.

Se sono elencate delle regole ILM, tali regole fanno comunque riferimento al sito, ma non vengono utilizzate in alcuna policy.



Quando StorageGRID dismette il sito, disattiverà automaticamente tutti i profili di codifica di cancellazione inutilizzati che fanno riferimento al sito ed eliminerà automaticamente tutti i pool di archiviazione inutilizzati che fanno riferimento al sito. Il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) è stato rimosso perché utilizza il sito All Sites.

2. Modifica o elimina ogni regola non utilizzata:

- Per modificare una regola, vai alla pagina delle regole ILM e aggiorna tutti i posizionamenti che utilizzano un profilo di codifica di cancellazione o un pool di archiviazione che fa riferimento al sito. Quindi, tornare al **Passaggio 4 (Rimuovere i riferimenti ILM)**.
- Per eliminare una regola, seleziona l'icona del cestino  e seleziona **OK**.



È necessario eliminare la regola **Crea 2 copie** prima di poter dismettere un sito.

3. Verificare che nessuna regola ILM inutilizzata faccia riferimento al sito e che il pulsante **Avanti** sia abilitato.

4. Selezionare **Avanti**.



Tutti i pool di archiviazione rimanenti e i profili di codifica di cancellazione che fanno riferimento al sito diventeranno non validi quando il sito verrà rimosso. Quando StorageGRID dismette il sito, disattiverà automaticamente tutti i profili di codifica di cancellazione inutilizzati che fanno riferimento al sito ed eliminerà automaticamente tutti i pool di archiviazione inutilizzati che fanno riferimento al sito. Il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) è stato rimosso perché utilizza il sito All Sites.

Viene visualizzato il passaggio 5 (Risolvi conflitti tra nodi).

Passaggio 5: risolvere i conflitti tra nodi (e avviare la dismissione)

Dal passaggio 5 (Risoluzione conflitti tra nodi) della procedura guidata Dismissione sito, è possibile determinare se qualche nodo nel sistema StorageGRID è disconnesso o se qualche nodo nel sito selezionato appartiene a un gruppo ad alta disponibilità (HA). Dopo aver risolto eventuali conflitti tra nodi, è possibile avviare la procedura di dismissione da questa pagina.

Prima di iniziare

È necessario assicurarsi che tutti i nodi del sistema StorageGRID siano nello stato corretto, come segue:

- Tutti i nodi nel sistema StorageGRID devono essere connessi ().



Se si esegue la dismissione di un 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 dismissione non verrà avviata se uno o più volumi sono offline (smontati) o se sono online (montati) ma in stato di errore.



Se uno o più volumi vanno offline mentre è in corso una dismissione, il processo di dismissione viene completato dopo che i volumi tornano online.

- Nessun nodo nel sito che stai rimuovendo può avere un'interfaccia che appartiene a un gruppo ad alta disponibilità (HA).

Informazioni su questo compito

Se un nodo è elencato per il passaggio 5 (Risoluzione dei conflitti tra nodi), è necessario correggere il problema prima di poter avviare la dismissione.

Prima di avviare la procedura di dismissione del sito da questa pagina, esaminare le seguenti considerazioni:

- È necessario prevedere un tempo adeguato per il completamento della procedura di disattivazione.



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 presenti nel sito, del carico sul sistema, delle latenze di rete e della natura delle modifiche ILM richieste.

- Mentre è in corso la procedura di dismissione del sito:
 - Non è possibile creare regole ILM che facciano riferimento al sito in fase di dismissione. Non è inoltre possibile modificare una regola ILM esistente per fare riferimento al sito.
 - Non è possibile eseguire altre procedure di manutenzione, come l'espansione o l'aggiornamento.



Se è necessario eseguire un'altra procedura di manutenzione durante la dismissione di un sito connesso, è possibile sospendere la procedura mentre vengono rimossi i nodi di archiviazione. Il pulsante **Pausa** è abilitato durante la fase di "Dismissione dei dati replicati e codificati per la cancellazione".

- Se è necessario ripristinare un nodo dopo aver avviato la procedura di dismissione del sito, è necessario contattare l'assistenza.

Passi

1. Esaminare la sezione sui nodi disconnessi del passaggio 5 (Risoluzione dei conflitti tra nodi) per determinare se uno qualsiasi dei nodi nel sistema StorageGRID ha uno stato di connessione sconosciuto

() o Amministrativamente inattivo () .

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

1 disconnected node in the grid

The following nodes have a Connection State of Unknown (blue) or Administratively Down (gray). You must bring these disconnected nodes back online.

For help bringing nodes back online, see the instructions for [monitoring and troubleshooting StorageGRID](#) and the [recovery and maintenance](#) instructions.

Node Name	Connection State	Site	Type
DC1-S3-99-193	Administratively Down	Data Center 1	Storage Node

1 node in the selected site belongs to an HA group

Passphrase

Provisioning Passphrase

Previous

Start Decommission

2. Se qualche nodo è disconnesso, riattivalo.

Vedi il "[Procedure del nodo](#)". Se hai bisogno di assistenza, contatta il supporto tecnico.

3. Una volta ripristinati tutti i nodi disconnessi, rivedere la sezione Gruppi HA del Passaggio 5 (Risoluzione dei conflitti tra nodi).

Questa tabella elenca tutti i nodi nel sito selezionato che appartengono a un gruppo ad alta disponibilità (HA).

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue:

All grid nodes are connected

1 node in the selected site belongs to an HA group 

The following nodes in the selected site belong to a high availability (HA) group. You must either edit the HA group to remove the node's interface or remove the entire HA group.

[Go to HA Groups page.](#) 

For information about HA groups, see the instructions for [administering StorageGRID](#)

HA Group Name	Node Name	Node Type
HA group	DC1-GW1-99-190	API Gateway Node

Passphrase

Provisioning Passphrase 

Previous

Start Decommission

4. Se sono elencati dei nodi, procedere in uno dei seguenti modi:

- Modificare ciascun gruppo HA interessato per rimuovere l'interfaccia del nodo.
- Rimuovi un gruppo HA che include solo nodi da questo sito. Consultare le istruzioni per l'amministrazione StorageGRID.

Se tutti i nodi sono connessi e nessun nodo nel sito selezionato viene utilizzato in un gruppo HA, il campo **Passphrase di provisioning** è abilitato.

5. Immettere la passphrase di provisioning.

Il pulsante **Avvia disattivazione** diventa attivo.

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be offline.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

All grid nodes are connected

No nodes in the selected site belong to an HA group

Passphrase

Provisioning Passphrase ?

.....|

Previous

Start Decommission

6. Se sei pronto ad avviare la procedura di dismissione del sito, seleziona **Avvia dismissione**.

Un avviso elenca il sito e i nodi che verranno rimossi. Ti ricordiamo che potrebbero volerci giorni, settimane o addirittura mesi per rimuovere completamente il sito.

Warning

The following site and its nodes have been selected for decommissioning and will be permanently removed from the StorageGRID system:

Data Center 3

- DC3-S1
- DC3-S2
- DC3-S3

When StorageGRID removes a site, it temporarily uses strong-site consistency to prevent object metadata from being written to the site being removed. Client write and delete operations can fail if multiple nodes become unavailable at the remaining sites.

This procedure might take days, weeks, or even months to complete. Select **Maintenance > Decommission** to monitor the decommission progress.

Do you want to continue?

Cancel

OK

7. Rivedi l'avviso. Se sei pronto per iniziare, seleziona **OK**.

Viene visualizzato un messaggio durante la generazione della nuova configurazione della griglia. Questo processo potrebbe richiedere del tempo, a seconda del tipo e del numero di nodi della rete dismessi.

Passphrase

Provisioning Passphrase 

 Generating grid configuration. This may take some time depending on the type and the number of decommissioned grid nodes.

Previous

Start Decommission 

Una volta generata la nuova configurazione della griglia, viene visualizzato il passaggio 6 (Monitoraggio disattivazione).



Il pulsante **Precedente** rimane disattivato finché la disattivazione non è completa.

Fase 6: Monitoraggio della dismissione

Dal passaggio 6 (Monitoraggio dismissione) della procedura guidata della pagina Dismissione sito, è possibile monitorare l'avanzamento della rimozione del sito.

Informazioni su questo compito

Quando StorageGRID rimuove un sito connesso, rimuove i nodi in questo ordine:

1. Nodi gateway
2. Nodi amministrativi
3. Nodi di archiviazione

Quando StorageGRID rimuove un sito disconnesso, rimuove i nodi in questo ordine:

1. Nodi gateway
2. Nodi di archiviazione
3. Nodi amministrativi

La rimozione di ciascun nodo gateway o nodo amministrativo potrebbe richiedere solo pochi minuti o un'ora; la rimozione dei nodi di archiviazione, invece, potrebbe richiedere giorni o settimane.

Passi

1. Non appena viene generato un nuovo pacchetto di ripristino, scaricare il file.

Decommission Site



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



Scarica il pacchetto di ripristino il prima possibile per assicurarti di poter ripristinare la tua rete se qualcosa va storto durante la procedura di dismissione.

- a. Selezionare il collegamento nel messaggio oppure selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino**.
- b. Scarica il .zip file.

Vedi le istruzioni per "[scaricando il pacchetto di ripristino](#)".

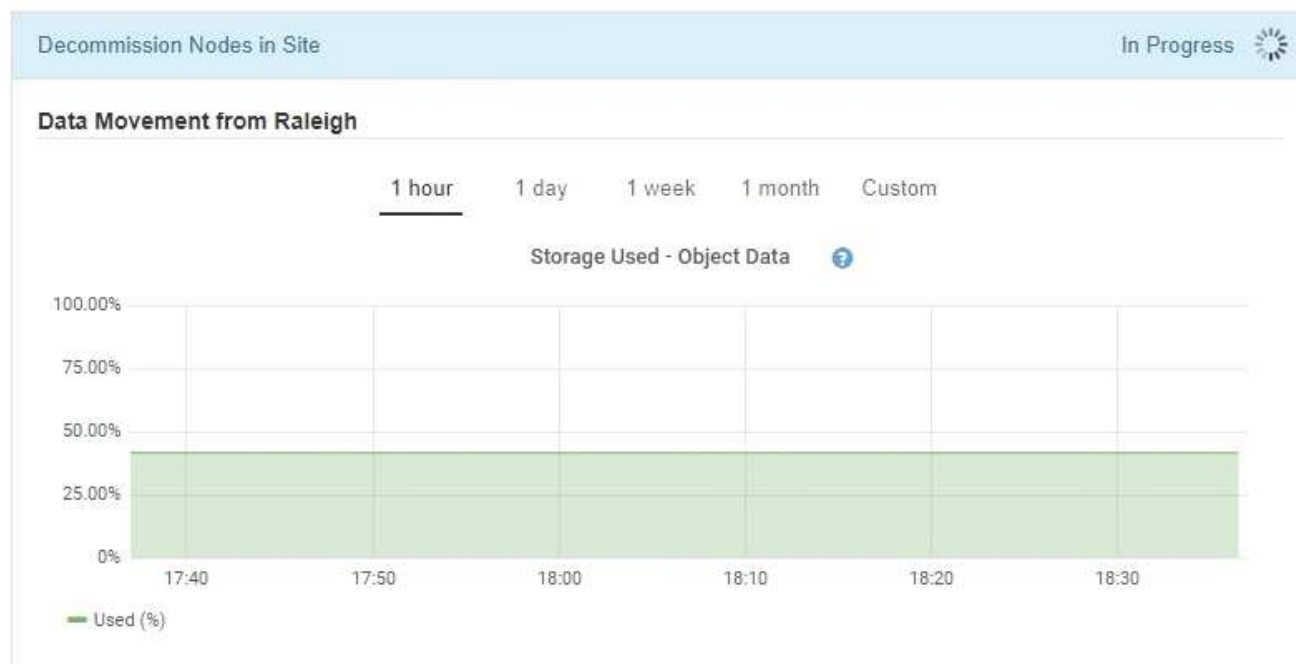


Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

2. Utilizzando il grafico Movimento dati, monitora lo spostamento dei dati degli oggetti da questo sito ad altri siti.

Lo spostamento dei dati è iniziato quando hai attivato la nuova policy ILM nel passaggio 3 (Revisione della policy ILM). Lo spostamento dei dati avverrà durante tutta la procedura di disattivazione.

Decommission Site Progress



3. Nella sezione Avanzamento nodi della pagina, è possibile monitorare l'avanzamento della procedura di dismissione man mano che i nodi vengono rimossi.

Quando un nodo di archiviazione viene rimosso, ogni nodo attraversa una serie di fasi. Sebbene la maggior parte di queste fasi avvenga rapidamente o addirittura in modo impercettibile, potrebbe essere necessario attendere giorni o addirittura settimane per il completamento di altre fasi, a seconda della quantità di dati da spostare. È necessario ulteriore tempo per gestire i dati codificati in modo da essere cancellati e rivalutare l'ILM.

Node Progress

 Depending on the number of objects stored, Storage Nodes might take significantly longer to decommission. Extra time is needed to manage erasure coded data and re-evaluate ILM.

The progress for each node is displayed while the decommission procedure is running. If you need to perform another maintenance procedure, select **Pause** to suspend the decommission (only allowed during certain stages).

Pause

Resume

Search 				
Name 	Type 	Progress 	Stage 	
RAL-S1-101-196	Storage Node		Decommissioning Replicated and Erasure Coded Data	
RAL-S2-101-197	Storage Node		Decommissioning Replicated and Erasure Coded Data	
RAL-S3-101-198	Storage Node		Decommissioning Replicated and Erasure Coded Data	

Se si sta monitorando l'avanzamento della dismissione di un sito connesso, fare riferimento a questa tabella per comprendere le fasi di dismissione di un nodo di archiviazione:

Palcoscenico	Durata stimata
In attesa di	Minuto o meno
Aspetta i blocchi	Minuti
Preparare l'attività	Minuto o meno
Marcatura LDR dismesso	Minuti
Dismissione dei dati replicati e codificati per cancellazione	Ore, giorni o settimane in base alla quantità di dati Nota: se è necessario eseguire altre attività di manutenzione, è possibile sospendere la dismissione del sito durante questa fase.
Stato del set LDR	Minuti
Svuota le code di controllo	Da minuti a ore, in base al numero di messaggi e alla latenza della rete.
Completare	Minuti

Se si sta monitorando l'avanzamento della dismissione di un sito disconnesso, fare riferimento a questa tabella per comprendere le fasi di dismissione di un nodo di archiviazione:

Palcoscenico	Durata stimata
In attesa di	Minuto o meno
Aspetta i blocchi	Minuti
Preparare l'attività	Minuto o meno
Disabilita i servizi esterni	Minuti
Revoca del certificato	Minuti
Annulla registrazione nodo	Minuti
Grado di archiviazione Annulla registrazione	Minuti
Rimozione del gruppo di archiviazione	Minuti
Rimozione dell'entità	Minuti

Palcoscenico	Durata stimata
Completare	Minuti

4. Dopo che tutti i nodi hanno raggiunto la fase Completata, attendere il completamento delle operazioni di dismissione del sito rimanente.
 - Durante la fase **Ripara Cassandra**, StorageGRID esegue tutte le riparazioni necessarie sui cluster Cassandra rimasti nella griglia. Queste riparazioni potrebbero richiedere diversi giorni o più, a seconda di quanti nodi di archiviazione rimangono nella griglia.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	In Progress 
StorageGRID is repairing the remaining Cassandra clusters after removing the site. This might take several days or more, depending on how many Storage Nodes remain in your grid.	
Overall Progress	0%
Deactivate EC Profiles & Delete Storage Pools	Pending
Remove Configurations	Pending

- Durante la fase **Disattiva profili EC ed elimina pool di archiviazione**, vengono apportate le seguenti modifiche ILM:
 - Tutti i profili di codifica di cancellazione che facevano riferimento al sito vengono disattivati.
 - Tutti i pool di archiviazione che facevano riferimento al sito vengono eliminati.



Anche il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) è stato rimosso perché utilizza il sito All Sites.

- Infine, durante la fase **Rimuovi configurazione**, tutti i riferimenti rimanenti al sito e ai suoi nodi vengono rimossi dal resto della griglia.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	Completed
Deactivate EC Profiles & Delete Storage Pools	Completed
Remove Configurations	In Progress 
StorageGRID is removing the site and node configurations from the rest of the grid.	

5. Una volta completata la procedura di dismissione, la pagina Decommission Site mostra un messaggio di successo e il sito rimosso non viene più visualizzato.

Decommission Site



The previous decommission procedure completed successfully at 2021-01-12 14:28:32 MST.

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

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

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

Sites

	Site Name	Used Storage Capacity ?	Decommission Possible
☒	Sunnyvale	4.79 MB	✓
☐	Vancouver	4.90 MB	No. This site contains the primary Admin Node.

Next

Dopo aver finito

Completare le seguenti attività dopo aver completato la procedura di dismissione del sito:

- Assicurarsi che le unità di tutti i nodi di archiviazione nel sito dismesso siano state cancellate. Utilizzare uno strumento o un servizio di cancellazione dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dalle unità.
- Se il sito include uno o più nodi amministrativi e l'accesso Single Sign-On (SSO) è abilitato per il sistema StorageGRID, rimuovere tutti i trust delle parti affidabili per il sito da Active Directory Federation Services (AD FS).
- Dopo che i nodi sono stati spenti automaticamente come parte della procedura di disattivazione del sito connesso, rimuovere le macchine virtuali associate.

Rinomina griglia, sito o nodo

Utilizzare la procedura di rinomina

Se necessario, è possibile modificare i nomi visualizzati in Grid Manager per l'intera griglia, per ciascun sito e per ciascun nodo. Puoi aggiornare i nomi visualizzati in modo sicuro e ogni volta che ne hai bisogno.

Qual è la procedura di rinomina?

Quando si installa inizialmente StorageGRID , si specifica un nome per la griglia, per ciascun sito e per ciascun nodo. Questi nomi iniziali sono noti come *nomi di sistema* e sono i nomi inizialmente visualizzati in StorageGRID.

I nomi di sistema sono necessari per le operazioni interne StorageGRID e non possono essere modificati. Tuttavia, è possibile utilizzare la procedura di ridenominazione per definire nuovi *nomi visualizzati* per la griglia, ciascun sito e ciascun nodo. Questi nomi visualizzati compaiono in varie posizioni StorageGRID al posto dei nomi di sistema sottostanti (o in alcuni casi, in aggiunta a essi).

Utilizzare la procedura di ridenominazione per correggere errori di battitura, per implementare una convenzione di denominazione diversa o per indicare che un sito e tutti i suoi nodi sono stati riposizionati. A differenza dei nomi di sistema, i nomi visualizzati possono essere aggiornati ogni volta che è necessario e senza influire sulle operazioni StorageGRID .

Dove compaiono i nomi di sistema e quelli visualizzati?

La tabella seguente riassume dove vengono mostrati i nomi di sistema e i nomi visualizzati nell'interfaccia utente StorageGRID e nei file StorageGRID .

Posizione	Nome del sistema	Nome da visualizzare
Pagine del gestore della griglia	Visualizzato a meno che l'elemento non venga rinominato	Se un elemento viene rinominato, viene visualizzato al posto del nome del sistema in queste posizioni: • Pannello di controllo • Pagina dei nodi • Pagine di configurazione per gruppi ad alta disponibilità, endpoint di bilanciamento del carico, interfacce VLAN, server di gestione delle chiavi, password di griglia e controllo del firewall • Avvisi • Definizioni del pool di archiviazione • Pagina di ricerca dei metadati degli oggetti • Pagine relative alle procedure di manutenzione, tra cui aggiornamento, hotfix, aggiornamento del sistema operativo SANtricity , dismissione, espansione, ripristino e controllo dell'esistenza degli oggetti • Pagine di supporto (registri e diagnostica) • Pagina Single Sign-On, accanto al nome host del nodo di amministrazione nella tabella per i dettagli del nodo di amministrazione

Posizione	Nome del sistema	Nome da visualizzare
NODI > Scheda Panoramica per un nodo	Sempre mostrato	Visualizzato solo se l'elemento è stato rinominato
Pagine legacy in Grid Manager (ad esempio, SUPPORTO > Topologia griglia)	Mostrato	Non mostrato
API node-health	Sempre tornato	Restituito solo se l'elemento viene rinominato
Richiedi 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` file nel pacchetto di ripristino	Mostrato come Server Name	Mostrato come Display Name
`/etc/hosts` file su tutti i nodi Per 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, mostrato 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, associa gli ID di griglia, sito e nodo ai rispettivi nomi visualizzati.

Requisiti del nome visualizzato

Prima di utilizzare questa procedura, rivedere i requisiti per i nomi visualizzati.

Nomi visualizzati per i nodi

I nomi visualizzati per i nodi devono seguire queste regole:

- Deve essere univoco in tutto il sistema StorageGRID .
- Non può essere uguale al nome di sistema di nessun 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 numeri.
- Non fanno distinzione tra maiuscole e minuscole. Per esempio, DC1-ADM E dc1-adm sono considerati duplicati.

È possibile rinominare un nodo con un nome visualizzato precedentemente utilizzato da un nodo diverso, purché la ridenominazione non determini un nome visualizzato o un nome di sistema duplicato.

Nomi visualizzati per griglia e siti

I nomi visualizzati per la griglia e i siti seguono le stesse regole, con queste eccezioni:

- Può includere spazi.
- Può includere questi caratteri speciali: = - _ : , . @ !
- Può iniziare e terminare con caratteri speciali, inclusi i trattini.
- Possono essere solo numeri o caratteri speciali.

Buone pratiche per il nome visualizzato

Se si prevede di rinominare più elementi, documentare lo schema di denominazione generale prima di utilizzare questa procedura. Elabora un sistema che garantisca che i nomi siano unici, coerenti e facili da capire a colpo d'occhio.

Puoi utilizzare qualsiasi convenzione di denominazione che si adatti alle esigenze della tua organizzazione. Ecco alcuni suggerimenti di base su cosa includere:

- **Indicatore sito:** se hai più siti, aggiungi un codice sito a ciascun nome di nodo.
- **Tipo di nodo:** i nomi dei nodi in genere indicano il tipo di nodo. Puoi usare abbreviazioni come s , adm , E gw (Nodo di archiviazione, nodo di amministrazione e nodo gateway).
- **Numero nodo:** se un sito contiene più di un nodo di un particolare tipo, aggiungere un numero univoco al nome di ciascun nodo.

Pensateci 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 questi indirizzi possono essere modificati. Allo stesso modo, le posizioni dei rack o i numeri dei modelli degli elettrodomestici possono cambiare se si sposta l'apparecchiatura o si aggiorna l'hardware.

Esempi di nomi visualizzati

Supponiamo che il tuo sistema StorageGRID abbia tre data center e nodi di tipo diverso in ogni 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 visualizzati utilizzati per la griglia, i siti e i nodi. È possibile rinominare un singolo elemento, più elementi o persino tutti gli elementi contemporaneamente. La definizione o l'aggiornamento di un nome visualizzato non influisce in alcun modo sulle operazioni StorageGRID .

Prima di iniziare

- Dal **nodo di amministrazione primario**, hai effettuato l'accesso al 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 aver effettuato l'accesso al nodo di amministrazione primario per scaricare un pacchetto di ripristino.

- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#) .
- Hai la passphrase di provisioning.
- Comprendi i requisiti e le best practice per i nomi visualizzati. Vedere ["Rinomina griglia, siti e nodi"](#) .

Come rinominare la griglia, i siti o i nodi

È possibile rinominare il sistema StorageGRID , uno o più siti oppure uno o più nodi.

È possibile utilizzare un nome visualizzato precedentemente utilizzato da un nodo diverso, purché la

ridenominazione non determini un nome visualizzato o un nome di sistema duplicato.

Seleziona gli elementi da rinominare

Per iniziare, seleziona gli elementi che vuoi rinominare.

Passi

1. Selezionare **MANUTENZIONE > Attività > Rinomina griglia, siti e nodi**.
2. Per il passaggio **Seleziona nomi**, seleziona gli elementi che desideri rinominare.

Elemento da modificare	Istruzioni
Nomi di tutto (o quasi tutto) nel tuo sistema	a. Seleziona Seleziona tutto. b. Facoltativamente, deseleziona tutti gli elementi che non vuoi rinominare.
Nome della griglia	Selezionare la casella di controllo per la griglia.
Nome di un sito e di alcuni o tutti i suoi nodi	a. Selezionare la casella di controllo nell'intestazione della tabella per il sito. b. Facoltativamente, cancella tutti i nodi che non vuoi rinominare.
Nome di un sito	Seleziona la casella di controllo per il sito.
Nome di un nodo	Selezionare la casella di controllo per il nodo.

3. Selezionare **Continua**.
4. Esamina 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 suo nome visualizzato è uguale al nome di sistema.
 - Nella colonna **Nome sistema** viene visualizzato il nome immesso per ciascun elemento durante l'installazione. I nomi di sistema vengono utilizzati per le operazioni interne StorageGRID e non possono essere modificati. Ad esempio, il nome di sistema di un nodo potrebbe essere il suo nome host.
 - La colonna **Tipo** indica il tipo di elemento: Griglia, Sito o il tipo specifico di nodo.

Proponi nuovi nomi

Per la fase **Proponi nuovi nomi**, puoi immettere un nome visualizzato per ogni elemento singolarmente oppure puoi rinominare gli elementi in blocco.

Rinomina gli elementi singolarmente

Seguire questi passaggi per immettere un nome visualizzato per ogni elemento che si desidera rinominare.

Passi

1. Nel campo **Nome visualizzato**, immettere un nome visualizzato proposto per ogni elemento nell'elenco.

Vedere "[Rinomina griglia, siti e nodi](#)" per apprendere i requisiti di denominazione.

2. Per rimuovere gli elementi che non vuoi rinominare, seleziona  nella colonna **Rimuovi dall'elenco**.

Se non intendi proporre un nuovo nome per un elemento, devi rimuoverlo dalla tabella.

3. Dopo aver proposto nuovi nomi per tutti gli elementi nella tabella, selezionare **Rinomina**.

Viene visualizzato un messaggio di successo. I nuovi nomi visualizzati vengono ora utilizzati in tutto Grid Manager.

Rinomina gli elementi in blocco

Utilizzare lo strumento di rinomina in blocco se i nomi degli elementi condividono una stringa comune che si desidera sostituire con una stringa diversa.

Passi

1. Per il passaggio **Proponi nuovi nomi**, seleziona **Usa strumento di rinomina in blocco**.

L'anteprima **Rinomina** include tutti gli elementi mostrati nel passaggio **Proponi nuovi nomi**. È possibile utilizzare l'anteprima per vedere come appariranno i nomi visualizzati dopo aver sostituito una stringa condivisa.

2. Nel campo **Stringa esistente**, immettere la stringa condivisa che si desidera sostituire. Ad esempio, se la stringa che vuoi sostituire è `Data-Center-1`, immettere **Data-Center-1**.

Mentre digiti, il testo viene evidenziato ovunque si trovi tra i nomi a sinistra.

3. Selezionare  per rimuovere tutti gli elementi che non vuoi rinominare con questo strumento.

Ad esempio, supponiamo di voler rinominare tutti i nodi che contengono la stringa `Data-Center-1`, ma non vuoi rinominare il `Data-Center-1` sito stesso. Selezionare  per rimuovere il sito dall'anteprima di ridenominazione.

Bulk rename tool

Rename preview ?

Data-Center-1

X

Data-Center-1-ADM1

X

Data-Center-1-ARC1

X

Data-Center-1-G1

X

Data-Center-1-S1

X

Data-Center-1-S2

X

Data-Center-1-S3

X

Data-Center-1-S4

▼

Cancel

Add names

Enter the shared string you want to replace. Then, enter a new string to use instead. Optionally, remove any items that you do not want to rename with this tool.

Existing string

Data-Center-1

The string you want to replace. Represented by *italicized text* in the preview section.

New string

The string you want to use instead. Represented by **bolded text** in the preview section.

4. Nel campo **Nuova stringa**, inserisci la stringa sostitutiva che desideri utilizzare. Ad esempio, immettere **DC1**.

Vedere "[Rinomina griglia, siti e nodi](#)" per apprendere i requisiti di denominazione.

Man mano che si immette la stringa sostitutiva, i nomi sulla sinistra vengono aggiornati, così è possibile verificare che i nuovi nomi siano corretti.

1439

Bulk rename tool

×

Rename preview ?

DC1-ADM1

×

DC1-ARC1

×

DC1-G1

×

DC1-S1

×

DC1-S2

×

DC1-S3

×

DC1-S4

×

Cancel

Add names

Enter the shared string you want to replace. Then, enter a new string to use instead. Optionally, remove any items that you do not want to rename with this tool.

Existing string

Data-Center-1

The string you want to replace. Represented by *italicized text* in the preview section.

New string

DC1

The string you want to use instead. Represented by **bolded text** in the preview section.

- Quando sei soddisfatto dei nomi mostrati nell'anteprima, seleziona **Aggiungi nomi** per aggiungere i nomi alla tabella per il passaggio **Proponi nuovi nomi**.
- Apportare eventuali modifiche aggiuntive richieste oppure selezionare **×** per rimuovere tutti gli elementi che non vuoi rinominare.
- Quando sei pronto a rinominare tutti gli elementi nella tabella, seleziona **Rinomina**.

Viene visualizzato un messaggio di conferma dell'operazione. I nuovi nomi visualizzati vengono ora utilizzati in tutto Grid Manager.

Scarica il pacchetto di ripristino

Una volta terminata la ridenominazione degli elementi, scarica e salva un nuovo pacchetto di ripristino. I nuovi nomi visualizzati per gli elementi rinominati sono inclusi nel `Passwords.txt` file.

Passi

- Immettere la passphrase di provisioning.
- Seleziona **Scarica pacchetto di ripristino**.

Il download inizia immediatamente.

- Una volta completato il download, apri il `Passwords.txt` file per visualizzare il nome del server per tutti i nodi e i nomi visualizzati per tutti i nodi rinominati.
- Copia il `sgws-recovery-package-id-revision.zip` archiviare il file in due posizioni sicure, protette 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.

Ripristina 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 rinominati. 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.

Passi

1. Selezionare **MANUTENZIONE > Attività > Rinomina griglia, siti e nodi**.
2. Per il passaggio **Seleziona nomi**, seleziona tutti gli elementi per i quali desideri ripristinare i nomi di sistema.
3. Selezionare **Continua**.
4. Per il passaggio **Proponi nuovi nomi**, ripristina i nomi visualizzati come nomi di sistema, singolarmente o in blocco.

Ripristinare i nomi di sistema singolarmente

- a. Copia il nome di sistema originale di ciascun elemento e incollalo nel campo **Nome visualizzato** oppure seleziona  per rimuovere tutti gli elementi che non vuoi ripristinare.

Per ripristinare un nome visualizzato, il nome del sistema deve apparire 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.

Ripristina i nomi di sistema in blocco

- a. Per il passaggio **Proponi nuovi nomi**, seleziona **Usa strumento di rinomina in blocco**.
- b. Nel campo **Stringa esistente**, immettere la stringa del nome visualizzato che si desidera sostituire.
- c. Nel campo **Nuova stringa**, immettere la stringa del nome del sistema che si desidera utilizzare.
- d. Selezionare **Aggiungi nomi** per aggiungere i nomi alla tabella per il passaggio **Proponi nuovi nomi**.
- e. Verificare che ogni voce nel campo **Nome visualizzato** corrisponda al nome nel campo **Nome del sistema**. Apportare eventuali modifiche o selezionare  per rimuovere tutti gli elementi che non vuoi ripristinare.

Per ripristinare un nome visualizzato, il nome del sistema deve apparire nel campo **Nome visualizzato**, ma il nome non fa distinzione tra maiuscole e minuscole.

- f. Selezionare **Rinomina**.

Viene visualizzato un messaggio di conferma dell'operazione. I nomi visualizzati per questi elementi non vengono più utilizzati.

5. Scarica e salva un nuovo pacchetto di ripristino .

I nomi visualizzati per gli elementi ripristinati non sono più inclusi nel `Passwords.txt` file.

Procedure del nodo

Procedure di manutenzione dei nodi

Potrebbe essere necessario eseguire procedure di manutenzione relative a specifici nodi della griglia o servizi dei nodi.

Procedure del Server Manager

Server Manager viene eseguito su ogni nodo della griglia 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 anche i servizi su ogni nodo della griglia e tenterà automaticamente di riavviare tutti i servizi che segnalano errori.

Per eseguire le procedure di Server Manager, in genere è necessario accedere alla riga di comando del nodo.



Dovresti accedere a Server Manager solo se il supporto tecnico ti ha indicato di farlo.



Dopo aver terminato di utilizzare Server Manager, è necessario chiudere la sessione corrente della shell dei comandi e disconnettersi. Inserisci: `exit`

Procedure di riavvio, spegnimento e alimentazione del nodo

È possibile utilizzare queste procedure per riavviare uno o più nodi, per arrestare e riavviare i nodi oppure per spegnere e riaccendere i nodi.

Procedure di rimappatura delle porte

È possibile utilizzare le procedure di rimappatura delle porte per rimuovere le rimappature delle porte da un nodo, ad esempio se si desidera configurare un endpoint del bilanciatore del carico utilizzando una porta che era stata precedentemente rimappata.

Procedure del Server Manager

Visualizza lo stato e la versione di Server Manager

Per ogni nodo della griglia è possibile visualizzare lo stato corrente e la versione di Server Manager in esecuzione su quel nodo della griglia. È anche possibile ottenere lo stato attuale di tutti i servizi in esecuzione su quel nodo della griglia.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Visualizza lo stato corrente di Server Manager in esecuzione sul nodo della griglia: **`service servermanager status`**

Viene segnalato lo stato corrente di Server Manager in esecuzione sul nodo della griglia (in esecuzione o meno). Se lo stato di Server Manager è `running`, viene indicato il tempo trascorso dall'ultimo avvio. Per esempio:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Visualizza la versione corrente di Server Manager in esecuzione su un nodo della griglia: **`service`**

servermanager version

È elencata la versione attuale. Per esempio:

```
11.1.0-20180425.1905.39c9493
```

4. Disconnettersi dalla shell dei comandi: **exit**

Visualizza lo stato attuale di tutti i servizi

È possibile visualizzare in qualsiasi momento lo stato attuale di tutti i servizi in esecuzione su un nodo della griglia.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Visualizza lo stato di tutti i servizi in esecuzione sul nodo della griglia: `storagegrid-status`

Ad esempio, l'output per il nodo di amministrazione primario mostra lo stato corrente dei servizi AMS, CMN e NMS come In esecuzione. Questo output viene aggiornato immediatamente se cambia lo stato di un servizio.

Host Name	190-ADM1	
IP Address		
Operating System Kernel	4.9.0	Verified
Operating System Environment	Debian 9.4	Verified
StorageGRID Webscale Release	11.1.0	Verified
Networking		Verified
Storage Subsystem		Verified
Database Engine	5.5.9999+default	Running
Network Monitoring	11.1.0	Running
Time Synchronization	1:4.2.8p10+dfsg	Running
ams	11.1.0	Running
cmn	11.1.0	Running
nms	11.1.0	Running
ssm	11.1.0	Running
mi	11.1.0	Running
dynip	11.1.0	Running
nginx	1.10.3	Running
tomcat	8.5.14	Running
grafana	4.2.0	Running
mgmt api	11.1.0	Running
prometheus	1.5.2+ds	Running
persistence	11.1.0	Running
ade exporter	11.1.0	Running
attrDownPurge	11.1.0	Running
attrDownSampl	11.1.0	Running
attrDownSamp2	11.1.0	Running
node exporter	0.13.0+ds	Running

3. Torna alla riga di comando e premi **Ctrl+C**.
4. Facoltativamente, visualizza un report statico per tutti i servizi in esecuzione sul nodo della griglia:
`/usr/local/servermanager/reader.rb`

Questo report include le stesse informazioni del report aggiornato continuamente, ma non viene aggiornato se cambia lo stato di un servizio.

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 della griglia.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Informazioni su questo compito

L'avvio di Server Manager su un nodo della griglia in cui è già in esecuzione determina il riavvio di Server Manager e di tutti i servizi sul nodo della griglia.

Passi

1. Accedi al nodo della griglia:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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 gestore del server e tutti i servizi in esecuzione su un nodo della griglia.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:

a. Immettere il seguente comando: `ssh admin@grid_node_IP`

b. Inserisci la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Riavviare Server Manager e tutti i servizi sul nodo della griglia: `service servermanager restart`

Server Manager e tutti i servizi sul nodo della griglia vengono arrestati e quindi riavviati.



Utilizzando il `restart` il comando è lo stesso dell'utilizzo del `stop` comando seguito dal `start` comando.

3. Disconnettersi dalla shell dei comandi: `exit`

Arresta Server Manager e tutti i servizi

Server Manager è progettato per essere sempre in esecuzione, ma potrebbe essere necessario arrestare Server Manager e tutti i servizi in esecuzione su un nodo della griglia.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:

a. Immettere il seguente comando: `ssh admin@grid_node_IP`

b. Inserisci la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Arrestare Server Manager e tutti i servizi in esecuzione sul nodo della griglia: `service servermanager stop`

Server Manager e tutti i servizi in esecuzione sul nodo della griglia vengono terminati correttamente. La chiusura dei servizi può richiedere fino a 15 minuti.

3. Disconnettersi dalla shell dei comandi: `exit`

Visualizza lo stato attuale del servizio

È possibile visualizzare in qualsiasi momento lo stato corrente di un servizio in esecuzione su un nodo della griglia.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:

a. Immettere il seguente comando: `ssh admin@grid_node_IP`

b. Inserisci la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Visualizza lo stato corrente di un servizio in esecuzione su un nodo della griglia: ``service servicename status`` Viene segnalato lo stato corrente del servizio richiesto in esecuzione sul nodo della griglia (in esecuzione o meno). Per esempio:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Disconnettersi dalla shell dei comandi: `exit`

Interrompere il servizio

Alcune procedure di manutenzione richiedono di interrompere un singolo servizio mantenendo in esecuzione gli altri servizi sul nodo della rete. Interrompere i singoli servizi solo quando richiesto da una procedura di manutenzione.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Informazioni su questo compito

Quando si utilizzano questi passaggi per "arrestare amministrativamente" un servizio, Server Manager non riavvierà automaticamente il servizio. È necessario avviare manualmente il singolo servizio oppure riavviare Server Manager.

Se è necessario arrestare il servizio LDR su un nodo di archiviazione, tenere presente che potrebbe essere necessario del tempo per arrestare il servizio se sono presenti connessioni attive.

Passi

1. Accedi al nodo della griglia:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Interrompere un singolo servizio: `service servicename stop`

Per esempio:

```
service ldr stop
```



L'interruzione del servizio può richiedere fino a 11 minuti.

3. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

["Forzare la terminazione del servizio"](#)

Forzare la terminazione del servizio

Se hai bisogno di interrompere immediatamente un servizio, puoi utilizzare `force-stop` comando.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da \$ A # .

2. Forzare manualmente la terminazione del servizio: `service servicename force-stop`

Per esempio:

```
service ldr force-stop
```

Il sistema attende 30 secondi prima di terminare il servizio.

3. Disconnettersi dalla shell dei comandi: `exit`

Avvia o riavvia il servizio

Potrebbe essere necessario avviare un servizio che è stato arrestato oppure potrebbe essere necessario arrestare e riavviare un servizio.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da \$ A # .

2. Decidere quale comando emettere, a seconda che il servizio sia attualmente in esecuzione o arrestato.
 - Se il servizio è attualmente interrotto, utilizzare il `start` comando per avviare manualmente il servizio:
`service servicename start`

Per esempio:

```
service ldr start
```

- Se il servizio è attualmente in esecuzione, utilizzare il `restart` comando per arrestare il servizio e poi riavviarlo: `service servicename restart`

Per esempio:

```
service ldr restart
```



Utilizzando il `restart` il comando è lo stesso dell'utilizzo del `stop` comando seguito dal `start` comando. Puoi emettere `restart` anche se il servizio è attualmente interrotto.

3. Disconnettersi dalla shell dei comandi: `exit`

Utilizzare un file DoNotStart

Se si eseguono varie procedure di manutenzione o configurazione sotto la supervisione 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.



Dovresti aggiungere o rimuovere un file DoNotStart solo se il supporto tecnico ti ha indicato di farlo.

Per impedire l'avvio di un servizio, inserire un file DoNotStart nella directory del servizio di cui si desidera impedire l'avvio. All'avvio, Server Manager cerca il file DoNotStart. Se il file è presente, il servizio (e tutti i servizi da esso dipendenti) non può essere avviato. Quando il file DoNotStart viene rimosso, il servizio precedentemente arrestato verrà 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 è 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.

Aggiungi il file DoNotStart per il servizio

È possibile impedire l'avvio di un singolo servizio aggiungendo un file DoNotStart alla directory di quel servizio su un nodo della griglia.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:

- a. Immettere il seguente comando: `ssh admin@grid_node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Aggiungere un file DoNotStart: `touch /etc/sv/service/DoNotStart`

Dove `service` è il nome del servizio di cui si desidera impedire l'avvio. Per esempio,

```
touch /etc/sv/ldr/DoNotStart
```

Viene creato un file `DoNotStart`. Non è necessario alcun contenuto del file.

Quando Server Manager o il nodo della griglia vengono riavviati, Server Manager si riavvia, ma il servizio no.

3. Disconnettersi dalla shell dei comandi: `exit`

Rimuovere il file `DoNotStart` per il servizio

Quando si rimuove un file `DoNotStart` che impedisce l'avvio di un servizio, è necessario avviare tale servizio.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Rimuovere il file `DoNotStart` dalla directory del servizio: `rm /etc/sv/service/DoNotStart`

Dove `service` è il nome del servizio. Per esempio,

```
rm /etc/sv/ldr/DoNotStart
```

3. Avvia il servizio: `service servicename start`
4. Disconnettersi dalla shell dei comandi: `exit`

Risoluzione dei problemi di Server Manager

Se si verifica un problema durante l'utilizzo di Server Manager, controllare il file di registro.

I messaggi di errore relativi a Server Manager vengono acquisiti nel file di registro di Server Manager, che si trova in: `/var/local/log/servermanager.log`

Controllare questo file per messaggi di errore relativi a guasti. Se necessario, segnalare il problema al supporto tecnico. Potrebbe esserti richiesto di inoltrare i file di registro al supporto tecnico.

Servizio con stato di errore

Se rilevi che un servizio è entrato in uno stato di errore, prova a riavviarlo.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Informazioni su questo compito

Server Manager monitora i servizi e riavvia quelli che si sono arrestati in modo imprevisto. Se un servizio non funziona, Server Manager tenta di riavviarlo. Se si verificano tre tentativi falliti di avvio di un servizio entro cinque minuti, il servizio entra in stato di errore. Server Manager non tenta un altro riavvio.

Passi

1. Accedi al nodo della griglia:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Conferma lo stato di errore del servizio: `service servicename status`

Per esempio:

```
service ldr status
```

Se il servizio è in stato di errore, viene restituito il seguente messaggio: `servicename in error state`. Per esempio:

```
ldr in error state
```



Se lo stato del servizio è `disabled`, vedere le istruzioni per ["rimozione di un file DoNotStart per un servizio"](#).

3. Prova a rimuovere lo stato di errore riavviando il servizio: `service servicename restart`

Se il servizio non si riavvia, contattare l'assistenza tecnica.

4. Disconnettersi dalla shell dei comandi: `exit`

Procedure di riavvio, spegnimento e accensione

Eseguire un riavvio progressivo

È possibile eseguire un riavvio progressivo per riavviare più nodi della griglia senza causare un'interruzione del servizio.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager sul nodo di amministrazione primario e stai utilizzando un ["browser web supportato"](#).



Per eseguire questa procedura è necessario aver effettuato l'accesso al nodo di amministrazione principale.

- Tu hai il "[Autorizzazione di accesso alla manutenzione o alla root](#)".

Informazioni su questo compito

Utilizzare questa procedura se è necessario riavviare più nodi contemporaneamente. Ad esempio, è possibile utilizzare questa procedura dopo aver modificato la modalità FIPS per la griglia "[Politica di sicurezza TLS e SSH](#)". Quando si modifica la modalità FIPS, è necessario riavviare tutti i nodi per rendere effettiva la modifica.



Se hai bisogno di riavviare solo un nodo, puoi "[riavviare il nodo dalla scheda Attività](#)".

Quando StorageGRID riavvia i nodi della griglia, emette il `reboot` comando su ciascun nodo, che determina 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 anche il contenitore.
- Il riavvio di un nodo StorageGRID Appliance riavvia anche il controller di elaborazione.

La procedura di riavvio progressivo 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.

Al contrario, questi nodi vengono riavviati in sequenza per garantire che i gruppi HA, i dati degli oggetti e i servizi dei nodi critici rimangano sempre disponibili.

Quando si riavvia il nodo di amministrazione primario, il browser perde temporaneamente l'accesso a Grid Manager, quindi non è più possibile monitorare la procedura. Per questo motivo, il nodo di amministrazione primario viene riavviato per ultimo.

Eseguire un riavvio progressivo

Seleziona i nodi che vuoi riavviare, rivedi le tue selezioni, avvia la procedura di riavvio e monitora l'avanzamento.

Seleziona nodi

Come primo passo, accedi alla pagina Riavvio progressivo e seleziona i nodi che desideri riavviare.

Passi

1. Selezionare **MANUTENZIONE > Attività > Riavvio progressivo**.
2. Esaminare lo stato della connessione e le icone di avviso nella colonna **Nome nodo**.



Non è possibile riavviare un nodo se è disconnesso dalla rete. Le caselle di controllo sono disabilitate per i nodi con queste icone:  .

3. Se alcuni nodi hanno avvisi attivi, rivedere l'elenco degli avvisi nella colonna **Riepilogo avvisi**.



Per visualizzare tutti gli avvisi correnti per un nodo, puoi anche 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**. Altrimenti, seleziona ogni nodo che vuoi riavviare.

È possibile utilizzare le opzioni di filtro della tabella per visualizzare sottoinsiemi di nodi. Ad esempio, è possibile visualizzare e selezionare solo i nodi di archiviazione oppure tutti i nodi in un determinato sito.

6. Seleziona **Rivedi selezione**.

Selezione della revisione

In questo passaggio puoi determinare quanto tempo potrebbe richiedere la procedura di riavvio totale e confermare di aver selezionato i nodi corretti.

1. Nella pagina Selezione revisione, rivedere il Riepilogo, che indica quanti nodi verranno riavviati e il tempo totale stimato per il riavvio di tutti i nodi.
2. Facoltativamente, per rimuovere un nodo specifico dall'elenco di riavvio, selezionare **Rimuovi**.
3. Facoltativamente, per aggiungere altri nodi, selezionare **Passaggio precedente**, selezionare i nodi aggiuntivi e selezionare **Rivedi selezione**.
4. Quando si è pronti ad avviare la procedura di riavvio progressivo per tutti i nodi selezionati, selezionare **Riavvia nodi**.
5. Se hai scelto di riavviare il nodo di amministrazione primario, leggi il messaggio informativo e seleziona **Sì**.



Il nodo di amministrazione primario sarà l'ultimo nodo a riavviarsi. Durante il riavvio di questo nodo, la connessione del browser verrà interrotta. Quando il nodo di amministrazione primario è nuovamente disponibile, è necessario ricaricare la pagina di riavvio progressivo.

Monitorare un riavvio progressivo

Mentre è in esecuzione la procedura di riavvio progressivo, è possibile monitorarla dal nodo di amministrazione primario.

Passi

1. Esaminare l'avanzamento complessivo dell'operazione, che include le seguenti informazioni:
 - Numero di nodi riavviati
 - Numero di nodi in fase 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 di riavviare
- Interruzione dei servizi

- Riavvio del sistema
- Servizi di avviamento
- Riavvio completato

Interrompere la procedura di riavvio progressivo

È possibile interrompere la procedura di riavvio progressivo dal nodo di amministrazione primario. Quando si interrompe la procedura, tutti i nodi con stato "Arresto servizi in corso", "Riavvio del sistema" o "Avvio servizi in corso" completeranno l'operazione di riavvio. Tuttavia, questi nodi non saranno più monitorati come parte della procedura.

Passi

1. Selezionare **MANUTENZIONE > Attività > Riavvio progressivo**.
2. Dal passaggio **Riavvio del monitor**, selezionare **Interrompi procedura di riavvio**.

Riavvia il nodo della griglia dalla scheda Attività

È possibile riavviare un singolo nodo della griglia dalla scheda Attività nella pagina Nodi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).
- Hai la passphrase di provisioning.
- Se si riavvia il nodo di amministrazione primario o un nodo di archiviazione, è necessario tenere presente quanto segue:
 - Quando si riavvia il nodo di amministrazione primario, il browser perde temporaneamente l'accesso a Grid Manager.
 - Se si riavviano due o più nodi di archiviazione in un determinato sito, potrebbe non essere possibile accedere a determinati oggetti per tutta la durata del riavvio. Questo problema può verificarsi se una regola ILM utilizza l'opzione di acquisizione **Dual commit** (o se una regola specifica **Balanced** e non è possibile creare immediatamente tutte le copie richieste). In questo caso, StorageGRID caricherà gli oggetti appena acquisiti su due nodi di archiviazione sullo stesso sito e valuterà ILM in un secondo momento.
 - Per assicurarti di poter accedere a tutti gli oggetti mentre un nodo di archiviazione è in fase di riavvio, interrompi l'acquisizione di oggetti in un sito per circa un'ora prima di riavviare il nodo.

Informazioni su questo compito

Quando StorageGRID riavvia un nodo della griglia, emette il `reboot` comando sul nodo, che provoca 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 anche il contenitore.
- Il riavvio di un nodo StorageGRID Appliance riavvia anche il controller di elaborazione.



Se è necessario riavviare più di un nodo, è possibile utilizzare ["procedura di riavvio progressivo"](#).

Passi

1. Selezionare **NODES**.
2. Selezionare il nodo della griglia che si desidera riavviare.
3. Selezionare la scheda **Attività**.
4. Selezionare **Riavvia**.

Viene visualizzata una finestra di dialogo di conferma. Se si riavvia il nodo di amministrazione primario, la finestra di dialogo di conferma ricorda che la connessione del browser al Grid Manager verrà interrotta temporaneamente quando i servizi vengono arrestati.

5. Immettere la passphrase di provisioning e selezionare **OK**.
6. Attendi il riavvio del nodo.

Potrebbe volerci del tempo prima che i servizi vengano chiusi.

Quando il nodo si riavvia, nella pagina Nodi viene visualizzata l'icona grigia (Amministrativamente inattivo) per il nodo. Una volta riavviati tutti i servizi e il nodo è connesso correttamente alla rete, la pagina Nodi dovrebbe visualizzare lo stato normale (nessuna icona a sinistra del nome del nodo), indicando che non ci sono avvisi attivi e che il nodo è connesso alla rete.

Riavviare il nodo della griglia dalla shell dei comandi

Se è necessario monitorare più attentamente l'operazione di riavvio o se non è possibile accedere a Grid Manager, è possibile accedere al nodo della griglia ed eseguire il comando di riavvio di Server Manager dalla shell dei comandi.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Passi

1. Accedi al nodo della griglia:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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; potrebbe essere opportuno accedere al sistema da remoto per monitorare il processo di arresto prima di riavviare il nodo nel passaggio successivo.

3. Riavviare il nodo della griglia: `reboot`
4. Disconnettersi dalla shell dei comandi: `exit`

Spegnere il nodo della griglia

È possibile arrestare un nodo della griglia dalla shell dei comandi del nodo.

Prima di iniziare

- Tu hai il `Passwords.txt` file.

Informazioni su questo compito

Prima di eseguire questa procedura, esaminare le seguenti considerazioni:

- In generale, non dovresti spegnere più di un nodo alla volta per evitare interruzioni.
- Non spegnere un nodo durante una procedura di manutenzione, a meno che non sia esplicitamente indicato nella documentazione o dal supporto tecnico.
- Il processo di spegnimento si basa sulla posizione in cui è installato il nodo, come segue:
 - L'arresto di un nodo VMware determina l'arresto della macchina virtuale.
 - L'arresto di un nodo Linux determina l'arresto del contenitore.
 - L'arresto di un nodo dell'appliance StorageGRID determina l'arresto del controller di elaborazione.
- Se si prevede di arrestare più di un nodo di archiviazione in un sito, interrompere l'acquisizione di oggetti in quel sito per circa un'ora prima di arrestare i nodi.

Se una regola ILM utilizza l'opzione di ingestione **Dual commit** (o se una regola utilizza l'opzione **Balanced** e non è possibile creare immediatamente tutte le copie richieste), StorageGRID esegue immediatamente il commit di tutti gli oggetti appena ingeriti su due nodi di archiviazione sullo stesso sito e valuta ILM in un secondo momento. Se più di un nodo di archiviazione in un sito viene arrestato, potresti non essere in grado di accedere ai nuovi oggetti acquisiti per tutta la durata dell'arresto. Le operazioni di scrittura potrebbero anche non riuscire se nel sito sono disponibili troppi pochi nodi di archiviazione. Vedere ["Gestire gli oggetti con ILM"](#).

Passi

1. Accedi al nodo della griglia:

- a. Immettere il seguente comando: `ssh admin@grid_node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Interrompere tutti i servizi: `service servermanager stop`

L'arresto dei servizi può richiedere fino a 15 minuti; potrebbe essere necessario accedere al sistema da remoto per monitorare il processo di arresto.

3. Se il nodo è in esecuzione su una macchina virtuale VMware o è un nodo appliance, emettere il comando di arresto: `shutdown -h now`

Eseguire questo passaggio indipendentemente dall'esito del `service servermanager stop` comando.



Dopo aver emesso il `shutdown -h now` comando su un nodo appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

Per l'apparecchio, questo comando spegne il controller, ma l'apparecchio rimane acceso. Devi completare il passaggio successivo.

4. Se si desidera spegnere un nodo appliance, seguire i passaggi specifici per l'appliance in uso.

SG6160

- a. Spegnere l'alimentazione del controller di archiviazione SG6100-CN.
- b. Attendere che il LED di alimentazione blu sul controller di archiviazione SG6100-CN si spenga.

SGF6112

- a. Spegnere l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

SG6000

- a. Attendere che il LED verde Cache Active sul retro dei controller di archiviazione si spenga.

Questo LED è acceso quando i dati memorizzati nella cache devono essere scritti sulle unità. Prima di interrompere l'alimentazione, attendere che il LED si spenga.

- b. Spegnere l'apparecchio e attendere che il LED blu di alimentazione si spenga.

SG5800

- a. Attendere che il LED verde Cache Active sul retro del controller di archiviazione si spenga.

Questo LED è acceso quando i dati memorizzati nella cache devono essere scritti sulle unità. Prima di interrompere l'alimentazione, attendere che il LED si spenga.

- b. Dalla home page di SANtricity System Manager, selezionare **Visualizza operazioni in corso**.
- c. Verificare che tutte le operazioni siano state completate prima di procedere con il passaggio successivo.
- d. Spegnere entrambi gli interruttori di alimentazione sul ripiano del controller e attendere che tutti i LED sul ripiano del controller si spengano.

SG5700

- a. Attendere che il LED verde Cache Active sul retro del controller di archiviazione si spenga.

Questo LED è acceso quando i dati memorizzati nella cache devono essere scritti sulle unità. Prima di interrompere l'alimentazione, attendere che il LED si spenga.

- b. Spegnere l'apparecchio e attendere che tutti i LED e il display a sette segmenti si arrestino.

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 arrestare i servizi su tutti i nodi della griglia su quell'host.

Passi

1. Accedi al nodo della griglia:

- a. Immettere il seguente comando: `ssh admin@grid_node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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; potrebbe essere necessario accedere al sistema da remoto per monitorare il processo di arresto.

3. Ripetere i passaggi 1 e 2 per ciascun nodo sull'host.

4. Se hai un host Linux:

- a. Accedere al sistema operativo host.
- b. Arresta il nodo: `storagegrid node stop`
- c. Arrestare il sistema operativo host.

5. Se il nodo è in esecuzione su una macchina virtuale VMware o è un nodo appliance, emettere il comando di arresto: `shutdown -h now`

Eseguire questo passaggio indipendentemente dall'esito del `service servermanager stop` comando.



Dopo aver emesso il `shutdown -h now` comando su un nodo appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

Per l'apparecchio, questo comando spegne il controller, ma l'apparecchio rimane acceso. Devi completare il passaggio successivo.

6. Se si desidera spegnere un nodo appliance, seguire i passaggi specifici per l'appliance in uso.

SG6160

- a. Spegner l'alimentazione del controller di archiviazione SG6100-CN.
- b. Attendere che il LED di alimentazione blu sul controller di archiviazione SG6100-CN si spenga.

SGF6112

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

SG6000

- a. Attendere che il LED verde Cache Active sul retro dei controller di archiviazione si spenga.

Questo LED è acceso quando i dati memorizzati nella cache devono essere scritti sulle unità. Prima di interrompere l'alimentazione, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che il LED blu di alimentazione si spenga.

SG5800

- a. Attendere che il LED verde Cache Active sul retro del controller di archiviazione si spenga.

Questo LED è acceso quando i dati memorizzati nella cache devono essere scritti sulle unità. Prima di interrompere l'alimentazione, attendere che il LED si spenga.

- b. Dalla home page di SANtricity System Manager, selezionare **Visualizza operazioni in corso**.
- c. Verificare che tutte le operazioni siano state completate prima di procedere con il passaggio successivo.
- d. Spegner entrambi gli interruttori di alimentazione sul ripiano del controller e attendere che tutti i LED sul ripiano del controller si spengano.

SG5700

- a. Attendere che il LED verde Cache Active sul retro del controller di archiviazione si spenga.

Questo LED è acceso quando i dati memorizzati nella cache devono essere scritti sulle unità. Prima di interrompere l'alimentazione, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che tutti i LED e il display a sette segmenti si arrestino.

SG110 o SG1100

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

SG100 o SG1000

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

7. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

- ["Dispositivi di archiviazione SGF6112 e SG6160"](#)

- ["Dispositivi di archiviazione SG6000"](#)
- ["Dispositivi di archiviazione SG5700"](#)
- ["Dispositivi di archiviazione SG5800"](#)
- ["Apparecchiature di servizio SG110 e SG1100"](#)
- ["Apparecchiature di servizio SG100 e SG1000"](#)

Spegnere e riaccendere tutti i nodi nella griglia

Potrebbe essere necessario arrestare 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 eseguire un arresto e un avvio controllati.

Quando si disattivano tutti i nodi in un sito o in una griglia, non sarà possibile accedere agli oggetti acquisiti mentre i nodi di archiviazione sono offline.

Arrestare i servizi e spegnere i nodi della griglia

Prima di poter spegnere un sistema StorageGRID , è necessario arrestare tutti i servizi in esecuzione su ciascun nodo della griglia, quindi arrestare tutte le macchine virtuali VMware, i motori dei container e le appliance StorageGRID .

Informazioni su questo compito

Arrestare prima i servizi sui nodi di amministrazione e sui nodi gateway, quindi arrestare i servizi sui nodi di archiviazione.

Questo approccio consente di utilizzare il nodo di amministrazione primario per monitorare lo stato degli altri nodi della griglia il più a lungo possibile.



Se un singolo host include più di un nodo della griglia, non arrestare l'host finché non hai arrestato tutti i nodi su quell'host. Se l'host include il nodo di amministrazione primario, arrestare quell'host per ultimo.



Se necessario, puoi ["migrare i nodi da un host Linux a un altro"](#) per eseguire la manutenzione dell'host senza compromettere la funzionalità o la disponibilità della griglia.

Passi

1. Impedisci 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. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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; potrebbe essere necessario accedere al sistema da remoto per monitorare il processo di arresto.

4. Ripetere i due passaggi precedenti per arrestare i servizi su tutti i nodi di archiviazione e sui nodi amministrativi non primari.

È possibile interrompere i servizi su questi nodi in qualsiasi ordine.



Se emetti il `service servermanager stop` comando per arrestare i servizi su un nodo di archiviazione dell'appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

5. Per il nodo di amministrazione primario, ripetere i passaggi per [accesso al nodo](#) **Arresto di tutti i servizi sul nodo**.
6. Per i nodi in esecuzione su host Linux:
 - a. Accedere al sistema operativo host.
 - b. Arresta il nodo: `storagegrid node stop`
 - c. Arrestare il sistema operativo host.
7. Per i nodi in esecuzione su macchine virtuali VMware e per i nodi di archiviazione dell'appliance, emettere il comando di arresto: `shutdown -h now`

Eseguire questo passaggio indipendentemente dall'esito del `service servermanager stop` comando.

Per l'appliance, questo comando arresta il controller di elaborazione, ma l'appliance rimane accesa. Devi completare il passaggio successivo.

8. Se disponi di nodi appliance, segui i passaggi per la tua appliance.

SG110 o SG1100

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

SG100 o SG1000

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

SG6160

- a. Spegner l'alimentazione del controller di archiviazione SG6100-CN.
- b. Attendere che il LED di alimentazione blu sul controller di archiviazione SG6100-CN si spenga.

SGF6112

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

SG6000

- a. Attendere che il LED verde Cache Active sul retro dei controller di archiviazione si spenga.

Questo LED è acceso quando i dati memorizzati nella cache devono essere scritti sulle unità. Prima di interrompere l'alimentazione, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che il LED blu di alimentazione si spenga.

SG5800

- a. Attendere che il LED verde Cache Active sul retro del controller di archiviazione si spenga.

Questo LED è acceso quando i dati memorizzati nella cache devono essere scritti sulle unità. Prima di interrompere l'alimentazione, attendere che il LED si spenga.

- b. Dalla home page di SANtricity System Manager, selezionare **Visualizza operazioni in corso**.
- c. Verificare che tutte le operazioni siano state completate prima di procedere con il passaggio successivo.
- d. Spegner entrambi gli interruttori di alimentazione sul ripiano del controller e attendere che tutti i LED sul ripiano del controller si spengano.

SG5700

- a. Attendere che il LED verde Cache Active sul retro del controller di archiviazione si spenga.

Questo LED è acceso quando i dati memorizzati nella cache devono essere scritti sulle unità. Prima di interrompere l'alimentazione, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che tutti i LED e il display a sette segmenti si arrestino.

9. Se necessario, disconnettersi dalla shell dei comandi: `exit`

La rete StorageGRID è stata ora disattivata.

Avviare i nodi della griglia



Se l'intera rete è rimasta spenta per più di 15 giorni, è necessario contattare l'assistenza tecnica prima di avviare qualsiasi nodo della rete. Non tentare di eseguire le procedure di ripristino che ricostruiscono i dati di Cassandra. Ciò potrebbe causare la perdita di dati.

Se possibile, accendere i nodi della rete in questo ordine:

- Applicare prima l'alimentazione ai nodi amministrativi.
- Applicare l'alimentazione ai nodi gateway per ultimi.



Se un host include più nodi della griglia, i nodi torneranno automaticamente online quando si accende l'host.

Passi

1. Accendere gli host per il nodo amministrativo primario e tutti i nodi amministrativi non primari.



Non sarà possibile accedere ai nodi di amministrazione finché i nodi di archiviazione non saranno stati riavviati.

2. Accendere gli host per tutti i nodi di archiviazione.

È possibile accendere questi nodi in qualsiasi ordine.

3. Accendere gli host per tutti i nodi gateway.
4. Sign in a Grid Manager.
5. Selezionare **NODI** e monitorare lo stato dei nodi della griglia. Verificare che non vi siano icone di avviso accanto ai nomi dei nodi.

Informazioni correlate

- ["Dispositivi di archiviazione SGF6112 e SG6160"](#)
- ["Apparecchiature di servizio SG110 e SG1100"](#)
- ["Apparecchiature di servizio SG100 e SG1000"](#)
- ["Dispositivi di archiviazione SG6000"](#)
- ["Dispositivi di archiviazione SG5800"](#)
- ["Dispositivi di archiviazione SG5700"](#)

Procedure di rimappatura delle porte

Rimuovi le rimappature delle porte

Se si desidera configurare un endpoint per il servizio Load Balancer e si desidera utilizzare una porta già configurata come porta mappata di una riassegnazione delle porte, è necessario prima rimuovere la riassegnazione delle porte esistente, altrimenti l'endpoint non sarà efficace. È necessario eseguire uno script su ciascun nodo di amministrazione e nodo gateway che presenta porte rimappate in conflitto per rimuovere tutte le rimappature delle porte del nodo.

Informazioni su questo compito

Questa procedura rimuove tutte le rimappature delle porte. Se hai bisogno di conservare alcune delle rimappature, contatta l'assistenza tecnica.

Per informazioni sulla configurazione degli endpoint del bilanciatore del carico, vedere ["Configurazione degli endpoint del bilanciatore del carico"](#).



Se la rimappatura della porta consente l'accesso al client, riconfigurare il client in modo che utilizzi una porta diversa come endpoint del bilanciatore del carico per evitare la perdita del servizio. In caso contrario, la rimozione della mappatura delle porte comporterà la perdita dell'accesso del client e dovrà essere pianificata di conseguenza.



Questa procedura non funziona per un sistema StorageGRID distribuito come contenitore su host bare metal. Vedi le istruzioni per ["rimozione delle rimappature delle porte sugli host bare metal"](#).

Passi

1. Accedi 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 del contenitore che esegue StorageGRID.

b. Inserisci la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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 di amministrazione e nodo gateway che presenta porte rimappate in conflitto.

Rimuovere le rimappature delle porte sugli host bare metal

Se si desidera configurare un endpoint per il servizio Load Balancer e si desidera utilizzare una porta già configurata come porta mappata di una riassegnazione delle porte, è necessario prima rimuovere la riassegnazione delle porte esistente, altrimenti l'endpoint non sarà efficace.

Informazioni su questo compito

Se si esegue StorageGRID su host bare metal, seguire questa procedura anziché la procedura generale per la rimozione delle rimappature delle porte. È necessario modificare il file di configurazione del nodo per ogni nodo amministrativo e nodo gateway che presenta porte rimappate in conflitto per rimuovere tutte le rimappature delle porte del nodo e riavviare il nodo.



Questa procedura rimuove tutte le rimappature delle porte. Se hai bisogno di conservare alcune delle rimappature, contatta l'assistenza tecnica.

Per informazioni sulla configurazione degli endpoint del bilanciatore del carico, consultare le istruzioni per l'amministrazione StorageGRID.



Questa procedura può causare una temporanea perdita del servizio quando i nodi vengono riavviati.

Passi

1. Accedi all'host che supporta il nodo. Accedi come root o con un account che abbia l'autorizzazione sudo.
2. Eseguire il seguente comando per disabilitare temporaneamente il nodo: `sudo storagegrid node stop node-name`
3. Utilizzando un editor di testo come vim o pico, modifica il file di configurazione del nodo.

Il file di configurazione del nodo può essere trovato su `/etc/storagegrid/nodes/node-name.conf`.

4. Individuare la sezione del file di configurazione del nodo che contiene le rimappature 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 le rimappature delle porte.

```

PORT_REMAP =
PORT_REMAP_INBOUND =

```

6. Eseguire il seguente comando per convalidare le modifiche apportate al file di configurazione del nodo: `sudo storagegrid node validate node-name`

Correggere eventuali errori o avvisi prima di procedere al passaggio successivo.

7. Eseguire il seguente comando per riavviare il nodo senza riassegnare le porte: `sudo storagegrid node start node-name`
8. Accedi al nodo come amministratore utilizzando la password elencata nel `Passwords.txt` file.
9. Verificare che i servizi si avviino correttamente.
 - a. Visualizza un elenco degli stati di tutti i servizi sul server: `sudo storagegrid-status`

Lo stato viene aggiornato automaticamente.

b. Attendi che tutti i servizi abbiano lo stato In esecuzione o Verificato.

c. Uscire dalla schermata di stato:Ctrl+C

10. Ripetere questi passaggi su ogni nodo di amministrazione e nodo gateway che presenta porte rimappate in conflitto.

Procedure di rete

Aggiorna le subnet per Grid Network

StorageGRID gestisce un elenco delle subnet di rete utilizzate per comunicare tra i nodi della griglia sulla rete Grid (eth0). Queste voci includono le subnet utilizzate per la rete Grid da ciascun sito nel sistema StorageGRID , nonché tutte le subnet utilizzate per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway della rete Grid. Quando si aggiungono nodi della griglia o un nuovo sito in un'espansione, potrebbe essere necessario aggiornare o aggiungere subnet alla rete della griglia.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"[browser web supportato](#)" .
- Tu hai il"[Autorizzazione di accesso alla manutenzione o alla root](#)" .
- Hai la passphrase di provisioning.
- Si dispone degli indirizzi di rete, in notazione CIDR, delle subnet che si desidera configurare.

Informazioni su questo compito

Se si esegue un'attività di espansione che include l'aggiunta di una nuova subnet, è necessario aggiungere una nuova subnet all'elenco delle subnet della rete Grid 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 amministrativa 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

Aggiungi una subnet

Passi

1. Selezionare **MANUTENZIONE > Rete > Rete a griglia**.
2. Selezionare **Aggiungi un'altra subnet** per aggiungere una nuova subnet in notazione CIDR.

Ad esempio, inserisci 10.96.104.0/22 .

3. Immettere la passphrase di provisioning e selezionare **Salva**.
4. Attendi che le modifiche vengano applicate, quindi scarica un nuovo pacchetto di ripristino.
 - a. Selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino**.
 - b. Immettere 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 . Viene utilizzato anche per recuperare il nodo di amministrazione primario.

Le subnet specificate vengono configurate automaticamente per il sistema StorageGRID .

Modifica una subnet

Passi

1. Selezionare **MANUTENZIONE > Rete > Rete a griglia**.
2. Selezionare la subnet che si desidera modificare e apportare le modifiche necessarie.
3. Immettere la passphrase di provisioning e selezionare **Salva**.
4. Selezionare **Sì** nella finestra di dialogo di conferma.

5. Attendi che le modifiche vengano applicate, quindi scarica un nuovo pacchetto di ripristino.
 - a. Selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino**.
 - b. Immettere la **Passphrase di provisioning**.

Elimina una subnet

Passi

1. Selezionare **MANUTENZIONE > Rete > Rete a griglia**.
2. Seleziona l'icona Elimina  accanto alla sottorete.
3. Immettere la passphrase di provisioning e selezionare **Salva**.
4. Selezionare **Sì** nella finestra di dialogo di conferma.
5. Attendi che le modifiche vengano applicate, quindi scarica un nuovo pacchetto di ripristino.
 - a. Selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino**.
 - b. Immettere la **Passphrase di provisioning**.

Configurare gli indirizzi IP

Linee guida per l'indirizzo IP

È possibile eseguire la configurazione di rete configurando gli indirizzi IP per i nodi della griglia tramite lo strumento Modifica IP.

È necessario utilizzare lo strumento Modifica IP per apportare la maggior parte delle modifiche alla configurazione di rete inizialmente impostata durante la distribuzione della griglia. Le modifiche manuali effettuate tramite comandi e file di rete Linux standard potrebbero non propagarsi a tutti i servizi StorageGRID e potrebbero non essere mantenute durante gli aggiornamenti, i riavvii o le procedure di ripristino dei nodi.



La procedura di modifica dell'IP può rivelarsi una procedura dirompente. Alcune parti della griglia potrebbero non essere disponibili finché non verrà applicata la nuova configurazione.



Se si apportano modifiche solo all'elenco delle subnet della rete Grid, utilizzare Grid Manager per aggiungere o modificare la configurazione di rete. In caso contrario, utilizzare lo strumento Modifica IP se Grid Manager non è accessibile a causa di un problema di configurazione di rete o se si sta eseguendo contemporaneamente una modifica del routing della rete Grid e altre modifiche di rete.



Se si desidera modificare l'indirizzo IP della rete Grid per tutti i nodi nella griglia, utilizzare ["procedura speciale per modifiche a livello di griglia"](#).

Interfacce Ethernet

L'indirizzo IP assegnato a eth0 è sempre l'indirizzo IP della rete Grid del nodo della griglia. L'indirizzo IP assegnato a eth1 è sempre l'indirizzo IP della rete di amministrazione 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 gli appliance StorageGRID, eth0, eth1 ed eth2 potrebbero essere interfacce aggregate composte da bridge subordinati o legami di interfacce fisiche o VLAN. Su queste piattaforme, la scheda **SSM > Risorse** potrebbe mostrare l'indirizzo IP di rete Grid, Admin e Client assegnato

ad altre interfacce oltre a eth0, eth1 o eth2.

DHCP

È possibile configurare DHCP solo durante la fase di distribuzione. Non è possibile impostare DHCP durante la configurazione. Se si desidera modificare gli indirizzi IP, le maschere di sottorete e i gateway predefiniti per un nodo della griglia, è necessario utilizzare le procedure di modifica dell'indirizzo IP. Utilizzando lo strumento Modifica IP, gli indirizzi DHCP diventeranno 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 in 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 della 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 in un indirizzo esterno alla subnet configurata per il gruppo HA.
- Non è possibile modificare l'indirizzo IP di Grid Network con il valore di un indirizzo IP virtuale esistente assegnato a un gruppo HA configurato sull'interfaccia di Grid Network.

Modifica la configurazione della rete del nodo

È possibile modificare la configurazione di rete di uno o più nodi utilizzando lo strumento Cambia IP. È possibile modificare la configurazione della rete Grid oppure aggiungere, modificare o rimuovere le reti Admin o Client.

Prima di iniziare

Tu hai il `Passwords.txt` file.

Informazioni su questo compito

Linux: Se si aggiunge un nodo griglia alla rete di amministrazione o alla rete client per la prima volta e in precedenza non si è configurato `ADMIN_NETWORK_TARGET` o `CLIENT_NETWORK_TARGET` nel file di configurazione del nodo, è necessario farlo ora.

Consultare le istruzioni di installazione StorageGRID per il sistema operativo Linux:

- ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
- ["Installa StorageGRID su Ubuntu o Debian"](#)

Appliance: Nelle appliance StorageGRID, se la rete client o amministrativa non è stata configurata nel programma di installazione dell'appliance StorageGRID durante l'installazione iniziale, la rete non può essere aggiunta utilizzando solo lo strumento Modifica IP. Per prima cosa devi ["mettere l'apparecchio in modalità manutenzione"](#), configurare i collegamenti, riportare l'appliance alla modalità operativa normale e quindi utilizzare lo strumento Modifica IP per modificare la configurazione di rete. Vedi il ["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 anche 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 al nodo un

indirizzo IP/maschera di sottorete su quella rete.

- È possibile rimuovere un nodo da una rete client o da una rete amministrativa eliminando l'indirizzo IP/la maschera di sottorete del nodo su quella rete.

I nodi non possono essere rimossi dalla rete Grid.



Non sono consentiti scambi di indirizzi IP. Se è necessario scambiare indirizzi IP tra nodi della griglia, è necessario utilizzare un indirizzo IP intermedio temporaneo.



Se per il sistema StorageGRID è abilitato l'accesso singolo (SSO) e si sta modificando l'indirizzo IP di un nodo di amministrazione, tenere presente che qualsiasi trust della parte affidabile configurato utilizzando l'indirizzo IP del nodo di amministrazione (anziché il suo nome di dominio completo, come consigliato) non sarà più valido. Non sarà più possibile accedere al nodo. Subito dopo aver modificato l'indirizzo IP, è necessario aggiornare o riconfigurare il trust della relying party del nodo in Active Directory Federation Services (AD FS) con il nuovo indirizzo IP. Vedi le istruzioni per "[configurazione SSO](#)".



Tutte le modifiche apportate alla rete tramite lo strumento Modifica IP vengono propagate al firmware di installazione per gli appliance StorageGRID. In questo modo, se il software StorageGRID viene reinstallato su un dispositivo o se un dispositivo viene messo in modalità di manutenzione, la configurazione di rete sarà corretta.

Passi

1. Accedi al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Avviare lo strumento Cambia IP immettendo il seguente comando: `change-ip`

3. Immettere la passphrase di provisioning al prompt.

Viene visualizzato il menu principale.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection: █
```


4. Facoltativamente, seleziona **1** per scegliere quali nodi aggiornare. Quindi seleziona una delle seguenti opzioni:

- **1:** Singolo nodo — seleziona per nome
- **2:** Singolo nodo: seleziona per sito, poi per nome
- **3:** Singolo nodo — seleziona in base all'IP corrente
- **4:** Tutti i nodi in un sito
- **5:** Tutti i nodi nella griglia

Nota: se si desidera aggiornare tutti i nodi, lasciare selezionato "tutti".

Dopo aver effettuato la selezione, viene visualizzato il menu principale, con il campo **Nodi selezionati** aggiornato per riflettere la scelta effettuata. Tutte le azioni successive vengono eseguite solo sui nodi visualizzati.

5. Nel menu principale, selezionare l'opzione **2** per modificare le informazioni IP/maschera, gateway e MTU per i nodi selezionati.

a. Seleziona la rete su cui vuoi apportare modifiche:

- **1:** Rete di griglia
- **2:** Rete di amministrazione
- **3:** Rete clienti
- **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.

La modifica dell'indirizzo IP, della lunghezza del prefisso, del gateway o dell'MTU di un'interfaccia configurata tramite DHCP modificherà l'interfaccia in statica. Quando si sceglie di modificare un'interfaccia configurata tramite DHCP, viene visualizzato un avviso per informare che l'interfaccia diventerà statica.

Interfacce configurate come `fixed` non può essere modificato.

b. Per impostare un nuovo valore, immetterlo nel formato mostrato per il valore corrente.

c. Per lasciare invariato il valore corrente, premere **Invio**.

d. Se il tipo di dati è `IP/mask`, puoi eliminare la rete di amministrazione o client dal nodo immettendo **d** o **0.0.0.0/0**.

e. Dopo aver modificato tutti i nodi che vuoi cambiare, digita **q** per tornare al menu principale.

Le modifiche verranno mantenute finché non verranno cancellate o applicate.

6. Rivedi le modifiche selezionando 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:

```

=====
Site: RTP
=====
username-x Grid IP [ 172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Admin IP [ 10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
Press Enter to continue

```

- **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 visualizzare aggiunte ed eliminazioni utilizzando il formato barrato. La corretta visualizzazione dipende dal fatto che il client terminale supporti 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 il divieto di utilizzare subnet sovrapposte, non vengano violate.

In questo esempio, la convalida ha restituito errori.

```

Validating new networking configuration... FAILED.

DK-10-224-S-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-S-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-S-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 aver completato la convalida, scegli una delle seguenti opzioni:

- **8:** Salva le modifiche non applicate.

Questa opzione consente di uscire dallo strumento Cambia IP e di riavviarlo in un secondo momento, senza perdere le modifiche non applicate.

- **10:** Applica la nuova configurazione di rete.

9. Se hai selezionato l'opzione **10**, scegli una delle seguenti opzioni:

- **applica:** applica immediatamente le modifiche e riavvia automaticamente ciascun nodo, se necessario.

Se la nuova configurazione di rete non richiede alcuna modifica fisica alla rete, è possibile selezionare **Applica** per applicare immediatamente le modifiche. Se necessario, i nodi verranno riavviati automaticamente. Verranno visualizzati i nodi che devono essere riavviati.

- **fase:** applica le modifiche al successivo riavvio manuale dei nodi.

Se è necessario apportare modifiche alla configurazione di rete fisica o virtuale affinché la nuova configurazione di rete funzioni, è necessario utilizzare l'opzione **stage**, arrestare i nodi interessati, apportare le modifiche necessarie alla rete fisica e riavviare i nodi interessati. Se si seleziona **Applica** senza prima apportare queste modifiche alla rete, solitamente le modifiche non andranno a buon fine.



Se si utilizza l'opzione **stage**, è necessario riavviare il nodo il prima possibile dopo lo staging per ridurre al minimo le interruzioni.

- **annulla:** Non apportare modifiche alla rete in questo momento.

Se non eri a conoscenza del fatto che le modifiche proposte richiedono il riavvio dei nodi, puoi rinviarle per ridurre al minimo l'impatto sull'utente. Selezionando **Annulla** si torna al menu principale e le modifiche vengono salvate, così da poterle applicare in seguito.

Quando si seleziona **applica** o **fase**, viene generato un nuovo file di configurazione di rete, viene eseguito il provisioning e i nodi vengono aggiornati con le 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
```

Dopo aver applicato o organizzato le modifiche, viene generato un nuovo pacchetto di ripristino come risultato della modifica alla configurazione della griglia.

10. Se hai selezionato **fase**, segui questi passaggi una volta completato il provisioning:

- a. Apportare le modifiche di rete fisiche o virtuali necessarie.

Modifiche alla rete fisica: apportare le modifiche necessarie alla rete fisica, arrestando in modo sicuro il nodo 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: aggiungi interfacce al nodo esistente](#)".

a. Riavviare i nodi interessati.

11. Selezionare **0** per uscire dallo strumento Modifica IP una volta completate le modifiche.

12. Scarica un nuovo pacchetto di ripristino da Grid Manager.

a. Selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino**.

b. Immettere la passphrase di provisioning.

Aggiungere o modificare gli elenchi di subnet sulla rete di amministrazione

È possibile aggiungere, eliminare o modificare le subnet nell'elenco delle subnet della rete di amministrazione di uno o più nodi.

Prima di iniziare

- Tu hai il `Passwords.txt` file.

È possibile aggiungere, eliminare o modificare le subnet di tutti i nodi nell'elenco delle subnet della rete di amministrazione.

Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete amministrativa 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

Passi

1. Accedi al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Avviare lo strumento Cambia IP immettendo il seguente comando: `change-ip`

3. Immettere la passphrase di provisioning al prompt.

Viene visualizzato il menu principale.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection: █
```

4. Facoltativamente, limitare le reti/nodi su cui vengono eseguite le operazioni. Scegli una delle seguenti opzioni:

- Selezionare i nodi da modificare scegliendo **1**, se si desidera filtrare in base a nodi specifici su cui eseguire l'operazione. Seleziona una delle seguenti opzioni:

- **1**: Singolo nodo (selezionare per nome)
- **2**: Singolo nodo (selezionare per sito, poi per nome)
- **3**: Singolo nodo (selezionabile tramite IP corrente)
- **4**: Tutti i nodi in un sito
- **5**: Tutti i nodi nella griglia
- **0**: Torna indietro

- Lascia che "tutto" rimanga selezionato. Dopo aver effettuato la selezione, viene visualizzata la schermata del menu principale. Il campo Nodi selezionati riflette la nuova selezione e ora tutte le operazioni selezionate verranno eseguite solo su questo elemento.

5. Nel menu principale, seleziona l'opzione per modificare le subnet per la rete di amministrazione (opzione **3**).

6. Scegli una delle seguenti opzioni:

- Aggiungi una subnet immettendo questo comando: `add CIDR`
- Elimina una subnet immettendo questo comando: `del CIDR`
- Imposta l'elenco delle subnet immettendo questo comando: `set CIDR`



Per tutti i comandi è possibile immettere 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 dati digitati utilizzando la "freccia su" per richiamare i valori digitati in precedenza nel prompt di input corrente e quindi modificarli se necessario.

L'esempio di input riportato di seguito mostra l'aggiunta di subnet all'elenco delle subnet della rete di amministrazione:

```
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
```

- Quando sei pronto, digita **q** per tornare alla schermata del menu principale. Le modifiche verranno mantenute finché non verranno cancellate o applicate.



Se nel passaggio 2 è stata selezionata una delle modalità di selezione dei nodi "tutti", premere **Invio** (senza **q**) per passare al nodo successivo nell'elenco.

- Scegli una delle seguenti opzioni:

- Selezionare l'opzione **5** per mostrare le modifiche nell'output isolato in modo da mostrare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'esempio di output 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 mostrare le modifiche nell'output che mostra la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni). **Nota:** Alcuni emulatori di terminale potrebbero visualizzare aggiunte ed eliminazioni utilizzando il formato barrato.

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 hai assegnato specificamente le subnet del server NTP e DNS a una rete, StorageGRID crea automaticamente un percorso host (/32) per la connessione. Se, ad esempio, si preferisce avere una rotta /16 o /24 per la connessione in uscita a un server DNS o NTP, è necessario eliminare la rotta /32 creata automaticamente e aggiungere le rotte desiderate. Se non si elimina la route host creata automaticamente, questa verrà mantenuta dopo aver applicato eventuali modifiche all'elenco delle subnet.



Sebbene sia possibile utilizzare questi percorsi host rilevati automaticamente, in genere è necessario configurare manualmente i percorsi DNS e NTP per garantire la connettività.

9. Selezionare l'opzione **7** per convalidare tutte le modifiche apportate.

Questa convalida garantisce che vengano rispettate le regole per le reti Grid, Admin e Client, ad esempio utilizzando subnet sovrapposte.

10. Facoltativamente, seleziona l'opzione **8** per salvare tutte le modifiche apportate e tornare in seguito per continuare ad apportare modifiche.

Questa opzione consente di uscire dallo strumento Cambia IP e di riavviarlo in un secondo momento, senza perdere le modifiche non applicate.

11. Eseguire 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 è pronti ad applicare le modifiche e a predisporre la nuova configurazione di rete. Durante il provisioning, l'output visualizza lo stato man mano che vengono applicati gli aggiornamenti, come mostrato nel seguente output di esempio:

```
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. Immettere la passphrase di provisioning.

Aggiungere o modificare gli elenchi di subnet su Grid Network

È possibile utilizzare lo strumento Modifica IP per aggiungere o modificare subnet sulla rete Grid.

Prima di iniziare

- Tu hai il `Passwords.txt` file.

È possibile aggiungere, eliminare o modificare le subnet nell'elenco delle subnet della rete Grid. Le modifiche interesseranno il routing su tutti i nodi della griglia.



Se si apportano modifiche solo all'elenco delle subnet della rete Grid, utilizzare Grid Manager per aggiungere o modificare la configurazione di rete. In caso contrario, utilizzare lo strumento Modifica IP se Grid Manager non è accessibile a causa di un problema di configurazione di rete o se si sta eseguendo contemporaneamente una modifica del routing della rete Grid e altre modifiche di rete.

Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete amministrativa 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

Passi

1. Accedi al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Avviare lo strumento Cambia IP immettendo il seguente comando: `change-ip`
3. Immettere la passphrase di provisioning al prompt.

Viene visualizzato il menu principale.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection: █
```

4. Nel menu principale, seleziona l'opzione per modificare le subnet per la rete Grid (opzione **4**).



Le modifiche all'elenco delle subnet della rete Grid riguardano l'intera griglia.

5. Scegli una delle seguenti opzioni:

- Aggiungi una subnet immettendo questo comando: `add CIDR`
- Elimina una subnet immettendo questo comando: `del CIDR`
- Imposta l'elenco delle subnet immettendo questo comando: `set CIDR`



Per tutti i comandi è possibile immettere 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 dati digitati utilizzando la "freccia su" per richiamare i valori digitati in precedenza nel prompt di input corrente e quindi modificarli se necessario.

L'esempio di input riportato di seguito mostra l'impostazione delle subnet per l'elenco delle subnet della rete Grid:

```

Editing: Grid Network Subnet List

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

Grid Network Subnet List
 172.16.0.0/21
 172.17.0.0/21
 172.18.0.0/21
192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21

```

6. Quando sei pronto, digita **q** per tornare alla schermata del menu principale. Le modifiche verranno mantenute finché non verranno cancellate o applicate.
7. Scegli una delle seguenti opzioni:
 - Selezionare l'opzione **5** per mostrare le modifiche nell'output isolato in modo da mostrare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'esempio di output riportato di seguito:

```

=====
Grid Network Subnet List (GNSL)
=====
                                     add 172.30.0.0/21
                                     add 172.31.0.0/21
                                     del 172.16.0.0/21
                                     del 172.17.0.0/21
                                     del 172.18.0.0/21
[      172.30.0.0/21 ]
[      172.31.0.0/21 ]
[      192.168.0.0/21 ]
Press Enter to continue

```

- Selezionare l'opzione **6** per mostrare le modifiche nell'output che mostra la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni).



Alcune interfacce della riga di comando potrebbero visualizzare aggiunte ed eliminazioni utilizzando il formato barrato.

8. Selezionare l'opzione **7** per convalidare tutte le modifiche apportate.

Questa convalida garantisce che vengano rispettate le regole per le reti Grid, Admin e Client, ad esempio utilizzando subnet sovrapposte.

9. Facoltativamente, seleziona l'opzione **8** per salvare tutte le modifiche apportate e tornare in seguito per continuare ad apportare modifiche.

Questa opzione consente di uscire dallo strumento Cambia IP e di riavviarlo in un secondo momento, senza perdere le modifiche non applicate.

10. Eseguire 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 è pronti ad applicare le modifiche e a predisporre la nuova configurazione di rete. Durante il provisioning, l'output visualizza lo stato man mano che vengono applicati gli aggiornamenti, come mostrato nel seguente output di esempio:

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

11. Se hai selezionato l'opzione **10** quando hai apportato modifiche alla rete Grid, seleziona una delle seguenti opzioni:

- **applica**: applica immediatamente le modifiche e riavvia automaticamente ciascun nodo, se necessario.

Se la nuova configurazione di rete funzionerà contemporaneamente alla vecchia configurazione di rete senza modifiche esterne, è possibile utilizzare l'opzione **applica** per una modifica della configurazione completamente automatizzata.

- **fase**: applica le modifiche al successivo riavvio dei nodi.

Se è necessario apportare modifiche alla configurazione di rete fisica o virtuale affinché la nuova configurazione di rete funzioni, è necessario utilizzare l'opzione **stage**, arrestare i nodi interessati, apportare le modifiche necessarie alla rete fisica 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.

- **annulla**: Non apportare modifiche alla rete in questo momento.

Se non eri a conoscenza del fatto che le modifiche proposte richiedono il riavvio dei nodi, puoi rinviarle per ridurre al minimo l'impatto sull'utente. Selezionando **Annulla** si torna al menu principale e le modifiche vengono salvate, così da poterle applicare in seguito.

Dopo aver applicato o organizzato le modifiche, viene generato un nuovo pacchetto di ripristino come risultato della modifica alla 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'IP e tornare al menu principale, digitare **a**.
- Per riprovare l'operazione non riuscita, immettere **r**.
- Per passare all'operazione successiva, immettere **c**.

L'operazione non riuscita può essere ripetuta in seguito selezionando l'opzione **10** (Applica modifiche) dal menu principale. La procedura di modifica dell'IP non sarà completata finché tutte le operazioni non saranno state completate correttamente.

- Se hai dovuto intervenire manualmente (ad esempio per riavviare un nodo) e sei sicuro che l'azione che lo strumento ritiene non riuscita sia stata effettivamente completata correttamente, immetti **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. Immettere 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 .

Cambia gli indirizzi IP per tutti i nodi nella griglia

Se è necessario modificare l'indirizzo IP della rete Grid per tutti i nodi della griglia, è necessario seguire questa procedura speciale. Non è possibile modificare l'IP della rete Grid a livello di griglia utilizzando la procedura per modificare singoli nodi.

Prima di iniziare

- Tu hai il `Passwords.txt` file.

Per garantire che la griglia si avvii correttamente, è necessario apportare tutte le modifiche contemporaneamente.



Questa procedura si applica solo alla rete Grid. Non è possibile utilizzare questa procedura per modificare gli indirizzi IP sulle reti di amministrazione o client.

Se si desidera modificare gli indirizzi IP e l'MTU per i nodi in un solo sito, seguire la procedura "[Modifica la configurazione della rete del nodo](#)" istruzioni.

Passi

1. Pianifica in anticipo le modifiche che devi apportare al di fuori dello strumento Modifica IP, come modifiche al DNS o NTP e modifiche alla configurazione Single Sign-On (SSO), se utilizzata.



Se i server NTP esistenti non saranno accessibili alla rete sui nuovi indirizzi IP, aggiungere i nuovi server NTP prima di eseguire la procedura di modifica dell'IP.



Se i server DNS esistenti non saranno accessibili alla griglia sui nuovi indirizzi IP, aggiungere i nuovi server DNS prima di eseguire la procedura di modifica dell'IP.



Se SSO è abilitato per il sistema StorageGRID e tutti i trust delle parti affidabili sono stati configurati utilizzando indirizzi IP del nodo di amministrazione (anziché nomi di dominio completi, come consigliato), prepararsi ad aggiornare o riconfigurare tali trust delle parti affidabili in Active Directory Federation Services (AD FS) subito dopo aver modificato gli indirizzi IP. Vedere "[Configurare l'accesso singolo](#)".



Se necessario, aggiungere la nuova subnet per i nuovi indirizzi IP.

2. Accedi al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

3. Avviare lo strumento Cambia IP immettendo il seguente comando: `change-ip`

4. Immettere la passphrase di provisioning al prompt.

Viene visualizzato il menu principale. Per impostazione predefinita, il `Selected nodes` il campo è impostato su `all`.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection: █
```

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 Grid.

Dopo aver effettuato la selezione, il prompt mostra i nomi dei nodi, il nome della rete Grid, il tipo di dati (IP/maschera, gateway o MTU) e i valori correnti.

La modifica dell'indirizzo IP, della lunghezza del prefisso, del gateway o dell'MTU di un'interfaccia configurata tramite DHCP modificherà l'interfaccia in statica. Prima di ogni interfaccia configurata da DHCP viene visualizzato un avviso.

Interfacce configurate come `fixed` non può essere modificato.

a. Per impostare un nuovo valore, immetterlo nel formato mostrato per il valore corrente.

b. Dopo aver modificato tutti i nodi che vuoi cambiare, digita **q** per tornare al menu principale.

Le modifiche verranno mantenute finché non verranno cancellate o applicate.

6. Rivedi le modifiche selezionando 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:

```

=====
Site: RTP
=====
username-x Grid IP [ 172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Admin IP [ 10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
Press Enter to continue

```

- 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 visualizzare aggiunte ed eliminazioni utilizzando il formato barrato. La corretta visualizzazione dipende dal fatto che il client terminale supporti le sequenze di escape VT100 necessarie.

7. Selezionare l'opzione 7 per convalidare tutte le modifiche.

Questa convalida garantisce che le regole per la rete Grid, come ad esempio il divieto di utilizzare subnet sovrapposte, non vengano violate.

In questo esempio, la convalida ha restituito errori.

```

Validating new networking configuration... FAILED.

DK-10-224-S-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-S-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-S-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 aver completato la convalida, selezionare **10** per applicare la nuova configurazione di rete.
9. Selezionare **fase** per applicare le modifiche al successivo riavvio dei nodi.



Devi selezionare **fase**. Non eseguire un riavvio progressivo, né manualmente né selezionando **applica** invece di **fase**; la griglia non si avvierà correttamente.

10. Dopo aver completato le modifiche, seleziona **0** per uscire dallo strumento Modifica IP.
11. Spegner tutti i nodi contemporaneamente.



L'intera rete deve essere spenta, in modo che tutti i nodi siano inattivi contemporaneamente.

12. Apportare le modifiche di rete fisiche o virtuali necessarie.
13. Verificare che tutti i nodi della griglia siano inattivi.
14. Accendere tutti i nodi.
15. Dopo che la rete si è avviata correttamente:
 - a. Se hai aggiunto nuovi server NTP, elimina i vecchi valori dei server NTP.
 - b. Se hai aggiunto nuovi server DNS, elimina i vecchi valori dei server DNS.
16. Scarica il nuovo pacchetto di ripristino da Grid Manager.
 - a. Selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino**.
 - b. Immettere la passphrase di provisioning.

Informazioni correlate

- ["Aggiungere o modificare gli elenchi di subnet su Grid Network"](#)
- ["Spegnere il nodo della griglia"](#)

Aggiungi interfacce al nodo esistente

Linux: aggiungi interfacce di amministrazione o client a un nodo esistente

Per aggiungere un'interfaccia sulla rete di amministrazione o sulla rete client a un nodo Linux dopo averla installata, seguire questi passaggi.

Se non hai configurato ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET nel file di configurazione del nodo sull'host Linux durante l'installazione, usa questa procedura per aggiungere l'interfaccia. Per ulteriori informazioni sul file di configurazione del nodo, consultare le istruzioni per il sistema operativo Linux:

- ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
- ["Installa StorageGRID su Ubuntu o Debian"](#)

Questa procedura va eseguita sul server Linux che ospita il nodo che necessita della nuova assegnazione di rete, non all'interno del nodo. Questa procedura aggiunge solo l'interfaccia al nodo; se si tenta di specificare altri parametri di rete, si verifica un errore di convalida.

Per fornire informazioni sull'indirizzamento, è necessario utilizzare lo strumento Modifica IP. Vedere ["Modifica la configurazione della rete del nodo"](#).

Passi

1. Accedi al server Linux che ospita il nodo.
2. Modifica il file di configurazione del nodo: `/etc/storagegrid/nodes/node-name.conf`.



Non specificare altri parametri di rete, altrimenti verrà generato un errore di convalida.

- a. Aggiungere una voce per la nuova destinazione di rete. Per esempio:

```
CLIENT_NETWORK_TARGET = bond0.3206
```

- b. Facoltativo: aggiungere una voce per l'indirizzo MAC. Per esempio:

```
CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
```

3. Eseguire il comando `node validate`:

```
sudo storagegrid node validate node-name
```

4. Risolvi tutti gli errori di convalida.
5. Eseguire il comando di ricaricamento del nodo:

```
sudo storagegrid node reload node-name
```

Linux: aggiungere interfacce trunk o di accesso a un nodo

È possibile aggiungere ulteriori trunk o interfacce di accesso a un nodo Linux dopo averlo installato. Le interfacce aggiunte vengono visualizzate nella pagina Interfacce VLAN e nella pagina Gruppi HA.

Prima di iniziare

- Hai accesso alle istruzioni per installare StorageGRID sulla tua piattaforma Linux.
 - ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
 - ["Installa StorageGRID su Ubuntu o Debian"](#)
- Tu hai il `Passwords.txt` file.
- Hai ["autorizzazioni di accesso specifiche"](#).



Non tentare di aggiungere interfacce a un nodo mentre è in corso un aggiornamento software, una procedura di ripristino o una procedura di espansione.

Informazioni su questo compito

Seguire questi passaggi per aggiungere una o più interfacce extra a un nodo Linux dopo che il nodo è stato installato. Ad esempio, potresti voler aggiungere un'interfaccia trunk a un nodo di amministrazione o gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico appartenente a diverse applicazioni o tenant. In alternativa, potresti voler aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (HA).

Se si aggiunge un'interfaccia trunk, 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 quando si aggiungono interfacce. Questa procedura dovrebbe essere eseguita su un nodo alla volta.

Passi

1. Accedi al server Linux che ospita il nodo.
2. Utilizzando un editor di testo come vim o pico, modifica 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. Utilizzare questo formato.

```
INTERFACE_TARGET_#####=value
```

Per *#####*, specificare un numero univoco per ciascuno INTERFACE_TARGET voce che stai aggiungendo.

Per *value*, 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 Interfacce VLAN e nella pagina Gruppi HA.

Per esempio:

```
INTERFACE_TARGET_0001=ens256, Trunk
```



Non specificare altri parametri di rete, altrimenti verrà generato un errore di convalida.

4. Eseguire il seguente comando per convalidare le modifiche al file di configurazione del nodo:

```
sudo storagegrid node validate node-name
```

Correggere eventuali errori o avvisi prima di procedere al passaggio successivo.

5. Eseguire il seguente comando per aggiornare la configurazione del nodo:

```
sudo storagegrid node reload node-name
```

Dopo aver finito

- Se hai aggiunto una o più interfacce trunk, vai a ["configurare le interfacce VLAN"](#) per configurare una o più interfacce VLAN per ogni nuova interfaccia padre.
- Se hai aggiunto una o più interfacce di accesso, vai a ["configurare gruppi ad alta disponibilità"](#) per aggiungere le nuove interfacce direttamente ai gruppi HA.

VMware: aggiungi trunk o interfacce di accesso a un nodo

È possibile aggiungere un trunk o un'interfaccia di accesso a un nodo VM dopo che il nodo è stato installato. Le interfacce aggiunte vengono visualizzate nella pagina Interfacce VLAN e nella pagina Gruppi HA.

Prima di iniziare

- Hai accesso alle istruzioni per ["installazione di StorageGRID sulla piattaforma VMware"](#).

- Sono presenti macchine virtuali VMware Admin Node e Gateway Node.
- Hai una subnet di rete che non viene utilizzata come rete Grid, Admin o Client.
- Tu hai il `Passwords.txt` file.
- Hai "autorizzazioni di accesso specifiche" .



Non tentare di aggiungere interfacce a un nodo mentre è in corso un aggiornamento software, una procedura di ripristino o una procedura di espansione.

Informazioni su questo compito

Per aggiungere una o più interfacce extra a un nodo VMware dopo averlo installato, seguire questi passaggi. Ad esempio, potresti voler aggiungere un'interfaccia trunk a un nodo di amministrazione o gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico appartenente a diverse applicazioni o tenant. Oppure potresti voler aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (HA).

Se si aggiunge un'interfaccia trunk, 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 quando si aggiungono interfacce.

Passi

1. In vCenter, aggiungere una nuova scheda di rete (tipo VMXNET3) a una VM Admin Node e Gateway Node. Selezionare le caselle di controllo **Connesso** e **Connetti all'accensione**.

Network adapter 4 *		CLIENT683_old_vlan	Connected
Status	☒ Connect At Power On		
Adapter Type	VMXNET 3		
DirectPath I/O	☒ Enable		

2. Utilizzare SSH per accedere al nodo di amministrazione o al nodo gateway.
3. Utilizzo `ip link show` per confermare che la nuova interfaccia di rete `ens256` è stata rilevata.

```
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
```

Dopo aver finito

- Se hai aggiunto una o più interfacce trunk, vai a [configurare le interfacce VLAN](#) per configurare una o più interfacce VLAN per ogni nuova interfaccia padre.
- Se hai aggiunto una o più interfacce di accesso, vai a [configurare gruppi ad alta disponibilità](#) per aggiungere le nuove interfacce direttamente ai gruppi HA.

Configurare i server DNS

È possibile aggiungere, aggiornare e rimuovere server DNS, in modo da poter utilizzare nomi host con nomi di dominio completi (FQDN) anziché indirizzi IP.

Per utilizzare nomi di dominio completi (FQDN) anziché indirizzi IP quando si specificano nomi host per destinazioni esterne, specificare l'indirizzo IP di ciascun server DNS che si utilizzerà. Queste voci vengono utilizzate per AutoSupport, e-mail di avviso, notifiche SNMP, endpoint dei servizi di piattaforma, pool di archiviazione cloud e altro ancora.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).
- Devi configurare gli indirizzi IP dei server DNS.

Informazioni su questo compito

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

Se possibile, utilizzare server DNS a cui ogni sito possa accedere localmente per garantire che un sito isolato possa risolvere gli FQDN per le destinazioni esterne.

Aggiungi un server DNS

Per aggiungere un server DNS, seguire questi passaggi.

Passi

1. Selezionare **MANUTENZIONE > Rete > Server DNS**.
2. Selezionare **Aggiungi un altro server** per aggiungere un server DNS.
3. Seleziona **Salva**.

Modificare un server DNS

Per modificare un server DNS, seguire questi passaggi.

Passi

1. Selezionare **MANUTENZIONE > Rete > Server DNS**.
2. Seleziona l'indirizzo IP del nome del server che vuoi modificare e apporta le modifiche necessarie.
3. Seleziona **Salva**.

Elimina un server DNS

Per eliminare un indirizzo IP di un server DNS, seguire questi passaggi.

Passi

1. Selezionare **MANUTENZIONE > Rete > Server DNS**.
2. Seleziona l'icona Elimina  accanto all'indirizzo IP.
3. Seleziona **Salva**.

Modifica la configurazione DNS per un singolo nodo della griglia

Invece di configurare il DNS globalmente per l'intera distribuzione, è possibile eseguire uno script per configurare il DNS in modo diverso per ciascun nodo della griglia.

In generale, dovresti usare l'opzione **MANUTENZIONE > Rete > Server DNS** su Grid Manager per configurare i server DNS. Utilizzare lo script seguente solo se è necessario utilizzare server DNS diversi per nodi di griglia diversi.

Passi

1. Accedi al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

- e. Aggiungere la chiave privata SSH all'agente SSH. Inserisci: `ssh-add`
- f. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.

2. Accedi al nodo che desideri aggiornare con una configurazione DNS personalizzata: `ssh node_IP_address`
3. Eseguire lo script di configurazione 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. Aggiungi l'indirizzo IPv4 di un server che fornisce il servizio di nomi di dominio per la tua rete: `add <nameserver IP_address>`
5. Ripeti il `add nameserver` comando per aggiungere server dei nomi.
6. Seguire le istruzioni richieste per gli altri comandi.

7. Salva le modifiche e esci dall'applicazione: `save`
8. Chiudere la shell dei comandi sul server: `exit`
9. Per ogni nodo della griglia, ripetere i passaggi da [accesso al nodo](#) Attraverso [chiusura della shell dei comandi](#) .
10. Quando non è più necessario l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserisci: `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 accuratamente tra i nodi della griglia nel sistema StorageGRID .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#) .
- Hai la passphrase di provisioning.
- Devi configurare gli indirizzi IPv4 dei server NTP.

Come StorageGRID utilizza NTP

Il sistema StorageGRID utilizza il Network Time Protocol (NTP) per sincronizzare l'ora tra tutti i nodi della griglia.

In ogni sito, ad almeno due nodi del sistema StorageGRID viene assegnato il ruolo NTP primario. Si sincronizzano con un minimo consigliato di quattro e un massimo di sei sorgenti temporali esterne e tra loro. Ogni nodo nel sistema StorageGRID che non sia un nodo NTP primario funge da client NTP e si sincronizza con questi nodi NTP primari.

I server NTP esterni si connettono ai nodi a cui in precedenza sono stati assegnati ruoli NTP primari. Per questo motivo, si consiglia di specificare almeno due nodi con ruoli NTP primari.

Linee guida del server NTP

Seguire queste linee guida per proteggersi dai problemi di tempistica:

- I server NTP esterni si connettono ai nodi a cui in precedenza sono stati assegnati ruoli NTP primari. Per questo motivo, si consiglia di specificare almeno due nodi con ruoli NTP primari.
- Assicurarsi che almeno due nodi in ogni sito possano accedere ad almeno quattro fonti NTP esterne. Se solo un nodo in un sito riesce a raggiungere le sorgenti NTP, si verificheranno problemi di temporizzazione se quel nodo non funziona. Inoltre, la designazione di due nodi per sito come fonti NTP primarie garantisce una temporizzazione accurata se un sito è isolato dal resto della griglia.
- I server NTP esterni specificati devono utilizzare il protocollo NTP. Per evitare problemi di deriva temporale, è necessario specificare riferimenti al server NTP di Stratum 3 o superiore.



Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Ora di Windows (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio orario delle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'uso in ambienti ad alta precisione, tra cui StorageGRID. Per i dettagli, vedere ["Limite di supporto per configurare il servizio Ora di Windows per ambienti ad alta precisione"](#).

Configurare i server NTP

Segui questi passaggi per aggiungere, aggiornare o rimuovere i server NTP.

Passi

1. Selezionare **MANUTENZIONE > Rete > Server NTP**.
2. Nella sezione Server, aggiungere, aggiornare o rimuovere le voci del server NTP, a seconda delle necessità.

Dovresti includere almeno quattro server NTP e puoi specificarne fino a sei.

3. Inserisci la passphrase di provisioning per il tuo sistema StorageGRID, quindi seleziona **Salva**.

La pagina è disabilitata finché gli aggiornamenti della configurazione non sono completati.



Se tutti i server NTP non superano il test di connessione dopo aver salvato i nuovi server NTP, non procedere. Contattare l'assistenza tecnica.

Risolvere i problemi del server NTP

Se si verificano problemi con la stabilità o la disponibilità dei server NTP specificati originariamente durante l'installazione, è possibile aggiornare l'elenco delle sorgenti NTP esterne utilizzate dal sistema StorageGRID aggiungendo altri server oppure aggiornando o rimuovendo i server esistenti.

Ripristinare la connettività di rete per i nodi isolati

In determinate circostanze, uno o più gruppi di nodi potrebbero non essere in grado di contattare il resto della griglia. Ad esempio, le modifiche degli indirizzi IP a livello di sito o di griglia possono dare origine a nodi isolati.

Informazioni su questo compito

L'isolamento del nodo è indicato da:

- Avvisi, come **Impossibile comunicare con il nodo (Avvisi > Correnti)**
- Diagnostica relativa alla connettività (**SUPPORTO > Strumenti > Diagnostica**)

Ecco alcune delle conseguenze derivanti dall'avere nodi isolati:

- Se più nodi sono isolati, potresti non essere in grado di accedere o accedere a Grid Manager.
- Se più nodi sono isolati, i valori di quota e utilizzo dello storage mostrati nella dashboard di Tenant Manager potrebbero non essere aggiornati. I totali verranno aggiornati quando la connettività di rete verrà ripristinata.

Per risolvere il problema di isolamento, eseguire un'utilità della riga di comando su ciascun nodo isolato o su un nodo in un gruppo (tutti i nodi in una subnet che non contiene il nodo di amministrazione primario) isolato dalla griglia. L'utilità fornisce ai nodi l'indirizzo IP di un nodo non isolato nella griglia, consentendo al nodo isolato o al gruppo di nodi di contattare nuovamente l'intera griglia.



Se il sistema dei nomi di dominio multicast (mDNS) è disabilitato nelle reti, potrebbe essere necessario eseguire l'utilità della riga di comando su ciascun nodo isolato.

Passi

Questa procedura non si applica quando solo alcuni servizi sono offline o segnalano errori di comunicazione.

1. Accedi al nodo e controlla `/var/local/log/dynip.log` per messaggi di isolamento.

Per 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, verrà visualizzato un messaggio che indica che il nodo potrebbe essere isolato.

Nelle distribuzioni Linux, i messaggi di isolamento apparirebbero 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 ogni nodo precedentemente isolato:

- I servizi del nodo sono stati avviati.
- Lo stato del servizio IP dinamico è "In esecuzione" dopo aver eseguito `storagegrid-status` comando.
- Nella pagina Nodi, il nodo non appare più disconnesso dal resto della griglia.



Se si esegue il `add_node_ip.py` comando non risolve il problema, potrebbero esserci altri problemi di rete che devono essere risolti.

Procedure host e middleware

Linux: Migrazione del nodo della griglia 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 compromettere la funzionalità o la disponibilità della griglia.

Ad esempio, potresti voler migrare un nodo per eseguire l'applicazione di patch al sistema operativo e il riavvio.

Prima di iniziare

- Hai pianificato la distribuzione StorageGRID in modo da includere il supporto per la migrazione.
 - ["Requisiti di migrazione dei container Node per Red Hat Enterprise Linux"](#)
 - ["Requisiti di migrazione dei container Node per Ubuntu o Debian"](#)
- L'host di destinazione è già preparato per l'utilizzo StorageGRID .
- L'archiviazione condivisa viene utilizzata per tutti i volumi di archiviazione per nodo
- Le interfacce di rete hanno nomi coerenti tra gli host.



In una distribuzione di produzione, non eseguire più di un nodo di archiviazione su un singolo host. Utilizzando un host dedicato per ogni nodo di archiviazione si ottiene un dominio di errore isolato.

Altri tipi di nodi, come i nodi amministrativi o i nodi gateway, possono essere distribuiti sullo stesso host. Tuttavia, se si dispone di più nodi dello stesso tipo (ad esempio due nodi gateway), non installare tutte le istanze sullo stesso host.

Esporta nodo dall'host di origine

Come primo passo, arresta il nodo della griglia ed esportalo dall'host Linux di origine.

Eseguire i seguenti comandi sull'host sorgente.

Passi

1. Ottieni lo stato di tutti i nodi attualmente in esecuzione sull'host di origine.

```
sudo storagegrid node status all
```

Esempio di output:

```
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 arrestarlo se il suo stato di esecuzione è In esecuzione.

```
sudo storagegrid node stop DC1-S3
```

Esempio di output:

```
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
```

Esempio di output:

```
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. Prendi nota del `import` comando suggerito nell'output.

Nel passaggio successivo, eseguiremo questo comando sull'host di destinazione.

Importa nodo sull'host di destinazione

Dopo aver esportato il nodo dall'host di origine, è necessario importare e convalidare il nodo sull'host di destinazione. La convalida conferma che il nodo ha accesso agli stessi dispositivi di archiviazione a blocchi e di interfaccia di rete che aveva sull'host di origine.

Eseguire i seguenti comandi sull'host di destinazione.

Passi

1. Importare il nodo sull'host di destinazione.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

Esempio di output:

```
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
```

Esempio di output:

```
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.

- ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
- ["Installa StorageGRID su Ubuntu o Debian"](#)

Avvia il nodo migrato

Dopo aver convalidato il nodo migrato, è possibile avviarlo eseguendo un comando sull'host di destinazione.

Passi

1. Avviare il nodo sul nuovo host.

```
sudo storagegrid node start DC1-S3
```

2. Sign in a Grid Manager e verifica che lo stato del nodo sia verde e senza avvisi.



La verifica che lo stato del nodo sia verde garantisce che il nodo migrato sia stato completamente riavviato e reinserito nella griglia. Se lo stato non è verde, non migrare altri nodi in modo da non avere più di un nodo fuori servizio.

3. Se non riesci ad accedere a Grid Manager, attendi 10 minuti, quindi esegui il seguente comando:

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

Verificare che il nodo migrato abbia uno stato di esecuzione impostato su In esecuzione.

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.

È necessario eseguire questa procedura se si nota che una macchina virtuale non si riavvia durante il ripristino di un nodo della griglia o l'esecuzione di un'altra procedura di manutenzione.

Passi

1. Nella struttura VMware vSphere Client, selezionare la macchina virtuale che non è avviata.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Accendi**.
3. Configurare VMware vSphere Hypervisor per riavviare automaticamente la macchina virtuale in futuro.

Recuperare o sostituire i nodi

Avvertenze e considerazioni per il ripristino del nodo della griglia

Se un nodo della griglia si guasta, è necessario ripristinarlo il prima possibile. Prima di iniziare, è necessario leggere attentamente tutti gli avvisi e le considerazioni sul ripristino del nodo.



StorageGRID è un sistema distribuito composto da più nodi che lavorano insieme. Non utilizzare snapshot del disco per ripristinare i nodi della griglia. Fare invece riferimento alle procedure di ripristino e manutenzione per ciascun tipo di nodo.



Se l'intero sito StorageGRID non funziona, contattare l'assistenza tecnica. Il supporto tecnico collaborerà con voi per sviluppare ed eseguire un piano di ripristino del sito che massimizzi la quantità di dati recuperati e soddisfi i vostri obiettivi aziendali. Vedere ["Come il supporto tecnico recupera un sito"](#).

Ecco alcuni dei motivi per cui è opportuno ripristinare un nodo della griglia non funzionante il prima possibile:

- Un nodo della griglia non funzionante può ridurre la ridondanza dei dati di sistema e degli oggetti, esponendoti al rischio di perdita permanente dei dati in caso di guasto di un altro nodo.
- Un nodo della rete non funzionante può avere ripercussioni sull'efficienza delle operazioni quotidiane.
- Un nodo della griglia non funzionante può ridurre la capacità di monitorare le operazioni del sistema.
- Un nodo della griglia non funzionante può causare un errore interno del server 500 se sono in atto rigide regole ILM.
- Se un nodo della griglia non viene ripristinato tempestivamente, i tempi di ripristino potrebbero aumentare. Ad esempio, potrebbero crearsi delle code che devono essere eliminate prima che il ripristino sia completato.

Seguire sempre la procedura di ripristino per il tipo specifico di nodo della griglia che si sta ripristinando. Le procedure di ripristino variano per i nodi amministrativi primari o non primari, i nodi gateway, i nodi appliance e i nodi di archiviazione.

Prerequisiti per il recupero dei nodi della griglia

Durante il recupero dei nodi della griglia si presuppongono tutte le seguenti condizioni:

- L'hardware fisico o virtuale guasto è stato sostituito e configurato.
- La versione di StorageGRID Appliance Installer sull'appliance sostitutiva corrisponde alla versione software del sistema StorageGRID, come descritto in ["Verificare e aggiornare la versione di StorageGRID Appliance Installer"](#).
- Se si sta ripristinando un nodo della griglia diverso dal nodo di amministrazione primario, esiste connettività tra il nodo della griglia in fase di ripristino e il nodo di amministrazione primario.
- Se si sta ripristinando un nodo di archiviazione dell'appliance, è necessario specificare lo stesso tipo di archiviazione dell'appliance originale (Combinato, Solo metadati o Solo dati) durante l'installazione dell'appliance. Se si specifica un tipo di archiviazione diverso, il ripristino non riuscirà e sarà necessario

reinstallare l'appliance con il tipo di archiviazione corretto specificato.

Ordine di ripristino del nodo se un server che ospita più di un nodo della griglia fallisce

Se un server che ospita più di un nodo della griglia si guasta, è possibile ripristinare i nodi in qualsiasi ordine. Tuttavia, se il server in errore ospita il nodo di amministrazione primario, è necessario prima ripristinare tale nodo. Ripristinando prima il nodo amministrativo primario si evita che altri ripristini dei nodi si interrompano mentre attendono di contattare il nodo amministrativo primario.

Indirizzi IP per i nodi recuperati

Non tentare di recuperare un nodo utilizzando un indirizzo IP attualmente assegnato a un altro nodo. Quando si distribuisce il nuovo nodo, utilizzare l'indirizzo IP corrente del nodo non riuscito o un indirizzo IP non utilizzato.

Se si utilizza un nuovo indirizzo IP per distribuire il nuovo nodo e poi si ripristina il nodo, il nuovo indirizzo IP continuerà a essere utilizzato per il nodo ripristinato. Se si desidera ripristinare l'indirizzo IP originale, utilizzare lo strumento Modifica IP una volta completato il ripristino.

Raccogliere i materiali necessari per il recupero del nodo della griglia

Prima di eseguire le procedure di manutenzione, è necessario assicurarsi di disporre dei materiali necessari per ripristinare un nodo della rete guasto.

Articolo	Note
Archivio di installazione di StorageGRID	Se è necessario recuperare un nodo della griglia, è necessario scarica i file di installazione di StorageGRID per la tua piattaforma. Nota: non è necessario scaricare file se si stanno ripristinando volumi di archiviazione non riusciti su un nodo di archiviazione.
Computer portatile di servizio	Il portatile di servizio deve avere quanto segue: • Porta di rete • Client SSH (ad esempio, PuTTY) • "Browser web supportato"

Articolo	Note
Pacchetto di recupero .zip file	Ottieni una copia del pacchetto di ripristino più recente .zip file: sgws-recovery-package-id-revision.zip Il contenuto del .zip i file vengono aggiornati ogni volta che il sistema viene modificato. Dopo aver apportato tali modifiche, ti verrà chiesto di archiviare la versione più recente del Pacchetto di ripristino in un luogo sicuro. Utilizzare la copia più recente per ripristinare la rete in caso di guasti. 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 riesci ad accedere a Grid Manager, puoi trovare copie crittografate del Recovery Package su alcuni nodi di archiviazione che contengono il servizio ADC. Su ciascun nodo di archiviazione, 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 recupero.
Frase segreta di provisioning	La passphrase viene creata e documentata quando il sistema StorageGRID viene installato per la prima volta. La passphrase di provisioning non è presente nel Passwords.txt file.
Documentazione attuale per la tua piattaforma	Per la documentazione, visitare il sito web del fornitore della piattaforma. Per le versioni attualmente supportate della tua piattaforma, consulta "Strumento matrice di interoperabilità NetApp" .

Scarica ed estrai i file di installazione StorageGRID

Scarica il software ed estrai i file, a meno che tu non sia ["recupero di volumi di archiviazione non riusciti su un nodo di archiviazione"](#) .

È necessario utilizzare la versione di StorageGRID attualmente in esecuzione sulla griglia.

Passi

1. Determina quale versione del software è attualmente installata. Nella parte superiore di Grid Manager, seleziona l'icona della guida e seleziona **Informazioni**.
2. Vai al ["Pagina di download di NetApp per StorageGRID"](#) .
3. Selezionare la versione di StorageGRID attualmente in esecuzione sulla griglia.

Le versioni del software StorageGRID hanno questo formato: 11.x.y .

4. Sign in 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 **Accetta e continua**.
6. Nella colonna **Installa StorageGRID** della pagina di download, seleziona .tgz O .zip file per la tua piattaforma.

La versione mostrata nel file di archivio di installazione deve corrispondere alla versione del software attualmente installato.

Utilizzare il .zip file se utilizzi 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. Scarica ed estrai il file di archivio.
8. Segui i passaggi appropriati per la tua piattaforma per scegliere i file di cui hai bisogno, in base alla piattaforma e ai nodi della griglia che devi recuperare.

I percorsi elencati nel passaggio per ciascuna piattaforma sono relativi alla directory di livello superiore installata dal file di archivio.

9. Se stai recuperando un ["Sistema Red Hat Enterprise Linux"](#) , seleziona i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download StorageGRID .
	Una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Pacchetto RPM per l'installazione delle immagini dei nodi StorageGRID sugli host RHEL.
	Pacchetto RPM per l'installazione del servizio host StorageGRID sugli host RHEL.
Strumento di scripting di distribuzione	Descrizione

Percorso e nome del file	Descrizione
	Uno script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID .
	Uno script Python utilizzato per automatizzare la configurazione degli appliance StorageGRID .
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Uno script Python di esempio che puoi utilizzare per accedere all'API di gestione della griglia quando è abilitato l'accesso singolo. È possibile utilizzare questo script anche per l'integrazione di Ping Federate.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Esempio di ruolo e playbook Ansible per la configurazione di host RHEL per la distribuzione di container StorageGRID . È possibile personalizzare il ruolo o il playbook in base alle proprie esigenze.
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO) tramite Active Directory o Ping Federate.
	Uno script di supporto chiamato dal compagno <code>storagegrid-ssoauth-azure.py</code> Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: prima di eseguire un aggiornamento, puoi utilizzare questi schemi per confermare che il codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova versione StorageGRID se non disponi di un ambiente StorageGRID non di produzione per i test di compatibilità dell'aggiornamento.

1. Se stai recuperando un "[Sistema Ubuntu o Debian](#)" , seleziona i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download StorageGRID .
	Un file di licenza NetApp non di produzione che puoi utilizzare per test e distribuzioni di prova di concetto.
	Pacchetto DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.
	Checksum MD5 per il file <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Pacchetto DEB per l'installazione del servizio host StorageGRID su host Ubuntu o Debian.
Strumento di scripting di distribuzione	Descrizione
	Uno script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID .
	Uno script Python utilizzato per automatizzare la configurazione degli appliance StorageGRID .
	Uno script Python di esempio che puoi utilizzare per accedere all'API di gestione della griglia quando è abilitato l'accesso singolo. È possibile utilizzare questo script anche per l'integrazione di Ping Federate.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Esempio di ruolo e playbook Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID . È possibile personalizzare il ruolo o il playbook in base alle proprie esigenze.
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO) tramite Active Directory o Ping Federate.

Percorso e nome del file	Descrizione
	Uno script di supporto chiamato dal compagno <code>storagegrid-ssoauth-azure.py</code> Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: prima di eseguire un aggiornamento, puoi utilizzare questi schemi per confermare che il codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova versione StorageGRID se non disponi di un ambiente StorageGRID non di produzione per i test di compatibilità dell'aggiornamento.

1. Se stai recuperando un ["Sistema VMware"](#) , seleziona i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download StorageGRID .
	Una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	File del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodi di griglia.
	Il file modello Open Virtualization Format(<code>.ovf</code>) e file manifesto(<code>.mf</code>) per distribuire il nodo di amministrazione primario.
	Il file modello(<code>.ovf</code>) e file manifesto(<code>.mf</code>) per distribuire nodi amministrativi non primari.
	Il file modello(<code>.ovf</code>) e file manifesto(<code>.mf</code>) per la distribuzione dei nodi gateway.
	Il file modello(<code>.ovf</code>) e file manifesto(<code>.mf</code>) per distribuire nodi di archiviazione basati su macchine virtuali.
Strumento di scripting di distribuzione	Descrizione
	Uno script shell Bash utilizzato per automatizzare la distribuzione di nodi di griglia virtuali.

Percorso e nome del file	Descrizione
	Un file di configurazione di esempio da utilizzare con <code>deploy-vsphere-ovftool.sh</code> sceneggiatura.
	Uno script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID .
	Uno script Python utilizzato per automatizzare la configurazione degli appliance StorageGRID .
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO). È possibile utilizzare questo script anche per l'integrazione di Ping Federate.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> sceneggiatura.
	Uno script Python di esempio che puoi utilizzare per accedere all'API Grid Management quando è abilitato l'accesso Single Sign-On (SSO) tramite Active Directory o Ping Federate.
	Uno script di supporto chiamato dal compagno <code>storagegrid-ssoauth-azure.py</code> Script Python per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: prima di eseguire un aggiornamento, puoi utilizzare questi schemi per confermare che il codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova versione StorageGRID se non disponi di un ambiente StorageGRID non di produzione per i test di compatibilità dell'aggiornamento.

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 dei nodi StorageGRID sui tuoi dispositivi.

Percorso e nome del file	Descrizione
	Checksum MD5 per il file /debs/storagegridwebscale- images-version-SHA.deb .



Per l'installazione dell'appliance, questi file sono necessari solo se si desidera evitare il traffico di rete. L'appliance può scaricare i file richiesti dal nodo di amministrazione primario.

Selezionare la procedura di ripristino del nodo

È necessario selezionare la procedura di ripristino corretta per il tipo di nodo che ha subito un errore.

Nodo della griglia	Procedura di recupero
Più di un nodo di archiviazione	Contattare l'assistenza tecnica. Se più di un nodo di archiviazione presenta un errore, il supporto tecnico deve intervenire per il ripristino, in modo da evitare incongruenze nel 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 archiviazione	La procedura di ripristino del nodo di archiviazione dipende dal tipo e dalla durata del guasto. "Ripristino da guasti del nodo di archiviazione"
Nodo di amministrazione	La procedura del nodo amministrativo varia a seconda che sia necessario ripristinare il nodo amministrativo primario o un nodo amministrativo non primario. "Ripristino da errori del nodo di amministrazione"
Nodo Gateway	"Ripristino da guasti del nodo gateway"
Nodo di archivio	"Ripristino da errori del nodo di archivio (sito di documentazione di StorageGRID 11.8)"



Se un server che ospita più di un nodo della griglia si guasta, è possibile ripristinare i nodi in qualsiasi ordine. Tuttavia, se il server in errore ospita il nodo di amministrazione primario, è necessario prima ripristinare tale nodo. Ripristinando prima il nodo amministrativo primario si evita che altri ripristini dei nodi si interrompano mentre attendono di contattare il nodo amministrativo primario.

Ripristino da guasti del nodo di archiviazione

Ripristino da guasti del nodo di archiviazione

La procedura per il ripristino di un nodo di archiviazione non riuscito dipende dal tipo di errore e dal tipo di nodo di archiviazione che ha subito il guasto.

Utilizzare questa tabella per selezionare la procedura di ripristino per un nodo di archiviazione non riuscito.

Problema	Azione	Note
- Più di un nodo di archiviazione è guasto. - Un secondo nodo di archiviazione ha subito un guasto meno di 15 giorni dopo un guasto o un ripristino del nodo di archiviazione. Ciò include il caso in cui un nodo di archiviazione si guasta mentre è ancora in corso il ripristino di un altro nodo di archiviazione.	Contattare l'assistenza tecnica.	Il ripristino di più di un nodo di archiviazione (o di più di un nodo di archiviazione nell'arco di 15 giorni) potrebbe compromettere l'integrità del database Cassandra, causando la perdita di dati. Il supporto tecnico può stabilire quando è sicuro iniziare il ripristino di un secondo nodo di archiviazione. Nota: se più di un nodo di archiviazione contenente il servizio ADC si guasta in un sito, si perdono tutte le richieste di servizio della piattaforma in sospeso per quel sito.
Si è verificato un errore in più di un nodo di archiviazione in un sito oppure in un intero sito.	Contattare l'assistenza tecnica. Potrebbe essere necessario eseguire una procedura di ripristino del sito.	Il supporto tecnico valuterà la tua situazione e svilupperà un piano di ripristino. Vedere "Come il supporto tecnico recupera un sito" .
Si è verificato un errore nel nodo di archiviazione di un'appliance.	"Ripristina il nodo di archiviazione dell'appliance"	La procedura di ripristino per i nodi di archiviazione dell'appliance è la stessa per tutti i guasti.
Uno o più volumi di archiviazione sono guasti, ma l'unità di sistema è intatta	"Ripristinare da un errore del volume di archiviazione in cui l'unità di sistema è intatta"	Questa procedura viene utilizzata per i nodi di archiviazione basati su software.
L'unità di sistema è guasta.	"Ripristino da un errore dell'unità di sistema"	La procedura di sostituzione del nodo dipende dalla piattaforma di distribuzione e dal fatto che anche altri volumi di archiviazione siano guasti.



Alcune procedure di ripristino StorageGRID utilizzano Reaper per gestire le riparazioni di Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Potresti notare che nell'output dello script viene menzionato "reaper" o "Cassandra repair". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

Ripristina il nodo di archiviazione dell'appliance

Avvisi per il ripristino dei nodi di archiviazione dell'appliance

La procedura per ripristinare un nodo di archiviazione dell'appliance StorageGRID non funzionante è la stessa, indipendentemente dal fatto che si stia ripristinando dalla perdita dell'unità di sistema o dalla perdita dei soli volumi di archiviazione.



Se più di un nodo di archiviazione è guasto (o è offline), contattare l'assistenza tecnica. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.



Se si tratta del secondo guasto del nodo di archiviazione in meno di 15 giorni dopo un guasto o un ripristino del nodo di archiviazione, contattare l'assistenza tecnica. La ricostruzione di Cassandra su due o più nodi di archiviazione entro 15 giorni può comportare la perdita di dati.



Se più di un nodo di archiviazione in un sito presenta un guasto, potrebbe essere necessaria una procedura di ripristino del sito. Vedere ["Come il supporto tecnico recupera un sito"](#).



Se le regole ILM sono configurate per archiviare solo una copia replicata e la copia esiste su un volume di archiviazione che ha subito un errore, non sarà possibile ripristinare l'oggetto.



Per le procedure di manutenzione hardware, come le istruzioni per la sostituzione di un controller o la reinstallazione del sistema operativo SANtricity, vedere ["Istruzioni per la manutenzione del tuo apparecchio di archiviazione"](#).

Preparare il nodo di archiviazione dell'appliance per la reinstallazione

Quando si ripristina un nodo di archiviazione dell'appliance, è necessario innanzitutto preparare l'appliance per la reinstallazione del software StorageGRID.

Passi

1. Accedi al nodo di archiviazione non riuscito:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Preparare l'appliance Storage Node per l'installazione del software StorageGRID. `sgareinstall`

3. Quando ti viene chiesto di continuare, inserisci: `y`

L'appliance si riavvia e la sessione SSH termina. In genere occorrono circa 5 minuti prima che StorageGRID Appliance Installer diventi disponibile, anche se in alcuni casi potrebbe essere necessario attendere fino a 30 minuti.



Non tentare di accelerare il riavvio spegnendo e riaccendendo il dispositivo o reimpostandolo in altro modo. Potresti interrompere gli aggiornamenti automatici del BIOS, BMC o di altri firmware.

Il nodo di archiviazione dell'appliance StorageGRID viene reimpostato e i dati sul nodo di archiviazione non sono più accessibili. Gli indirizzi IP configurati durante il processo di installazione originale dovrebbero rimanere intatti; tuttavia, si consiglia di confermarlo al termine della procedura.

Dopo aver eseguito il `sgareinstall` comando, tutti gli account, le password e le chiavi SSH forniti StorageGRID vengono rimossi e vengono generate nuove chiavi host.

Avvia l'installazione dell'appliance StorageGRID

Per installare StorageGRID su un nodo di archiviazione dell'appliance, utilizzare StorageGRID Appliance Installer, incluso nell'appliance.

Prima di iniziare

- L'apparecchio è stato installato in un rack, collegato alle reti e acceso.
- I collegamenti di rete e gli indirizzi IP sono stati configurati per l'appliance utilizzando StorageGRID Appliance Installer.
- Conosci l'indirizzo IP del nodo di amministrazione primario per la griglia StorageGRID .
- Tutte le subnet della rete Grid elencate nella pagina Configurazione IP del programma di installazione dell'appliance StorageGRID sono state definite nell'elenco delle subnet della rete Grid sul nodo di amministrazione primario.
- Hai completato queste attività preliminari seguendo le istruzioni di installazione per il tuo dispositivo di archiviazione. Vedere ["Avvio rapido per l'installazione dell'hardware"](#) .
- Stai utilizzando un ["browser web supportato"](#) .
- Conosci uno degli indirizzi IP assegnati al controller di elaborazione nell'appliance. È possibile utilizzare l'indirizzo IP per la rete di amministrazione (porta di gestione 1 sul controller), la rete di griglia o la rete client.

Informazioni su questo compito

Per installare StorageGRID su un nodo di archiviazione dell'appliance:

- Specificare o confermare l'indirizzo IP del nodo di amministrazione primario e il nome host (nome del sistema) del nodo.
- Si avvia l'installazione e si attende che i volumi vengano configurati e il software installato.



Quando si ripristina un nodo di archiviazione dell'appliance, reinstallarlo con lo stesso tipo di archiviazione dell'appliance originale (combinato, solo metadati o solo dati). Se si specifica un tipo di archiviazione diverso, il ripristino non riuscirà e sarà necessario reinstallare l'appliance con il tipo di archiviazione corretto specificato.

- A metà del processo, l'installazione si interrompe. Per riprendere l'installazione, è necessario accedere a Grid Manager e configurare il nodo di archiviazione in sospeso come sostituto del nodo non riuscito.
- Dopo aver configurato il nodo, il processo di installazione dell'appliance viene completato e l'appliance viene riavviata.

Passi

1. Aprire un browser e immettere uno degli indirizzi IP per il controller di elaborazione nell'appliance.

`https://Controller_IP:8443`

Viene visualizzata la home page del programma di installazione dell'appliance StorageGRID .

2. Nella sezione Connessione al nodo di amministrazione primario, determinare se è necessario specificare l'indirizzo IP per il nodo di amministrazione primario.

Il programma di installazione dell'appliance StorageGRID può rilevare automaticamente questo indirizzo IP, presupponendo che il nodo di amministrazione primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente sulla stessa subnet.

3. Se questo indirizzo IP non viene visualizzato o è necessario modificarlo, specificare l'indirizzo:

Opzione	Passi
Inserimento manuale dell'IP	a. Deselezionare la casella di controllo Abilita individuazione nodo amministratore. b. Inserire manualmente l'indirizzo IP. c. Fare clic su Salva. d. Attendi che lo stato di connessione per il nuovo indirizzo IP diventi "pronto".
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo Abilita individuazione nodo amministratore. b. Dall'elenco degli indirizzi IP rilevati, seleziona il nodo di amministrazione primario per la griglia in cui verrà distribuito questo nodo di archiviazione dell'appliance. c. Fare clic su Salva. d. Attendi che lo stato di connessione per il nuovo indirizzo IP diventi "pronto".

4. Nel campo **Nome nodo**, immettere lo stesso nome host (nome del sistema) utilizzato per il nodo che si sta ripristinando e fare clic su **Salva**.
5. Nella sezione Installazione, confermare che lo stato corrente è "Pronto per avviare l'installazione di *node name* nella griglia con il nodo di amministrazione primario *admin_ip*" e che il pulsante **Avvia installazione** sia abilitato.

Se il pulsante **Avvia installazione** non è abilitato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per le istruzioni, consultare le istruzioni di manutenzione dell'apparecchio.

6. Dalla home page di StorageGRID Appliance Installer, fare clic su **Avvia installazione**.

NetApp® StorageGRID® Appliance Installer

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Home

The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node discovery

☐

Primary Admin Node IP

172.16.4.210

Connection state

Connection to 172.16.4.210 ready

Cancel

Save

Node name

Node name

NetApp-SGA

Cancel

Save

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Start Installation

Lo stato corrente cambia in "Installazione in corso" e viene visualizzata la pagina Installazione del monitor.



Se è necessario accedere manualmente alla pagina Installazione monitor, fare clic su **Installazione monitor** dalla barra dei menu. Vedere ["Installazione dell'apparecchio di monitoraggio"](#).

Monitorare l'installazione dell'appliance StorageGRID

Il programma di installazione dell'appliance StorageGRID fornisce informazioni sullo stato fino al completamento dell'installazione. Una volta completata l'installazione del software,

l'appliance viene riavviata.

Passi

1. Per monitorare l'avanzamento dell'installazione, fare clic su **Monitora installazione** dalla barra dei menu.

La pagina Installazione del monitor mostra lo stato di avanzamento dell'installazione.

Monitor Installation

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

La barra di stato blu indica quale attività è attualmente in corso. Le barre di stato verdi indicano le attività completate con successo.



Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si sta rieseguendo un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "Ignorato".

2. Esaminare lo stato di avanzamento delle prime due fasi di installazione.

- **1. Configura l'archiviazione**

Durante questa fase, il programma di installazione si connette al controller di archiviazione, cancella qualsiasi configurazione esistente, comunica con SANtricity OS per configurare i volumi e configura le impostazioni host.

- **2. Installa il sistema operativo**

Durante questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID nell'appliance.

3. Continuare a monitorare l'avanzamento dell'installazione finché la fase **Install StorageGRID** non si interrompe e sulla console incorporata viene visualizzato un messaggio che richiede di approvare questo nodo sul nodo di amministrazione tramite Grid Manager.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Vai a ["Selezionare Avvia ripristino per configurare il nodo di archiviazione dell'appliance"](#) .

Selezionare Avvia ripristino per configurare il nodo di archiviazione dell'appliance

È necessario selezionare Avvia ripristino in Grid Manager per configurare un nodo di archiviazione dell'appliance come sostituto del nodo guasto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#) .
- Hai la passphrase di provisioning.

- Hai distribuito un'appliance di ripristino Storage Node.
- Hai la data di inizio di tutti i lavori di riparazione per i dati codificati in modo da essere cancellati.
- Hai verificato che il nodo di archiviazione non è stato ricostruito negli ultimi 15 giorni.

Passi

1. Da Grid Manager, seleziona **MANUTENZIONE > Attività > Ripristino**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Nodi in sospeso.

I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionarne uno finché non è stato reinstallato e non è pronto per il ripristino.

3. Immettere la **Passphrase di provisioning**.
4. Fare clic su **Avvia ripristino**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitorare l'avanzamento del ripristino nella tabella Nodo griglia in fase di ripristino.

Quando il nodo della griglia raggiunge la fase "In attesa di passaggi manuali", passare all'argomento successivo ed eseguire i passaggi manuali per rimontare e riformattare i volumi di archiviazione dell'appliance.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset



In qualsiasi momento durante il ripristino, puoi fare clic su **Reimposta** per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che se si reimposta la procedura, il nodo verrà lasciato in uno stato indeterminato.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo dell'appliance a uno stato preinstallato eseguendo `sgareinstall` sul nodo.

Rimontare e riformattare i volumi di archiviazione dell'appliance (passaggi manuali)

È necessario eseguire manualmente due script per rimontare i volumi di archiviazione conservati e riformattare quelli non riusciti. Il primo script rimonta i volumi formattati correttamente come volumi di archiviazione StorageGRID. Il secondo script riformatta tutti i volumi non montati, ricostruisce il database Cassandra, se necessario, e avvia i servizi.

Prima di iniziare

- Hai già sostituito l'hardware per tutti i volumi di archiviazione guasti che sai che necessitano di essere sostituiti.

Esecuzione del `sn-remount-volumes` potrebbe aiutarti a identificare ulteriori volumi di archiviazione non riusciti.

- Hai verificato che non è in corso la dismissione di un nodo di archiviazione oppure hai sospeso la procedura di dismissione del nodo. (Nel Grid Manager, seleziona **MANUTENZIONE** > **Attività** > **Dismissione**.)
- Hai verificato che non è in corso un'espansione. (Nel Grid Manager, seleziona **MANUTENZIONE** > **Attività** > **Espansione**.)



Contattare l'assistenza tecnica se più di un nodo di archiviazione è offline o se un nodo di archiviazione in questa griglia è stato ricostruito negli ultimi 15 giorni. Non eseguire il `sn-recovery-postinstall.sh` sceneggiatura. La ricostruzione di Cassandra su due o più nodi di archiviazione a distanza di 15 giorni l'uno dall'altro potrebbe comportare la perdita di dati.

Informazioni su questo compito

Per completare questa procedura, è necessario eseguire le seguenti attività di alto livello:

- Accedere al nodo di archiviazione recuperato.

- Esegui il `sn-remount-volumes` script per rimontare i volumi di archiviazione formattati correttamente. Quando questo script viene eseguito, esegue le seguenti operazioni:
 - Monta e smonta ciascun volume di archiviazione per riprodurre il journal XFS.
 - Esegue un controllo di coerenza del file XFS.
 - Se il file system è coerente, determina se il volume di archiviazione è un volume di archiviazione StorageGRID formattato correttamente.
 - Se il volume di archiviazione è formattato correttamente, rimonta il volume di archiviazione. Tutti i dati esistenti sul volume rimangono intatti.
- Esaminare l'output dello script e risolvere eventuali problemi.
- Esegui il `sn-recovery-postinstall.sh` sceneggiatura. Quando questo script viene eseguito, esegue le seguenti operazioni.



Non riavviare un nodo di archiviazione durante il ripristino prima dell'esecuzione `sn-recovery-postinstall.sh` (passaggio 4) per riformattare i volumi di archiviazione non riusciti e ripristinare i metadati degli oggetti. Riavvio del nodo di archiviazione prima `sn-recovery-postinstall.sh` completa causa errori per i servizi che tentano di avviarsi e fa sì che i nodi dell'appliance StorageGRID escano dalla modalità di manutenzione.

- Riformatta tutti i volumi di archiviazione che `sn-remount-volumes` script che non è stato possibile montare o che sono stati trovati formattati in modo non corretto.



Se un volume di archiviazione viene riformattato, tutti i dati presenti su quel volume andranno persi. È necessario eseguire una procedura aggiuntiva per ripristinare i dati degli oggetti da altre posizioni nella griglia, presupponendo che le regole ILM siano state configurate per archiviare più di una copia dell'oggetto.

- Se necessario, ricostruisce il database Cassandra sul nodo.
- Avvia i servizi sul nodo di archiviazione.

Passi

1. Accedi al nodo di archiviazione recuperato:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Eseguire il primo script per rimontare tutti i volumi di archiviazione formattati correttamente.



Se tutti i volumi di archiviazione sono nuovi e devono essere formattati, oppure se tutti i volumi di archiviazione sono guasti, è possibile saltare questo passaggio ed eseguire il secondo script per riformattare tutti i volumi di archiviazione non montati.

- Esegui lo script: `sn-remount-volumes`

L'esecuzione di questo script su volumi di archiviazione contenenti dati potrebbe richiedere ore.

b. Durante l'esecuzione dello script, rivedere l'output e rispondere a eventuali richieste.



Se necessario, è possibile utilizzare il `tail -f` comando per monitorare il contenuto del file di registro dello script(`/var/local/log/sn-remount-volumes.log`). Il file di registro 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 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 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 archiviazione è stato rimontato correttamente e tre volumi di archiviazione presentavano errori.

- `/dev/sdb` ha superato il controllo di coerenza del file system XFS e aveva una struttura del volume valida, quindi è stato rimontato correttamente. I dati sui dispositivi rimontati dallo script vengono conservati.
- `/dev/sdc` il controllo di coerenza del file system XFS non è riuscito perché il volume di archiviazione era nuovo o danneggiato.
- `/dev/sdd` non è stato possibile montarlo perché il disco non è stato inizializzato o il superblocco del disco è danneggiato. Quando lo script non riesce a montare un volume di archiviazione, chiede se si desidera eseguire il controllo di coerenza del file system.

- Se il volume di archiviazione è collegato a un nuovo disco, rispondere **N** al prompt. Non è necessario controllare il file system su un nuovo disco.
- Se il volume di archiviazione è collegato a un disco esistente, rispondere **Y** al prompt. È possibile utilizzare i risultati del controllo del file system per determinare l'origine del danneggiamento. I risultati vengono salvati nel `/var/local/log/sn-remount-volumes.log` file di registro.
- `/dev/sde` ha superato il controllo di coerenza del file system XFS e aveva una struttura del volume valida; tuttavia, l'ID del nodo LDR nel ``volID` il file non corrisponde all'ID per questo nodo di archiviazione (il configured LDR noid visualizzato in alto). Questo messaggio indica che questo volume appartiene a un altro nodo di archiviazione.

3. Esaminare l'output dello script e risolvere eventuali problemi.



Se un volume di archiviazione 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 del `sn-recovery-postinstall.sh` sceneggiatura su questi volumi.

- Verificare che i risultati includano una voce per tutti i volumi previsti. Se non sono elencati volumi, eseguire nuovamente lo script.
- Esaminare i messaggi per tutti i dispositivi montati. Assicurarsi che non vi siano errori che indicano che un volume di archiviazione non appartiene a questo nodo di archiviazione.

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 archiviazione viene segnalato come appartenente a un altro nodo di archiviazione, contattare l'assistenza tecnica. Se esegui il `sn-recovery-postinstall.sh` script, il volume di archiviazione verrà riformattato, il che potrebbe causare la perdita di dati.

- Se non è stato possibile montare un dispositivo di archiviazione, prendere nota del nome del dispositivo e ripararlo o sostituirlo.



È necessario riparare o sostituire tutti i dispositivi di archiviazione che non è stato possibile montare.

Utilizzerai il nome del dispositivo per cercare l'ID del volume, che è un input obbligatorio quando esegui il `repair-data` script per ripristinare i dati dell'oggetto nel volume (procedura successiva).

- Dopo aver riparato o sostituito tutti i dispositivi non montabili, eseguire il `sn-remount-volumes` script di nuovo per confermare che tutti i volumi di archiviazione che possono essere rimontati siano stati rimontati.



Se un volume di archiviazione non può essere montato o non è formattato correttamente e si procede con il passaggio successivo, il volume e tutti i dati in esso contenuti verranno eliminati. Se si dispone di due copie dei dati dell'oggetto, sarà disponibile una sola copia finché non si completa la procedura successiva (ripristino dei dati dell'oggetto).



Non eseguire il `sn-recovery-postinstall.sh` script se ritieni che i dati rimanenti su un volume di archiviazione non riuscito non possano essere ricostruiti da nessun'altra parte nella griglia (ad esempio, se la policy ILM utilizza una regola che crea una sola copia o se i volumi sono falliti su più nodi). Contatta invece l'assistenza tecnica per scoprire come recuperare i tuoi dati.

4. Esegui il `sn-recovery-postinstall.sh` sceneggiatura: `sn-recovery-postinstall.sh`

Questo script riformatta tutti i volumi di archiviazione che non è stato possibile montare o che sono stati trovati formattati in modo non corretto; ricostruisce il database Cassandra sul nodo, se necessario; e avvia i servizi sul nodo di archiviazione.

Siate consapevoli di quanto segue:

- L'esecuzione dello script potrebbe richiedere ore.
- In generale, è consigliabile lasciare inalterata la sessione SSH mentre lo script è in esecuzione.
- Non premere **Ctrl+C** mentre la sessione SSH è attiva.
- Lo script verrà eseguito in background se si verifica un'interruzione della rete e termina la sessione SSH, ma è possibile visualizzare l'avanzamento dalla pagina Ripristino.
- Se il nodo di archiviazione utilizza il servizio RSM, lo script potrebbe bloccarsi 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 archiviazione che includono il servizio ADC.



Alcune procedure di ripristino StorageGRID utilizzano Reaper per gestire le riparazioni di Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Potresti notare che nell'output dello script viene menzionato "reaper" o "Cassandra repair". 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 il `sn-recovery-postinstall.sh` quando lo script viene eseguito, monitorare la pagina Ripristino in Grid Manager.

La barra di avanzamento e la colonna Fase nella pagina Ripristino forniscono uno stato di alto livello del `sn-recovery-postinstall.sh` sceneggiatura.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

6. Dopo il `sn-recovery-postinstall.sh` Una volta che lo script ha avviato i servizi sul nodo, è possibile ripristinare i dati dell'oggetto su qualsiasi volume di archiviazione 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 l'archiviazione degli oggetti rispetto al nodo originale, è necessario [ripristinare manualmente i dati dell'oggetto](#) utilizzando il `repair-data` sceneggiatura. Se si verifica uno di questi casi, rispondi `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.

Ripristina i dati dell'oggetto nel volume di archiviazione per l'appliance

Dopo aver ripristinato i volumi di archiviazione per l'appliance Storage Node, è possibile ripristinare i dati degli oggetti replicati o codificati per la cancellazione che sono andati persi a causa del guasto dell'appliance Storage Node.

Quale procedura dovrei usare?

Se possibile, ripristinare i dati dell'oggetto utilizzando la pagina **Ripristino volume** in Grid Manager.

- Se i volumi sono elencati in **MANUTENZIONE > Ripristino volume > Nodi da ripristinare**, ripristinare i dati dell'oggetto utilizzando [Pagina di ripristino del volume in Grid Manager](#) .

- Se i volumi non sono elencati in **MANUTENZIONE > Ripristino volume > Nodi da ripristinare**, seguire i passaggi seguenti per utilizzare `repair-data` script per ripristinare i dati dell'oggetto.

Se il nodo di archiviazione recuperato contiene meno volumi rispetto al nodo che sta sostituendo, è necessario utilizzare `repair-data` sceneggiatura.



Lo script `repair-data` è obsoleto e verrà rimosso in una versione futura. Quando possibile, utilizzare il "[Procedura di ripristino del volume in Grid Manager](#)".

Utilizzare il `repair-data` script per ripristinare i dati dell'oggetto

Prima di iniziare

- Hai confermato che il nodo di archiviazione recuperato ha uno stato di connessione **Connesso***  nella scheda ***NODI > Panoramica** nel Grid Manager.

Informazioni su questo compito

I dati degli oggetti possono essere ripristinati da altri nodi di archiviazione o da un pool di archiviazione cloud, presupponendo che le regole ILM della griglia siano state configurate in modo che siano disponibili copie degli oggetti.

Notare quanto segue:

- Se una regola ILM è stata configurata per archiviare solo una copia replicata e tale copia esisteva su un volume di archiviazione che ha generato un errore, non sarà possibile ripristinare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID deve inviare più richieste all'endpoint del Cloud Storage Pool per ripristinare i dati dell'oggetto. Prima di eseguire questa procedura, contattare l'assistenza tecnica per ottenere assistenza nella stima dei tempi di ripristino e dei costi associati.

Informazioni su `repair-data` sceneggiatura

Per ripristinare i dati dell'oggetto, eseguire il comando `repair-data` sceneggiatura. Questo script avvia il processo di ripristino dei dati dell'oggetto e funziona con la scansione ILM per garantire che le regole ILM vengano rispettate.

Seleziona **Dati replicati** o **Dati con codice di cancellazione (EC)** qui sotto per conoscere le diverse opzioni per `repair-data` script, a seconda che si stiano ripristinando dati replicati o dati con codice di cancellazione. Se è necessario ripristinare entrambi i tipi di dati, è necessario eseguire entrambi i set di comandi.



Per maggiori informazioni sul `repair-data` script, inserisci `repair-data --help` dalla riga di comando del nodo di amministrazione primario.



Lo script `repair-data` è obsoleto e verrà rimosso in una versione futura. Quando possibile, utilizzare il "[Procedura di ripristino del volume in Grid Manager](#)".

Dati replicati

Sono disponibili due comandi per ripristinare i dati replicati, a seconda che sia necessario riparare l'intero nodo o solo determinati volumi sul nodo:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

È possibile monitorare le riparazioni dei dati replicati con questo comando:

```
repair-data show-replicated-repair-status
```

Dati con codice di cancellazione (EC)

Sono disponibili due comandi per ripristinare i dati codificati in modo da essere cancellati, 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 monitorare le riparazioni dei dati codificati in modo da cancellarli con questo comando:

```
repair-data show-ec-repair-status
```



Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. Tuttavia, se non è possibile recuperare tutti i dati codificati in modo da cancellarli, la riparazione non può essere completata. La riparazione verrà completata quando tutti i nodi saranno disponibili.



Il lavoro di riparazione EC riserva temporaneamente una grande quantità di spazio di archiviazione. Potrebbero essere attivati avvisi di archiviazione, ma il problema si risolverà al termine della riparazione. Se non c'è abbastanza spazio per la prenotazione, il lavoro di riparazione EC fallirà. Le prenotazioni di archiviazione vengono rilasciate al termine del processo di riparazione EC, indipendentemente dal fatto che il processo sia fallito o riuscito.

Trova il nome host per il nodo di archiviazione

1. Accedi al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Utilizzare il `/etc/hosts` file per trovare il nome host del nodo di archiviazione per i volumi di archiviazione ripristinati. Per visualizzare un elenco di tutti i nodi nella griglia, immettere quanto segue: `cat`

/etc/hosts .

Ripara i dati se tutti i volumi sono falliti

Se tutti i volumi di archiviazione sono guasti, riparare l'intero nodo. Seguire le istruzioni per i **dati replicati**, i **dati con codice di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codice di cancellazione (EC) o entrambi.

Se solo alcuni volumi sono falliti, vai a [Riparare i dati se solo alcuni volumi sono falliti](#) .



Non puoi correre `repair-data` operazioni per più di un nodo contemporaneamente. Per recuperare più nodi, contattare l'assistenza tecnica.

Dati replicati

Se la griglia include dati replicati, utilizzare `repair-data start-replicated-node-repair` comando con il `--nodes` opzione, dove `--nodes` è il nome host (nome del sistema) per riparare l'intero nodo di archiviazione.

Questo comando ripara i dati replicati su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Quando i dati degli oggetti vengono ripristinati, viene attivato l'avviso **Oggetti persi** se il sistema StorageGRID non riesce a individuare i dati degli oggetti replicati. Gli avvisi potrebbero essere attivati sui nodi di archiviazione in tutto il sistema. Dovresti determinare la causa della perdita e se è possibile un recupero. Vedere "[Indagare sugli oggetti smarriti](#)" .

Dati con codice di cancellazione (EC)

Se la griglia contiene dati con codice di cancellazione, utilizzare `repair-data start-ec-node-repair` comando con il `--nodes` opzione, dove `--nodes` è il nome host (nome del sistema) per riparare l'intero nodo di archiviazione.

Questo comando ripara i dati codificati in modo da essere cancellati su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'operazione restituisce un valore univoco `repair ID` che identifica questo `repair_data` operazione. Usa questo `repair ID` per monitorare i progressi e i risultati del `repair_data` operazione. Non verrà restituito alcun altro feedback una volta completato il processo di recupero.

Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. La riparazione verrà completata quando tutti i nodi saranno disponibili.

Riparare i dati se solo alcuni volumi sono falliti

Se solo alcuni volumi sono guasti, riparare i volumi interessati. Seguire le istruzioni per i **dati replicati**, i **dati con codice di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codice di cancellazione (EC) o entrambi.

Se tutti i volumi sono falliti, vai a [Ripara i dati se tutti i volumi sono falliti](#) .

Immettere gli ID del volume in formato esadecimale. Per esempio, 0000 è il primo volume e 000F è il sedicesimo volume. È possibile specificare un volume, un intervallo di volumi o più volumi non in sequenza.

Tutti i volumi devono trovarsi sullo stesso nodo di archiviazione. Se è necessario ripristinare volumi per più di un nodo di archiviazione, contattare l'assistenza tecnica.

Dati replicati

Se la griglia contiene dati replicati, utilizzare `start-replicated-volume-repair` comando con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi aggiungere o il `--volumes` O `--volume-range` opzione, come mostrato negli esempi seguenti.

Volume singolo: questo comando ripristina i dati replicati nel volume 0002 su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervallo di volumi: questo comando ripristina i dati replicati su tutti i volumi nell'intervallo 0003 A 0009 su un nodo di archiviazione 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 archiviazione denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Quando i dati degli oggetti vengono ripristinati, viene attivato l'avviso **Oggetti persi** se il sistema StorageGRID non riesce a individuare i dati degli oggetti replicati. Gli avvisi potrebbero essere attivati sui nodi di archiviazione in tutto il sistema. Prendere nota della descrizione dell'avviso e delle azioni consigliate per determinare la causa della perdita e se è possibile un recupero.

Dati con codice di cancellazione (EC)

Se la griglia contiene dati con codice di cancellazione, utilizzare `start-ec-volume-repair` comando con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi aggiungere o il `--volumes` O `--volume-range` opzione, come mostrato negli esempi seguenti.

Volume singolo: questo comando ripristina i dati codificati in cancellazione nel volume 0007 su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervallo di volumi: questo comando ripristina i dati codificati in cancellazione su tutti i volumi nell'intervallo 0004 A 0006 su un nodo di archiviazione 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 codificati in cancellazione nei volumi 000A , 000C , E 000E su un nodo di archiviazione 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` che identifica questo `repair_data` operazione. Usa questo `repair ID` per monitorare i progressi e i risultati del `repair_data` operazione. Non verrà restituito alcun altro feedback una volta completato il processo di

recupero.



Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. La riparazione verrà completata quando tutti i nodi saranno disponibili.

Riparazioni del monitor

Monitorare lo stato dei lavori di riparazione, a seconda che si utilizzino **dati replicati**, **dati con codice di cancellazione (EC)** o entrambi.

È inoltre possibile monitorare lo stato dei lavori di ripristino del volume in corso e visualizzare una cronologia dei lavori di ripristino completati in ["Responsabile della griglia"](#) .

Dati replicati

- Per ottenere una percentuale stimata di completamento per la riparazione replicata, aggiungere `show-replicated-repair-status` opzione al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Per determinare se le riparazioni sono state completate:
 - a. Selezionare **NODI > Nodo di archiviazione in riparazione > ILM**.
 - b. Esaminare gli attributi nella sezione Valutazione. Una volta completate le riparazioni, l'attributo **In attesa - Tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
 - a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - b. Selezionare **grid > Nodo di archiviazione in riparazione > LDR > Data Store**.
 - c. Utilizzare una combinazione dei seguenti attributi per determinare, nel miglior modo possibile, se le riparazioni replicate sono complete.



Potrebbero essere presenti incongruenze in Cassandra e le riparazioni non riuscite non vengono tracciate.

- **Riparazioni tentate (XRPA)**: utilizzare questo attributo per monitorare l'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di archiviazione tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo più lungo del periodo di scansione corrente (fornito dall'attributo **Periodo di scansione - Stimato**), significa che la scansione ILM non ha trovato oggetti ad alto rischio che necessitano di riparazione su alcun nodo.



Gli oggetti ad alto rischio sono oggetti che rischiano di andare completamente persi. Sono esclusi gli oggetti che non soddisfano la loro configurazione ILM.

- **Periodo di scansione - Stimato (XSCM)**: utilizzare questo attributo per stimare quando una modifica della policy verrà applicata agli oggetti precedentemente acquisiti. Se l'attributo **Riparazioni tentate** non aumenta per un periodo più lungo del periodo di scansione corrente, è probabile che siano state eseguite riparazioni replicate. Si noti che il periodo di scansione può variare. L'attributo **Periodo di scansione - Stimato (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione dei nodi. È possibile interrogare la cronologia degli attributi **Periodo di scansione - Stima** per la griglia per determinare un intervallo di tempo appropriato.

Dati con codice di cancellazione (EC)

Per monitorare la riparazione dei dati codificati in modo da cancellarli e riprovare eventuali richieste non riuscite:

1. Determinare lo stato delle riparazioni dei dati codificati tramite cancellazione:
 - Selezionare **SUPPORTO > Strumenti > Metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, seleziona **Panoramica EC** nella sezione Grafana. Consulta i dashboard **Tempo stimato per il completamento del lavoro EC in griglia** e **Percentuale completata del lavoro EC in griglia**.
 - Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` operazione:

```
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 eseguite in precedenza e attualmente.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

Questo comando riprova una riparazione del nodo non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Questo comando riprova una riparazione del volume non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Controllare lo stato di archiviazione dopo il ripristino del nodo di archiviazione dell'appliance

Dopo aver ripristinato un nodo di archiviazione dell'appliance, è necessario verificare che lo stato desiderato del nodo di archiviazione dell'appliance sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che il server del nodo di archiviazione viene riavviato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Il nodo di archiviazione è stato recuperato e il ripristino dei dati è completo.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Controllare i valori di **Recovered Storage Node > LDR > Storage > Storage State — Desired e Storage State — Current**.

Il valore di entrambi gli attributi dovrebbe essere Online.

3. Se lo Stato di archiviazione - Desiderato è impostato su Sola lettura, completare i seguenti passaggi:
 - a. Fare clic sulla scheda **Configurazione**.
 - b. Dall'elenco a discesa **Stato di archiviazione - Desiderato**, selezionare **Online**.
 - c. Fare clic su **Applica modifiche**.
 - d. Fare clic sulla scheda **Panoramica** e verificare che i valori di **Stato di archiviazione — Desiderato e Stato di archiviazione — Corrente** siano aggiornati su Online.

Ripristinare da un errore del volume di archiviazione in cui l'unità di sistema è intatta

Ripristinare da un errore del volume di archiviazione in cui l'unità di sistema è intatta

È necessario completare una serie di attività per ripristinare un nodo di archiviazione basato su software in cui uno o più volumi di archiviazione sul nodo di archiviazione sono guasti, ma l'unità di sistema è intatta. Se solo i volumi di archiviazione sono guasti, il nodo di archiviazione è ancora disponibile per il sistema StorageGRID .



Questa procedura di ripristino si applica solo ai nodi di archiviazione basati su software. Se i volumi di archiviazione si sono guastati su un nodo di archiviazione dell'appliance, utilizzare invece la procedura dell'appliance: ["Ripristina il nodo di archiviazione dell'appliance"](#) .

Questa procedura di recupero comprende le seguenti attività:

- ["Rivedere gli avvisi per il ripristino del volume di archiviazione"](#)
- ["Identificare e smontare i volumi di archiviazione non riusciti"](#)
- ["Recupera i volumi e ricostruisci il database Cassandra"](#)
- ["Ripristina i dati dell'oggetto"](#)
- ["Controllare lo stato di archiviazione"](#)

Avvisi per il ripristino del volume di archiviazione

Prima di ripristinare volumi di archiviazione non riusciti per un nodo di archiviazione, leggere i seguenti avvisi.

I volumi di archiviazione (o rangedb) in un nodo di archiviazione sono identificati da un numero esadecimale, noto come ID volume. Ad esempio, 0000 è il primo volume e 000F è il sedicesimo volume. Il primo archivio oggetti (volume 0) su ciascun nodo di archiviazione utilizza fino a 4 TB di spazio per i metadati degli oggetti e le operazioni del database Cassandra; tutto lo spazio rimanente su tale volume viene utilizzato per i dati degli oggetti. Tutti gli altri volumi di archiviazione vengono utilizzati esclusivamente per i dati degli 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 anche essere ricostruita nelle seguenti circostanze:

- Un nodo di archiviazione viene riportato online dopo essere stato offline per più di 15 giorni.
- L'unità di sistema e uno o più volumi di archiviazione si guastano e vengono ripristinati.

Quando Cassandra viene ricostruita, il sistema utilizza le informazioni provenienti da altri nodi di archiviazione. Se troppi nodi di archiviazione sono offline, alcuni dati Cassandra potrebbero non essere disponibili. Se Cassandra è stata ricostruita di recente, i dati di Cassandra potrebbero non essere ancora coerenti in tutta la griglia. La perdita di dati può verificarsi se Cassandra viene ricostruita quando troppi nodi di archiviazione sono offline o se due o più nodi di archiviazione vengono ricostruiti entro 15 giorni l'uno dall'altro.



Se più di un nodo di archiviazione è guasto (o è offline), contattare l'assistenza tecnica. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.



Se si tratta del secondo guasto del nodo di archiviazione in meno di 15 giorni dopo un guasto o un ripristino del nodo di archiviazione, contattare l'assistenza tecnica. La ricostruzione di Cassandra su due o più nodi di archiviazione entro 15 giorni può comportare la perdita di dati.



Se più di un nodo di archiviazione in un sito presenta un guasto, potrebbe essere necessaria una procedura di ripristino del sito. Vedere ["Come il supporto tecnico recupera un sito"](#).



Se le regole ILM sono configurate per archiviare solo una copia replicata e la copia esiste su un volume di archiviazione che ha subito un errore, non sarà possibile ripristinare l'oggetto.

Informazioni correlate

["Avvertenze e considerazioni per il ripristino del nodo della griglia"](#)

Identificare e smontare i volumi di archiviazione non riusciti

Quando si ripristina un nodo di archiviazione con volumi di archiviazione non riusciti, è necessario identificare e smontare i volumi non riusciti. È necessario verificare che solo i volumi di archiviazione non riusciti vengano riformattati come parte della procedura di ripristino.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

Informazioni su questo compito

È necessario ripristinare i volumi di archiviazione non riusciti il prima possibile.

Il primo passaggio del processo di ripristino consiste nel rilevare i volumi che si sono staccati, che devono essere smontati o che presentano errori di I/O. Se i volumi danneggiati sono ancora collegati ma hanno un file system danneggiato in modo casuale, il sistema potrebbe non rilevare alcun danneggiamento nelle parti inutilizzate o non allocate del disco.



È necessario completare questa procedura prima di eseguire passaggi manuali per ripristinare i volumi, ad esempio aggiungere o ricollegare i dischi, arrestare il nodo, avviare il nodo o riavviare. Altrimenti, quando esegui il `reformat_storage_block_devices.rb` script, potresti riscontrare un errore del file system che causa il blocco o il fallimento dello script.



Riparare l'hardware e collegare correttamente i dischi prima di eseguire il `reboot` comando.



Identificare attentamente i volumi di archiviazione non riusciti. Utilizzerai queste informazioni per verificare quali volumi devono essere riformattati. Dopo aver riformattato un volume, i dati in esso contenuti non possono essere recuperati.

Per ripristinare correttamente i volumi di archiviazione non riusciti, è necessario conoscere sia i nomi dei dispositivi dei volumi di archiviazione non riusciti sia i relativi ID volume.

Durante l'installazione, a ciascun dispositivo di archiviazione viene assegnato un identificatore univoco universale (UUID) del file system e viene montato in una directory `rangedb` sul nodo di archiviazione utilizzando tale UUID 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 la dimensione del volume montato vengono

visualizzati in Grid Manager.

Nell'esempio seguente, dispositivo `/dev/sdc` ha una dimensione del 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` nell'`/etc/fstab` file:

var

local

rangedb

0

1

2

/dev/sdc

4396 GB

/dev/sdd

4396 GB

/dev/sde

4396 GB

/dev/sdc

/etc/fstab file

ext3

errors=remount-ro,barri

/dev/sdd

/var/local

ext3

errors=remount-ro,barri

/dev/sde

swap

swap

defaults

0

proc

/proc

proc

defaults

0

sysfs

/sys

sysfs

noauto

0

debugfs

/sys/kernel/debug

debugfs

noauto

0

devpts

/dev/pts

devpts

mode=0620,gid=5

0

/dev/td0

/media/floppy

auto

noauto,user,sync

0

/dev/cdrom

/cdrom iso9660 ro,noauto 0 0

/dev/disk/by-uuid/384c4687-8811-47a7-9700-7b31b495a0b8

/var/local/mysql_ibda

/dev/mapper/fsgvg-fsglv

/fsg xfs daapi,mtpt=/fsg,noalign,nobarrier,ik

/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba

/var/local/rangedb/0

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.53 GB	655,360	559,513	Unknown
/var/local	cyloc	Online	96.6 GB	92.8 GB	94,369,792	94,369,445	Unknown
/var/local/rangedb/0	sdc	Online	4,396 GB	4,379 GB	858,993,408	858,983,455	Unavailable
/var/local/rangedb/1	sdd	Online	4,396 GB	4,362 GB	858,993,408	858,973,530	Unavailable
/var/local/rangedb/2	sde	Online	4,396 GB	4,370 GB	858,993,408	858,982,305	Unavailable

Passi

1. Completare i seguenti passaggi per registrare i volumi di archiviazione non riusciti e i relativi nomi di dispositivo:
- a. Selezionare **SUPPORTO > Strumenti > Topologia griglia.**

b. Selezionare **sito > nodo di archiviazione non riuscito > LDR > Archiviazione > 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 di archiviazione non riuscito > SSM > Risorse > Panoramica > Principale**. Determinare il punto di montaggio e la dimensione del volume di ciascun volume di archiviazione non riuscito 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 oggetti con ID 0000 corrisponde a `/var/local/rangedb/0` con nome dispositivo `sdc` e dimensione pari a 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. Accedi al nodo di archiviazione non riuscito:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

3. Eseguire lo script seguente per smontare un volume di archiviazione non riuscito:

```
sn-unmount-volume object_store_ID
```

IL `object_store_ID` è l'ID del volume di archiviazione non riuscito. Ad esempio, specificare 0 nel comando per un archivio oggetti con ID 0000.

4. Se richiesto, premere **y** per interrompere il servizio Cassandra in base al volume di archiviazione 0.



Se il servizio Cassandra è già stato arrestato, non verrà visualizzato alcun messaggio. Il servizio Cassandra è interrotto 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 verrà smontato. Vengono visualizzati messaggi che indicano ogni fase del processo. Il messaggio finale indica che il volume è smontato.

5. Se lo smontaggio fallisce perché il volume è occupato, è possibile forzare lo smontaggio utilizzando `--use-umountof` opzione:



Forzare uno smontaggio utilizzando `--use-umountof` L'opzione potrebbe causare un comportamento imprevisto o un arresto anomalo 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
```

Recupera i volumi di archiviazione non riusciti e ricostruisci il database Cassandra

È necessario eseguire uno script che riformatti e rimonti l'archiviazione sui volumi di archiviazione non riusciti e ricostruisca il database Cassandra sul nodo di archiviazione se il sistema determina che è necessario.

Prima di iniziare

- Tu hai il `Passwords.txt` file.
- Le unità di sistema sul server sono intatte.
- La causa del guasto è stata individuata e, se necessario, è già stato acquistato un hardware di archiviazione sostitutivo.
- La dimensione totale dello spazio di archiviazione sostitutivo è la stessa dell'originale.
- Hai verificato che non è in corso la dismissione di un nodo di archiviazione oppure hai sospeso la procedura di dismissione del nodo. (Nel Grid Manager, seleziona **MANUTENZIONE** > **Attività** > **Dismissione**.)
- Hai verificato che non è in corso un'espansione. (Nel Grid Manager, seleziona **MANUTENZIONE** > **Attività** > **Espansione**.)
- Hai ["esaminati gli avvisi sul ripristino del volume di archiviazione"](#) .

Passi

1. Se necessario, sostituire l'archiviazione fisica o virtuale non riuscita associata ai volumi di archiviazione non riusciti identificati e smontati in precedenza.

Non rimontare i volumi in questo passaggio. Lo spazio di archiviazione viene rimontato e aggiunto a `/etc/fstab` in una fase successiva.

2. Nel Grid Manager, vai su **NODI** > **appliance Storage Node** > **Hardware**. Nella sezione StorageGRID Appliance della pagina, verificare che la modalità Storage RAID sia integra.
3. Accedi al nodo di archiviazione non riuscito:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da \$ A # .

4. Utilizzare un editor di testo (vi o vim) per eliminare i volumi non riusciti dal `/etc/fstab` file e quindi salvarlo.



Commentare un volume non riuscito nel `/etc/fstab` il file non è sufficiente. Il volume deve essere eliminato da `fstab` poiché il processo di recupero verifica che tutte le linee nel `fstab` i file corrispondono ai file system montati.

5. Riformattare tutti i volumi di archiviazione non riusciti e ricostruire il database Cassandra, se necessario. Inserisci: `reformat_storage_block_devices.rb`

- Quando il volume di archiviazione 0 viene smontato, prompt e messaggi indicheranno che il servizio Cassandra è in fase di arresto.
- Se necessario, ti verrà chiesto di ricostruire il database Cassandra.
 - Rivedere gli avvertimenti. Se nessuna di queste soluzioni è applicabile, ricostruire il database Cassandra. Inserisci: **y**
 - Se più di un nodo di archiviazione è offline o se un altro nodo di archiviazione è stato ricostruito negli ultimi 15 giorni. Inserisci: **n**

Lo script uscirà senza ricostruire Cassandra. Contattare l'assistenza tecnica.

- Per ogni unità `rangedb` sul nodo di archiviazione, quando ti viene chiesto: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, inserisci una delle seguenti risposte:
 - **y** per riformattare un'unità che presentava errori. Ciò riformatta il volume di archiviazione e aggiunge il volume di archiviazione riformattato al `/etc/fstab` file.
 - **n** se l'unità non contiene errori e non si desidera riformattarla.



Selezionando **n** si esce dallo script. Montare l'unità (se si ritiene che i dati sull'unità debbano essere conservati e l'unità è stata smontata per errore) oppure rimuoverla. Quindi, esegui il `reformat_storage_block_devices.rb` comando di nuovo.



Alcune procedure di ripristino StorageGRID utilizzano Reaper per gestire le riparazioni di Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Potresti notare che nell'output dello script viene menzionato "reaper" o "Cassandra repair". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

Nell'esempio seguente, l'unità `/dev/sdf` deve essere riformattato e Cassandra non ha avuto bisogno di essere ricostruita:

```
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 b951bfcf-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.
```

Dopo che i volumi di archiviazione sono stati riformattati e rimontati e le operazioni Cassandra necessarie sono state completate, è possibile ["ripristinare i dati degli oggetti utilizzando Grid Manager"](#) .

Ripristina i dati dell'oggetto nel volume di archiviazione in cui l'unità di sistema è intatta

Dopo aver ripristinato un volume di archiviazione su un nodo di archiviazione in cui l'unità di sistema è intatta, è possibile ripristinare i dati degli oggetti replicati o con codice di cancellazione che sono andati persi quando il volume di archiviazione si è guastato.

Quale procedura dovrei usare?

Se possibile, ripristinare i dati dell'oggetto utilizzando la pagina **Ripristino volume** in Grid Manager.

- Se i volumi sono elencati in **MANUTENZIONE > Ripristino volume > Nodi da ripristinare**, ripristinare i dati dell'oggetto utilizzando ["Pagina di ripristino del volume in Grid Manager"](#) .
- Se i volumi non sono elencati in **MANUTENZIONE > Ripristino volume > Nodi da ripristinare**, seguire i passaggi seguenti per utilizzare `repair-data` script per ripristinare i dati dell'oggetto.

Se il nodo di archiviazione recuperato contiene meno volumi rispetto al nodo che sta sostituendo, è necessario utilizzare `repair-data` sceneggiatura.



Lo script `repair-data` è obsoleto e verrà rimosso in una versione futura. Quando possibile, utilizzare il ["Procedura di ripristino del volume in Grid Manager"](#) .

Utilizzare il `repair-data` script per ripristinare i dati dell'oggetto

Prima di iniziare

- Hai confermato che il nodo di archiviazione recuperato ha uno stato di connessione **Connesso***  nella scheda ***NODI > Panoramica** nel Grid Manager.

Informazioni su questo compito

I dati degli oggetti possono essere ripristinati da altri nodi di archiviazione o da un pool di archiviazione cloud, presupponendo che le regole ILM della griglia siano state configurate in modo che siano disponibili copie degli oggetti.

Notare quanto segue:

- Se una regola ILM è stata configurata per archiviare solo una copia replicata e tale copia esisteva su un volume di archiviazione che ha generato un errore, non sarà possibile ripristinare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID deve inviare più richieste all'endpoint del Cloud Storage Pool per ripristinare i dati dell'oggetto. Prima di eseguire questa procedura, contattare l'assistenza tecnica per ottenere assistenza nella stima dei tempi di ripristino e dei costi associati.

Informazioni su `repair-data` sceneggiatura

Per ripristinare i dati dell'oggetto, eseguire il comando `repair-data` sceneggiatura. Questo script avvia il processo di ripristino dei dati dell'oggetto e funziona con la scansione ILM per garantire che le regole ILM vengano rispettate.

Seleziona **Dati replicati** o **Dati con codice di cancellazione (EC)** qui sotto per conoscere le diverse opzioni per `repair-data` script, a seconda che si stiano ripristinando dati replicati o dati con codice di cancellazione. Se è necessario ripristinare entrambi i tipi di dati, è necessario eseguire entrambi i set di comandi.



Per maggiori informazioni sul `repair-data` script, inserisci `repair-data --help` dalla riga di comando del nodo di amministrazione primario.



Lo script `repair-data` è obsoleto e verrà rimosso in una versione futura. Quando possibile, utilizzare il "[Procedura di ripristino del volume in Grid Manager](#)".

Dati replicati

Sono disponibili due comandi per ripristinare i dati replicati, a seconda che sia necessario riparare l'intero nodo o solo determinati volumi sul nodo:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

È possibile monitorare le riparazioni dei dati replicati con questo comando:

```
repair-data show-replicated-repair-status
```

Dati con codice di cancellazione (EC)

Sono disponibili due comandi per ripristinare i dati codificati in modo da essere cancellati, 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 monitorare le riparazioni dei dati codificati in modo da cancellarli con questo comando:

```
repair-data show-ec-repair-status
```



Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. Tuttavia, se non è possibile recuperare tutti i dati codificati in modo da cancellarli, la riparazione non può essere completata. La riparazione verrà completata quando tutti i nodi saranno disponibili.



Il lavoro di riparazione EC riserva temporaneamente una grande quantità di spazio di archiviazione. Potrebbero essere attivati avvisi di archiviazione, ma il problema si risolverà al termine della riparazione. Se non c'è abbastanza spazio per la prenotazione, il lavoro di riparazione EC fallirà. Le prenotazioni di archiviazione vengono rilasciate al termine del processo di riparazione EC, indipendentemente dal fatto che il processo sia fallito o riuscito.

Trova il nome host per il nodo di archiviazione

1. Accedi al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Utilizzare il `/etc/hosts` file per trovare il nome host del nodo di archiviazione per i volumi di archiviazione ripristinati. Per visualizzare un elenco di tutti i nodi nella griglia, immettere quanto segue: `cat`

/etc/hosts .

Ripara i dati se tutti i volumi sono falliti

Se tutti i volumi di archiviazione sono guasti, riparare l'intero nodo. Seguire le istruzioni per i **dati replicati**, i **dati con codice di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codice di cancellazione (EC) o entrambi.

Se solo alcuni volumi sono falliti, vai a [Riparare i dati se solo alcuni volumi sono falliti](#) .



Non puoi correre `repair-data` operazioni per più di un nodo contemporaneamente. Per recuperare più nodi, contattare l'assistenza tecnica.

Dati replicati

Se la griglia include dati replicati, utilizzare `repair-data start-replicated-node-repair` comando con il `--nodes` opzione, dove `--nodes` è il nome host (nome del sistema) per riparare l'intero nodo di archiviazione.

Questo comando ripara i dati replicati su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Quando i dati degli oggetti vengono ripristinati, viene attivato l'avviso **Oggetti persi** se il sistema StorageGRID non riesce a individuare i dati degli oggetti replicati. Gli avvisi potrebbero essere attivati sui nodi di archiviazione in tutto il sistema. Dovresti determinare la causa della perdita e se è possibile un recupero. Vedere "[Indagare sugli oggetti smarriti](#)" .

Dati con codice di cancellazione (EC)

Se la griglia contiene dati con codice di cancellazione, utilizzare `repair-data start-ec-node-repair` comando con il `--nodes` opzione, dove `--nodes` è il nome host (nome del sistema) per riparare l'intero nodo di archiviazione.

Questo comando ripara i dati codificati in modo da essere cancellati su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'operazione restituisce un valore univoco `repair ID` che identifica questo `repair_data` operazione. Usa questo `repair ID` per monitorare i progressi e i risultati del `repair_data` operazione. Non verrà restituito alcun altro feedback una volta completato il processo di recupero.

Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. La riparazione verrà completata quando tutti i nodi saranno disponibili.

Riparare i dati se solo alcuni volumi sono falliti

Se solo alcuni volumi sono guasti, riparare i volumi interessati. Seguire le istruzioni per i **dati replicati**, i **dati con codice di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codice di cancellazione (EC) o entrambi.

Se tutti i volumi sono falliti, vai a [Ripara i dati se tutti i volumi sono falliti](#) .

Immettere gli ID del volume in formato esadecimale. Per esempio, 0000 è il primo volume e 000F è il sedicesimo volume. È possibile specificare un volume, un intervallo di volumi o più volumi non in sequenza.

Tutti i volumi devono trovarsi sullo stesso nodo di archiviazione. Se è necessario ripristinare volumi per più di un nodo di archiviazione, contattare l'assistenza tecnica.

Dati replicati

Se la griglia contiene dati replicati, utilizzare `start-replicated-volume-repair` comando con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi aggiungere o il `--volumes` O `--volume-range` opzione, come mostrato negli esempi seguenti.

Volume singolo: questo comando ripristina i dati replicati nel volume 0002 su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervallo di volumi: questo comando ripristina i dati replicati su tutti i volumi nell'intervallo 0003 A 0009 su un nodo di archiviazione 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 archiviazione denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Quando i dati degli oggetti vengono ripristinati, viene attivato l'avviso **Oggetti persi** se il sistema StorageGRID non riesce a individuare i dati degli oggetti replicati. Gli avvisi potrebbero essere attivati sui nodi di archiviazione in tutto il sistema. Prendere nota della descrizione dell'avviso e delle azioni consigliate per determinare la causa della perdita e se è possibile un recupero.

Dati con codice di cancellazione (EC)

Se la griglia contiene dati con codice di cancellazione, utilizzare `start-ec-volume-repair` comando con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi aggiungere o il `--volumes` O `--volume-range` opzione, come mostrato negli esempi seguenti.

Volume singolo: questo comando ripristina i dati codificati in cancellazione nel volume 0007 su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervallo di volumi: questo comando ripristina i dati codificati in cancellazione su tutti i volumi nell'intervallo 0004 A 0006 su un nodo di archiviazione 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 codificati in cancellazione nei volumi 000A , 000C , E 000E su un nodo di archiviazione 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` che identifica questo `repair_data` operazione. Usa questo `repair ID` per monitorare i progressi e i risultati del `repair_data` operazione. Non verrà restituito alcun altro feedback una volta completato il processo di

recupero.



Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. La riparazione verrà completata quando tutti i nodi saranno disponibili.

Riparazioni del monitor

Monitorare lo stato dei lavori di riparazione, a seconda che si utilizzino **dati replicati**, **dati con codice di cancellazione (EC)** o entrambi.

È inoltre possibile monitorare lo stato dei lavori di ripristino del volume in corso e visualizzare una cronologia dei lavori di ripristino completati in "[Responsabile della griglia](#)".

Dati replicati

- Per ottenere una percentuale stimata di completamento per la riparazione replicata, aggiungere `show-replicated-repair-status` opzione al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Per determinare se le riparazioni sono state completate:
 - a. Selezionare **NODI > Nodo di archiviazione in riparazione > ILM**.
 - b. Esaminare gli attributi nella sezione Valutazione. Una volta completate le riparazioni, l'attributo **In attesa - Tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
 - a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - b. Selezionare **grid > Nodo di archiviazione in riparazione > LDR > Data Store**.
 - c. Utilizzare una combinazione dei seguenti attributi per determinare, nel miglior modo possibile, se le riparazioni replicate sono complete.



Potrebbero essere presenti incongruenze in Cassandra e le riparazioni non riuscite non vengono tracciate.

- **Riparazioni tentate (XRPA)**: utilizzare questo attributo per monitorare l'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di archiviazione tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo più lungo del periodo di scansione corrente (fornito dall'attributo **Periodo di scansione - Stimato**), significa che la scansione ILM non ha trovato oggetti ad alto rischio che necessitano di riparazione su alcun nodo.



Gli oggetti ad alto rischio sono oggetti che rischiano di andare completamente persi. Sono esclusi gli oggetti che non soddisfano la loro configurazione ILM.

- **Periodo di scansione - Stimato (XSCM)**: utilizzare questo attributo per stimare quando una modifica della policy verrà applicata agli oggetti precedentemente acquisiti. Se l'attributo **Riparazioni tentate** non aumenta per un periodo più lungo del periodo di scansione corrente, è probabile che siano state eseguite riparazioni replicate. Si noti che il periodo di scansione può variare. L'attributo **Periodo di scansione - Stimato (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione dei nodi. È possibile interrogare la cronologia degli attributi **Periodo di scansione - Stima** per la griglia per determinare un intervallo di tempo appropriato.

Dati con codice di cancellazione (EC)

Per monitorare la riparazione dei dati codificati in modo da cancellarli e riprovare eventuali richieste non riuscite:

1. Determinare lo stato delle riparazioni dei dati codificati tramite cancellazione:
 - Selezionare **SUPPORTO > Strumenti > Metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, seleziona **Panoramica EC** nella sezione Grafana. Consulta i dashboard **Tempo stimato per il completamento del lavoro EC in griglia** e **Percentuale completata del lavoro EC in griglia**.
 - Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` operazione:

```
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 eseguite in precedenza e attualmente.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

Questo comando riprova una riparazione del nodo non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Questo comando riprova una riparazione del volume non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Controllare lo stato di archiviazione dopo il ripristino dei volumi di archiviazione

Dopo aver ripristinato i volumi di archiviazione, è necessario verificare che lo stato desiderato del nodo di archiviazione sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che il server del nodo di archiviazione viene riavviato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Il nodo di archiviazione è stato recuperato e il ripristino dei dati è completo.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Controllare i valori di **Recovered Storage Node > LDR > Storage > Storage State — Desired e Storage State — Current**.

Il valore di entrambi gli attributi dovrebbe essere Online.

3. Se lo Stato di archiviazione - Desiderato è impostato su Sola lettura, completare i seguenti passaggi:
 - a. Fare clic sulla scheda **Configurazione**.
 - b. Dall'elenco a discesa **Stato di archiviazione - Desiderato**, selezionare **Online**.
 - c. Fare clic su **Applica modifiche**.
 - d. Fare clic sulla scheda **Panoramica** e verificare che i valori di **Stato di archiviazione — Desiderato e Stato di archiviazione — Corrente** siano aggiornati su Online.

Ripristino da un errore dell'unità di sistema

Avvisi per il ripristino dell'unità di sistema del nodo di archiviazione

Prima di ripristinare un'unità di sistema guasta di un nodo di archiviazione, rivedere le informazioni generali ["avvertenze e considerazioni per il ripristino del nodo della griglia"](#) e le seguenti avvertenze specifiche.

I nodi di archiviazione dispongono di un database Cassandra che include metadati degli oggetti. Il database Cassandra potrebbe essere ricostruito nelle seguenti circostanze:

- Un nodo di archiviazione viene riportato online dopo essere stato offline per più di 15 giorni.
- Un volume di archiviazione è guasto ed è stato recuperato.
- L'unità di sistema e uno o più volumi di archiviazione si guastano e vengono ripristinati.

Quando Cassandra viene ricostruita, il sistema utilizza le informazioni provenienti da altri nodi di archiviazione. Se troppi nodi di archiviazione sono offline, alcuni dati Cassandra potrebbero non essere disponibili. Se Cassandra è stata ricostruita di recente, i dati di Cassandra potrebbero non essere ancora coerenti in tutta la griglia. La perdita di dati può verificarsi se Cassandra viene ricostruita quando troppi nodi di archiviazione sono offline o se due o più nodi di archiviazione vengono ricostruiti entro 15 giorni l'uno dall'altro.



Se più di un nodo di archiviazione è guasto (o è offline), contattare l'assistenza tecnica. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.



Se si tratta del secondo guasto del nodo di archiviazione in meno di 15 giorni dopo un guasto o un ripristino del nodo di archiviazione, contattare l'assistenza tecnica. La ricostruzione di Cassandra su due o più nodi di archiviazione entro 15 giorni può comportare la perdita di dati.



Se più di un nodo di archiviazione in un sito presenta un guasto, potrebbe essere necessaria una procedura di ripristino del sito. Vedere ["Come il supporto tecnico recupera un sito"](#).



Se questo nodo di archiviazione è in modalità di manutenzione di sola lettura per consentire il recupero di oggetti da parte di un altro nodo di archiviazione con volumi di archiviazione non riusciti, ripristinare i volumi sul nodo di archiviazione con volumi di archiviazione non riusciti prima di ripristinare questo nodo di archiviazione non riuscito. Vedi le istruzioni per ["ripristino da un errore del volume di archiviazione in cui l'unità di sistema è intatta"](#).



Se le regole ILM sono configurate per archiviare solo una copia replicata e la copia esiste su un volume di archiviazione che ha subito un errore, non sarà possibile ripristinare l'oggetto.

Sostituisci il nodo di archiviazione

Se l'unità di sistema è guasta, è necessario prima sostituire il nodo di archiviazione.

È necessario selezionare la procedura di sostituzione dei nodi per la propria piattaforma. I passaggi per sostituire un nodo sono gli stessi per tutti i tipi di nodi della griglia.



Questa procedura si applica solo ai nodi di archiviazione basati su software. È necessario seguire una procedura diversa per ["ripristinare un nodo di archiviazione dell'appliance"](#).

Linux: Se non sei sicuro che l'unità di sistema sia guasta, segui le istruzioni per sostituire il nodo e determinare quali passaggi di ripristino sono necessari.

Piattaforma	Procedura
VMware	"Sostituisci un nodo VMware"
Linux	"Sostituisci un nodo Linux"
OpenStack	I file del disco della macchina virtuale e gli script forniti da NetApp per OpenStack non sono più supportati per le operazioni di ripristino. Se devi ripristinare un nodo in esecuzione in una distribuzione OpenStack, scarica i file per il tuo sistema operativo Linux. Quindi, seguire la procedura per "sostituzione di un nodo Linux" .

Selezionare Avvia ripristino per configurare il nodo di archiviazione

Dopo aver sostituito un nodo di archiviazione, è necessario selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo in sostituzione del nodo guasto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).
- Hai la passphrase di provisioning.
- Hai distribuito e configurato il nodo sostitutivo.
- Hai la data di inizio di tutti i lavori di riparazione per i dati codificati in modo da essere cancellati.
- Hai verificato che il nodo di archiviazione non è stato ricostruito negli ultimi 15 giorni.

Informazioni su questo compito

Se il nodo di archiviazione è installato come contenitore su un host Linux, è necessario eseguire questo passaggio solo se si verifica una delle seguenti condizioni:

- Dovevi usare il `--force` flag per importare il nodo, oppure hai emesso `storagegrid node force-recovery node-name`
- Era necessario reinstallare l'intero nodo oppure ripristinare `/var/local`.

Passi

1. Da Grid Manager, seleziona **MANUTENZIONE > Attività > Ripristino**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Nodi in sospeso.

I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionarne uno finché non è stato reinstallato e non è pronto per il ripristino.

3. Immettere la **Passphrase di provisioning**.
4. Fare clic su **Avvia ripristino**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitorare l'avanzamento del ripristino nella tabella Nodo griglia in fase di ripristino.



Mentre la procedura di ripristino è in esecuzione, puoi fare clic su **Reimposta** per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che se si reimposta la procedura, il nodo verrà lasciato in uno stato indeterminato.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware:** Elimina il nodo della griglia virtuale distribuito. Quindi, quando sei pronto per riavviare il ripristino, ridistribuisce 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 di passaggi manuali", passare a ["Rimontare e riformattare i volumi di archiviazione \(passaggi manuali\)"](#).

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset

Rimontare e riformattare i volumi di archiviazione (passaggi manuali)

È necessario eseguire manualmente due script per rimontare i volumi di archiviazione conservati e riformattare eventuali volumi di archiviazione non riusciti. Il primo script rimonta i volumi formattati correttamente come volumi di archiviazione StorageGRID . Il secondo script riformatta tutti i volumi non montati, ricostruisce Cassandra, se necessario, e avvia i servizi.

Prima di iniziare

- Hai già sostituito l'hardware per tutti i volumi di archiviazione guasti che sai che necessitano di essere sostituiti.

Esecuzione del `sn-remount-volumes` potrebbe aiutarti a identificare ulteriori volumi di archiviazione non riusciti.

- Hai verificato che non è in corso la dismissione di un nodo di archiviazione oppure hai sospeso la procedura di dismissione del nodo. (Nel Grid Manager, seleziona **MANUTENZIONE > Attività > Dismissione.**)
- Hai verificato che non è in corso un'espansione. (Nel Grid Manager, seleziona **MANUTENZIONE > Attività > Espansione.**)
- Hai [esaminati gli avvisi per il ripristino dell'unità di sistema del nodo di archiviazione](#) .



Contattare l'assistenza tecnica se più di un nodo di archiviazione è offline o se un nodo di archiviazione in questa griglia è stato ricostruito negli ultimi 15 giorni. Non eseguire il `sn-recovery-postinstall.sh` sceneggiatura. La ricostruzione di Cassandra su due o più nodi di archiviazione a distanza di 15 giorni l'uno dall'altro potrebbe comportare la perdita di dati.

Informazioni su questo compito

Per completare questa procedura, è necessario eseguire le seguenti attività di alto livello:

- Accedere al nodo di archiviazione recuperato.
- Esegui il `sn-remount-volumes` script per rimontare i volumi di archiviazione formattati correttamente. Quando questo script viene eseguito, esegue le seguenti operazioni:
 - Monta e smonta ciascun volume di archiviazione per riprodurre il journal XFS.
 - Esegue un controllo di coerenza del file XFS.
 - Se il file system è coerente, determina se il volume di archiviazione è un volume di archiviazione StorageGRID formattato correttamente.

- Se il volume di archiviazione è formattato correttamente, rimonta il volume di archiviazione. Tutti i dati esistenti sul volume rimangono intatti.
- Esaminare l'output dello script e risolvere eventuali problemi.
- Esegui il `sn-recovery-postinstall.sh` sceneggiatura. Quando questo script viene eseguito, esegue le seguenti operazioni.



Non riavviare un nodo di archiviazione durante il ripristino prima dell'esecuzione `sn-recovery-postinstall.sh` per riformattare i volumi di archiviazione danneggiati e ripristinare i metadati degli oggetti. Riavvio del nodo di archiviazione prima `sn-recovery-postinstall.sh` completa causa errori per i servizi che tentano di avviarsi e fa sì che i nodi dell'appliance StorageGRID escano dalla modalità di manutenzione. Vedi il passaggio per [script post-installazione](#).

- Riformatta tutti i volumi di archiviazione che `sn-remount-volumes` script che non è stato possibile montare o che sono stati trovati formattati in modo non corretto.



Se un volume di archiviazione viene riformattato, tutti i dati presenti su quel volume andranno persi. È necessario eseguire una procedura aggiuntiva per ripristinare i dati degli oggetti da altre posizioni nella griglia, presupponendo che le regole ILM siano state configurate per archiviare più di una copia dell'oggetto.

- Se necessario, ricostruisce il database Cassandra sul nodo.
- Avvia i servizi sul nodo di archiviazione.

Passi

1. Accedi al nodo di archiviazione recuperato:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Eseguire il primo script per rimontare tutti i volumi di archiviazione formattati correttamente.



Se tutti i volumi di archiviazione sono nuovi e devono essere formattati, oppure se tutti i volumi di archiviazione sono guasti, è possibile saltare questo passaggio ed eseguire il secondo script per riformattare tutti i volumi di archiviazione non montati.

- Esegui lo script: `sn-remount-volumes`

L'esecuzione di questo script su volumi di archiviazione contenenti dati potrebbe richiedere ore.

- Durante l'esecuzione dello script, rivedere l'output e rispondere a eventuali richieste.



Se necessario, è possibile utilizzare il `tail -f` comando per monitorare il contenuto del file di registro dello script (`/var/local/log/sn-remount-volumes.log`). Il file di registro 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 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 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 archiviazione è stato rimontato correttamente e tre volumi di archiviazione presentavano errori.

- `/dev/sdb` ha superato il controllo di coerenza del file system XFS e aveva una struttura del volume valida, quindi è stato rimontato correttamente. I dati sui dispositivi rimontati dallo script vengono conservati.
- `/dev/sdc` il controllo di coerenza del file system XFS non è riuscito perché il volume di archiviazione era nuovo o danneggiato.

- `/dev/sdd` non è stato possibile montarlo perché il disco non è stato inizializzato o il superblocco del disco è danneggiato. Quando lo script non riesce a montare un volume di archiviazione, chiede se si desidera eseguire il controllo di coerenza del file system.
 - Se il volume di archiviazione è collegato a un nuovo disco, rispondere **N** al prompt. Non è necessario controllare il file system su un nuovo disco.
 - Se il volume di archiviazione è collegato a un disco esistente, rispondere **Y** al prompt. È possibile utilizzare i risultati del controllo del file system per determinare l'origine del danneggiamento. I risultati vengono salvati nel `/var/local/log/sn-remount-volumes.log` file di registro.
- `/dev/sde` ha superato il controllo di coerenza del file system XFS e aveva una struttura del volume valida; tuttavia, l'ID del nodo LDR nel file `volID` non corrispondeva all'ID per questo nodo di archiviazione (il `configured LDR noid` visualizzato in alto). Questo messaggio indica che questo volume appartiene a un altro nodo di archiviazione.

3. Esaminare l'output dello script e risolvere eventuali problemi.



Se un volume di archiviazione 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 del `sn-recovery-postinstall.sh` sceneggiatura su questi volumi.

- Verificare che i risultati includano una voce per tutti i volumi previsti. Se non sono elencati volumi, eseguire nuovamente lo script.
- Esaminare i messaggi per tutti i dispositivi montati. Assicurarsi che non vi siano errori che indicano che un volume di archiviazione non appartiene a questo nodo di archiviazione.

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 archiviazione viene segnalato come appartenente a un altro nodo di archiviazione, contattare l'assistenza tecnica. Se esegui il `sn-recovery-postinstall.sh` script, il volume di archiviazione verrà riformattato, il che potrebbe causare la perdita di dati.

- Se non è stato possibile montare un dispositivo di archiviazione, prendere nota del nome del dispositivo e ripararlo o sostituirlo.



È necessario riparare o sostituire tutti i dispositivi di archiviazione che non è stato possibile montare.

Utilizzerai il nome del dispositivo per cercare l'ID del volume, che è un input obbligatorio quando esegui il `repair-data` script per ripristinare i dati dell'oggetto nel volume (procedura successiva).

- Dopo aver riparato o sostituito tutti i dispositivi non montabili, eseguire il `sn-remount-volumes` script di nuovo per confermare che tutti i volumi di archiviazione che possono essere rimontati siano stati rimontati.



Se un volume di archiviazione non può essere montato o non è formattato correttamente e si procede con il passaggio successivo, il volume e tutti i dati in esso contenuti verranno eliminati. Se si dispone di due copie dei dati dell'oggetto, sarà disponibile una sola copia finché non si completa la procedura successiva (ripristino dei dati dell'oggetto).



Non eseguire il `sn-recovery-postinstall.sh` script se ritieni che i dati rimanenti su un volume di archiviazione non riuscito non possano essere ricostruiti da nessun'altra parte nella griglia (ad esempio, se la policy ILM utilizza una regola che crea una sola copia o se i volumi sono falliti su più nodi). Contatta invece l'assistenza tecnica per scoprire come recuperare i tuoi dati.

4. Esegui il `sn-recovery-postinstall.sh` sceneggiatura: `sn-recovery-postinstall.sh`

Questo script riformatta tutti i volumi di archiviazione che non è stato possibile montare o che sono stati trovati formattati in modo non corretto; ricostruisce il database Cassandra sul nodo, se necessario; e avvia i servizi sul nodo di archiviazione.

Siate consapevoli di quanto segue:

- L'esecuzione dello script potrebbe richiedere ore.
- In generale, è consigliabile lasciare inalterata la sessione SSH mentre lo script è in esecuzione.
- Non premere **Ctrl+C** mentre la sessione SSH è attiva.
- Lo script verrà eseguito in background se si verifica un'interruzione della rete e termina la sessione SSH, ma è possibile visualizzare l'avanzamento dalla pagina Ripristino.
- Se il nodo di archiviazione utilizza il servizio RSM, lo script potrebbe bloccarsi 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 archiviazione che includono il servizio ADC.



Alcune procedure di ripristino StorageGRID utilizzano Reaper per gestire le riparazioni di Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Potresti notare che nell'output dello script viene menzionato "reaper" o "Cassandra repair". 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 il `sn-recovery-postinstall.sh` quando lo script viene eseguito, monitorare la pagina Ripristino in Grid Manager.

La barra di avanzamento e la colonna Fase nella pagina Ripristino forniscono uno stato di alto livello del `sn-recovery-postinstall.sh` sceneggiatura.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

6. Dopo il `sn-recovery-postinstall.sh` Una volta che lo script ha avviato i servizi sul nodo, è possibile ripristinare i dati dell'oggetto su qualsiasi volume di archiviazione 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 l'archiviazione degli oggetti rispetto al nodo originale, è necessario [ripristinare manualmente i dati dell'oggetto](#) utilizzando il `repair-data` sceneggiatura. Se si verifica uno di questi casi, rispondi `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 archiviazione (errore dell'unità di sistema)

Dopo aver ripristinato i volumi di archiviazione per un nodo di archiviazione non appliance, è possibile ripristinare i dati degli oggetti replicati o codificati per la cancellazione che sono andati persi a causa del guasto del nodo di archiviazione.

Quale procedura dovrei usare?

Se possibile, ripristinare i dati dell'oggetto utilizzando la pagina **Ripristino volume** in Grid Manager.

- Se i volumi sono elencati in **MANUTENZIONE > Ripristino volume > Nodi da ripristinare**, ripristinare i dati dell'oggetto utilizzando [Pagina di ripristino del volume in Grid Manager](#) .

- Se i volumi non sono elencati in **MANUTENZIONE > Ripristino volume > Nodi da ripristinare**, seguire i passaggi seguenti per utilizzare `repair-data` script per ripristinare i dati dell'oggetto.

Se il nodo di archiviazione recuperato contiene meno volumi rispetto al nodo che sta sostituendo, è necessario utilizzare `repair-data` sceneggiatura.



Lo script `repair-data` è obsoleto e verrà rimosso in una versione futura. Quando possibile, utilizzare il "[Procedura di ripristino del volume in Grid Manager](#)".

Utilizzare il `repair-data` script per ripristinare i dati dell'oggetto

Prima di iniziare

- Hai confermato che il nodo di archiviazione recuperato ha uno stato di connessione **Connesso***  nella scheda ***NODI > Panoramica** nel Grid Manager.

Informazioni su questo compito

I dati degli oggetti possono essere ripristinati da altri nodi di archiviazione o da un pool di archiviazione cloud, presupponendo che le regole ILM della griglia siano state configurate in modo che siano disponibili copie degli oggetti.

Notare quanto segue:

- Se una regola ILM è stata configurata per archiviare solo una copia replicata e tale copia esisteva su un volume di archiviazione che ha generato un errore, non sarà possibile ripristinare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID deve inviare più richieste all'endpoint del Cloud Storage Pool per ripristinare i dati dell'oggetto. Prima di eseguire questa procedura, contattare l'assistenza tecnica per ottenere assistenza nella stima dei tempi di ripristino e dei costi associati.

Informazioni su `repair-data` sceneggiatura

Per ripristinare i dati dell'oggetto, eseguire il comando `repair-data` sceneggiatura. Questo script avvia il processo di ripristino dei dati dell'oggetto e funziona con la scansione ILM per garantire che le regole ILM vengano rispettate.

Seleziona **Dati replicati** o **Dati con codice di cancellazione (EC)** qui sotto per conoscere le diverse opzioni per `repair-data` script, a seconda che si stiano ripristinando dati replicati o dati con codice di cancellazione. Se è necessario ripristinare entrambi i tipi di dati, è necessario eseguire entrambi i set di comandi.



Per maggiori informazioni sul `repair-data` script, inserisci `repair-data --help` dalla riga di comando del nodo di amministrazione primario.



Lo script `repair-data` è obsoleto e verrà rimosso in una versione futura. Quando possibile, utilizzare il "[Procedura di ripristino del volume in Grid Manager](#)".

Dati replicati

Sono disponibili due comandi per ripristinare i dati replicati, a seconda che sia necessario riparare l'intero nodo o solo determinati volumi sul nodo:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

È possibile monitorare le riparazioni dei dati replicati con questo comando:

```
repair-data show-replicated-repair-status
```

Dati con codice di cancellazione (EC)

Sono disponibili due comandi per ripristinare i dati codificati in modo da essere cancellati, 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 monitorare le riparazioni dei dati codificati in modo da cancellarli con questo comando:

```
repair-data show-ec-repair-status
```



Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. Tuttavia, se non è possibile recuperare tutti i dati codificati in modo da cancellarli, la riparazione non può essere completata. La riparazione verrà completata quando tutti i nodi saranno disponibili.



Il lavoro di riparazione EC riserva temporaneamente una grande quantità di spazio di archiviazione. Potrebbero essere attivati avvisi di archiviazione, ma il problema si risolverà al termine della riparazione. Se non c'è abbastanza spazio per la prenotazione, il lavoro di riparazione EC fallirà. Le prenotazioni di archiviazione vengono rilasciate al termine del processo di riparazione EC, indipendentemente dal fatto che il processo sia fallito o riuscito.

Trova il nome host per il nodo di archiviazione

1. Accedi al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Utilizzare il `/etc/hosts` file per trovare il nome host del nodo di archiviazione per i volumi di archiviazione ripristinati. Per visualizzare un elenco di tutti i nodi nella griglia, immettere quanto segue: `cat`

/etc/hosts.

Ripara i dati se tutti i volumi sono falliti

Se tutti i volumi di archiviazione sono guasti, riparare l'intero nodo. Seguire le istruzioni per i **dati replicati**, i **dati con codice di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codice di cancellazione (EC) o entrambi.

Se solo alcuni volumi sono falliti, vai a [Riparare i dati se solo alcuni volumi sono falliti](#).



Non puoi correre `repair-data` operazioni per più di un nodo contemporaneamente. Per recuperare più nodi, contattare l'assistenza tecnica.

Dati replicati

Se la griglia include dati replicati, utilizzare `repair-data start-replicated-node-repair` comando con il `--nodes` opzione, dove `--nodes` è il nome host (nome del sistema) per riparare l'intero nodo di archiviazione.

Questo comando ripara i dati replicati su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Quando i dati degli oggetti vengono ripristinati, viene attivato l'avviso **Oggetti persi** se il sistema StorageGRID non riesce a individuare i dati degli oggetti replicati. Gli avvisi potrebbero essere attivati sui nodi di archiviazione in tutto il sistema. Dovresti determinare la causa della perdita e se è possibile un recupero. Vedere "[Indagare sugli oggetti smarriti](#)".

Dati con codice di cancellazione (EC)

Se la griglia contiene dati con codice di cancellazione, utilizzare `repair-data start-ec-node-repair` comando con il `--nodes` opzione, dove `--nodes` è il nome host (nome del sistema) per riparare l'intero nodo di archiviazione.

Questo comando ripara i dati codificati in modo da essere cancellati su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'operazione restituisce un valore univoco `repair ID` che identifica questo `repair_data` operazione. Usa questo `repair ID` per monitorare i progressi e i risultati del `repair_data` operazione. Non verrà restituito alcun altro feedback una volta completato il processo di recupero.

Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. La riparazione verrà completata quando tutti i nodi saranno disponibili.

Riparare i dati se solo alcuni volumi sono falliti

Se solo alcuni volumi sono guasti, riparare i volumi interessati. Seguire le istruzioni per i **dati replicati**, i **dati con codice di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codice di cancellazione (EC) o entrambi.

Se tutti i volumi sono falliti, vai a [Ripara i dati se tutti i volumi sono falliti](#) .

Immettere gli ID del volume in formato esadecimale. Per esempio, 0000 è il primo volume e 000F è il sedicesimo volume. È possibile specificare un volume, un intervallo di volumi o più volumi non in sequenza.

Tutti i volumi devono trovarsi sullo stesso nodo di archiviazione. Se è necessario ripristinare volumi per più di un nodo di archiviazione, contattare l'assistenza tecnica.

Dati replicati

Se la griglia contiene dati replicati, utilizzare `start-replicated-volume-repair` comando con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi aggiungere o il `--volumes` O `--volume-range` opzione, come mostrato negli esempi seguenti.

Volume singolo: questo comando ripristina i dati replicati nel volume 0002 su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervallo di volumi: questo comando ripristina i dati replicati su tutti i volumi nell'intervallo 0003 A 0009 su un nodo di archiviazione 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 archiviazione denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Quando i dati degli oggetti vengono ripristinati, viene attivato l'avviso **Oggetti persi** se il sistema StorageGRID non riesce a individuare i dati degli oggetti replicati. Gli avvisi potrebbero essere attivati sui nodi di archiviazione in tutto il sistema. Prendere nota della descrizione dell'avviso e delle azioni consigliate per determinare la causa della perdita e se è possibile un recupero.

Dati con codice di cancellazione (EC)

Se la griglia contiene dati con codice di cancellazione, utilizzare `start-ec-volume-repair` comando con il `--nodes` opzione per identificare il nodo (dove `--nodes` è il nome host del nodo). Quindi aggiungere o il `--volumes` O `--volume-range` opzione, come mostrato negli esempi seguenti.

Volume singolo: questo comando ripristina i dati codificati in cancellazione nel volume 0007 su un nodo di archiviazione denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervallo di volumi: questo comando ripristina i dati codificati in cancellazione su tutti i volumi nell'intervallo 0004 A 0006 su un nodo di archiviazione 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 codificati in cancellazione nei volumi 000A , 000C , E 000E su un nodo di archiviazione 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` che identifica questo `repair_data` operazione. Usa questo `repair ID` per monitorare i progressi e i risultati del `repair_data` operazione. Non verrà restituito alcun altro feedback una volta completato il processo di

recupero.



Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. La riparazione verrà completata quando tutti i nodi saranno disponibili.

Riparazioni del monitor

Monitorare lo stato dei lavori di riparazione, a seconda che si utilizzino **dati replicati**, **dati con codice di cancellazione (EC)** o entrambi.

È inoltre possibile monitorare lo stato dei lavori di ripristino del volume in corso e visualizzare una cronologia dei lavori di ripristino completati in ["Responsabile della griglia"](#) .

Dati replicati

- Per ottenere una percentuale stimata di completamento per la riparazione replicata, aggiungere `show-replicated-repair-status` opzione al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Per determinare se le riparazioni sono state completate:
 - a. Selezionare **NODI > Nodo di archiviazione in riparazione > ILM**.
 - b. Esaminare gli attributi nella sezione Valutazione. Una volta completate le riparazioni, l'attributo **In attesa - Tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
 - a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - b. Selezionare **grid > Nodo di archiviazione in riparazione > LDR > Data Store**.
 - c. Utilizzare una combinazione dei seguenti attributi per determinare, nel miglior modo possibile, se le riparazioni replicate sono complete.



Potrebbero essere presenti incongruenze in Cassandra e le riparazioni non riuscite non vengono tracciate.

- **Riparazioni tentate (XRPA)**: utilizzare questo attributo per monitorare l'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di archiviazione tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo più lungo del periodo di scansione corrente (fornito dall'attributo **Periodo di scansione - Stimato**), significa che la scansione ILM non ha trovato oggetti ad alto rischio che necessitano di riparazione su alcun nodo.



Gli oggetti ad alto rischio sono oggetti che rischiano di andare completamente persi. Sono esclusi gli oggetti che non soddisfano la loro configurazione ILM.

- **Periodo di scansione - Stimato (XSCM)**: utilizzare questo attributo per stimare quando una modifica della policy verrà applicata agli oggetti precedentemente acquisiti. Se l'attributo **Riparazioni tentate** non aumenta per un periodo più lungo del periodo di scansione corrente, è probabile che siano state eseguite riparazioni replicate. Si noti che il periodo di scansione può variare. L'attributo **Periodo di scansione - Stimato (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione dei nodi. È possibile interrogare la cronologia degli attributi **Periodo di scansione - Stima** per la griglia per determinare un intervallo di tempo appropriato.

Dati con codice di cancellazione (EC)

Per monitorare la riparazione dei dati codificati in modo da cancellarli e riprovare eventuali richieste non riuscite:

1. Determinare lo stato delle riparazioni dei dati codificati tramite cancellazione:
 - Selezionare **SUPPORTO > Strumenti > Metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, seleziona **Panoramica EC** nella sezione Grafana. Consulta i dashboard **Tempo stimato per il completamento del lavoro EC in griglia** e **Percentuale completata del lavoro EC in griglia**.
 - Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` operazione:

```
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 eseguite in precedenza e attualmente.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

Questo comando riprova una riparazione del nodo non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Questo comando riprova una riparazione del volume non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Controllare lo stato di archiviazione dopo aver ripristinato l'unità di sistema del nodo di archiviazione

Dopo aver ripristinato l'unità di sistema per un nodo di archiviazione, è necessario verificare che lo stato desiderato del nodo di archiviazione sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che il server del nodo di archiviazione viene riavviato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Il nodo di archiviazione è stato recuperato e il ripristino dei dati è completo.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Controllare i valori di **Recovered Storage Node > LDR > Storage > Storage State — Desired** e **Storage State — Current**.

Il valore di entrambi gli attributi dovrebbe essere Online.

3. Se lo Stato di archiviazione - Desiderato è impostato su Sola lettura, completare i seguenti passaggi:
 - a. Fare clic sulla scheda **Configurazione**.
 - b. Dall'elenco a discesa **Stato di archiviazione - Desiderato**, selezionare **Online**.
 - c. Fare clic su **Applica modifiche**.
 - d. Fare clic sulla scheda **Panoramica** e verificare che i valori di **Stato di archiviazione — Desiderato** e **Stato di archiviazione — Corrente** siano aggiornati su Online.

Ripristina i dati degli oggetti utilizzando Grid Manager

È possibile ripristinare i dati degli oggetti per un volume di archiviazione o un nodo di archiviazione non riuscito utilizzando Grid Manager. È inoltre possibile utilizzare Grid Manager per monitorare i processi di ripristino in corso e visualizzare la cronologia dei ripristini.

Prima di iniziare

- Hai completato una di queste procedure per formattare i volumi non riusciti:
 - ["Rimontare e riformattare i volumi di archiviazione dell'appliance \(passaggi manuali\)"](#)
 - ["Rimontare e riformattare i volumi di archiviazione \(passaggi manuali\)"](#)
- Hai confermato che il nodo di archiviazione in cui stai ripristinando gli oggetti ha uno stato di connessione **Connesso***  nella scheda ***NODI > Panoramica** nel Grid Manager.
- Hai confermato quanto segue:
 - Non è in corso l'espansione della griglia per aggiungere un nodo di archiviazione.
 - La dismissione di un nodo di archiviazione non è in corso o non è riuscita.
 - Non è in corso il ripristino di un volume di archiviazione non riuscito.
 - Non è in corso il ripristino di un nodo di archiviazione con un'unità di sistema guasta.
 - Non è in corso alcun processo di ribilanciamento della CE.
 - La clonazione del nodo dell'appliance non è in corso.

Informazioni su questo compito

Dopo aver sostituito le unità ed eseguito i passaggi manuali per formattare i 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 Ripristino volume in Grid Manager. Puoi anche [abilitare la modalità di ripristino automatico](#) per avviare automaticamente il ripristino del volume quando i volumi sono pronti per essere ripristinati o [seguire manualmente il ripristino del volume](#). Seguire queste linee guida:

- Se i volumi sono elencati in **MANUTENZIONE > Ripristino volume > Nodi da ripristinare**, ripristinare i dati dell'oggetto come descritto nei passaggi seguenti. I volumi saranno elencati se:
 - Alcuni, ma non tutti, i volumi di archiviazione in un nodo sono falliti
 - Tutti i volumi di archiviazione in un nodo sono guasti e vengono sostituiti con lo stesso numero di volumi o più volumi

La pagina Ripristino volume in Grid Manager consente inoltre di [monitorare il processo di ripristino del volume](#) e [visualizzare la cronologia dei restauri](#).

- Se i volumi non sono elencati in Grid Manager come candidati per il ripristino, seguire i passaggi appropriati per l'utilizzo di `repair-data` script per ripristinare i dati dell'oggetto:
 - ["Ripristino dei dati dell'oggetto nel volume di archiviazione \(errore dell'unità di sistema\)"](#)
 - ["Ripristina i dati dell'oggetto nel volume di archiviazione in cui l'unità di sistema è intatta"](#)
 - ["Ripristina i dati dell'oggetto nel volume di archiviazione per l'appliance"](#)



Lo script `repair-data` è obsoleto e verrà rimosso in una versione futura.

Se il nodo di archiviazione recuperato contiene meno volumi rispetto al nodo che sta sostituendo, è necessario utilizzare `repair-data` sceneggiatura.

È possibile ripristinare due tipi di dati oggetto:

- Gli oggetti dati replicati vengono ripristinati da altre posizioni, presupponendo che le regole ILM della griglia siano state configurate per rendere disponibili le copie degli oggetti.
 - Se una regola ILM è stata configurata per archiviare solo una copia replicata e tale copia esisteva su un volume di archiviazione che ha generato un errore, non sarà possibile ripristinare l'oggetto.
 - Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID deve inviare più richieste all'endpoint del Cloud Storage Pool per ripristinare i dati dell'oggetto.
- Gli oggetti dati con codice di cancellazione (EC) vengono ripristinati ri assemblando i frammenti memorizzati. I frammenti danneggiati o persi vengono ricreati dall'algoritmo di codifica di cancellazione a partire dai dati rimanenti e dai frammenti di parità.

Le riparazioni dei dati codificati in modo da essere cancellati possono iniziare mentre alcuni nodi di archiviazione sono offline. Tuttavia, se non è possibile recuperare tutti i dati codificati in modo da cancellarli, la riparazione non può essere completata. La riparazione verrà completata quando tutti i nodi saranno disponibili.



Il ripristino del volume dipende dalla disponibilità delle risorse in cui sono archiviate le copie degli oggetti. Il processo di ripristino del volume non è lineare e potrebbe richiedere giorni o settimane per essere completato.

Abilita la modalità di ripristino automatico

Quando si abilita la modalità di ripristino automatico, il ripristino del volume si avvia automaticamente quando i volumi sono pronti per essere ripristinati.

Passi

1. In Grid Manager vai su **MANUTENZIONE > Ripristino volume**.
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 del volume su alcun nodo.
- I ripristini del volume inizieranno automaticamente solo quando non saranno in corso altre procedure di manutenzione.
- È possibile monitorare lo stato del lavoro dalla pagina di monitoraggio dell'avanzamento.
- StorageGRID riprova automaticamente i ripristini dei volumi che non riescono ad avviarsi.

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.

Ripristina manualmente il volume o il nodo non riuscito

Per ripristinare un volume o un nodo non riuscito, seguire questi passaggi.

Passi

1. In Grid Manager vai su **MANUTENZIONE > Ripristino volume**.
2. Selezionare la scheda **Nodi da ripristinare**, quindi spostare l'interruttore per la **Modalità di ripristino automatico** sulla posizione disattivata.

Il numero sulla scheda indica il numero di nodi con volumi che richiedono il ripristino.

3. Espandi ciascun nodo per visualizzare i volumi in esso contenuti che necessitano di ripristino e il loro stato.
4. Correggere eventuali problemi che impediscono il ripristino di ciascun volume. I problemi verranno segnalati 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 lo stato Pronto per il ripristino.

È possibile ripristinare i volumi di un solo nodo alla volta.

Ogni volume nel nodo deve indicare che è pronto per il ripristino.

6. Selezionare **Avvia ripristino**.
7. Rispondere a tutti gli avvisi che potrebbero apparire oppure selezionare **Avvia comunque** per ignorare gli avvisi e avviare il ripristino.

Quando il ripristino inizia, i nodi vengono spostati dalla scheda **Nodi da ripristinare** alla scheda **Avanzamento del ripristino**.

Se non è possibile avviare il ripristino di un volume, il nodo torna alla scheda **Nodi da ripristinare**.

Visualizza l'avanzamento del restauro

La scheda **Avanzamento ripristino** mostra lo stato del processo di ripristino del volume e informazioni sui volumi di un nodo in fase di ripristino.

I tassi di riparazione dei dati per oggetti replicati e con codice di cancellazione in tutti i volumi sono medie che riassumono tutti i restauri in corso, compresi quelli avviati utilizzando `repair-data` sceneggiatura. Viene indicata anche la percentuale di oggetti intatti presenti in quei volumi che non necessitano di restauro.



Il ripristino dei dati replicati dipende dalla disponibilità delle risorse in cui sono archiviate le copie replicate. Il processo di 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 Processi di ripristino indica il numero di volumi in fase di ripristino o in coda per il ripristino.
- Nella tabella vengono visualizzate informazioni su ciascun volume in un nodo in fase di ripristino e sul relativo avanzamento.

- L'avanzamento per ciascun nodo mostra la percentuale per ogni processo.
- Espandi la colonna Dettagli per visualizzare l'ora di inizio del ripristino e l'ID del processo.
- Se il ripristino del volume fallisce:
 - La colonna Stato indica `failed (attempting retry)` e verrà ritentato automaticamente.
 - Se più processi di ripristino non sono riusciti, il processo più recente verrà automaticamente ritentato per primo.
 - L'avviso **Errore di riparazione EC** viene attivato se i tentativi continuano a fallire. Per risolvere il problema, seguire i passaggi indicati nell'avviso.

Visualizza la cronologia dei restauri

La scheda **Cronologia restauri** mostra informazioni su tutti i restauri dei volumi completati con successo.



Le dimensioni non sono applicabili agli oggetti replicati e vengono visualizzate solo per i restauri che contengono oggetti dati con codice di cancellazione (EC).

Monitorare i lavori di riparazione dei dati

È possibile monitorare lo stato dei lavori di riparazione utilizzando `repair-data` script dalla riga di comando.

Tra questi rientrano i lavori avviati manualmente o i lavori avviati automaticamente da StorageGRID come parte di una procedura di dismissione.



Se si eseguono lavori di ripristino del volume, "[monitorare l'avanzamento e visualizzare la cronologia di tali lavori in Grid Manager](#)" Invece.

Monitorare lo stato di `repair-data` lavori in base all'utilizzo di **dati replicati**, **dati con codice di cancellazione (EC)** o entrambi.

Dati replicati

- Per ottenere una percentuale stimata di completamento per la riparazione replicata, aggiungere `show-replicated-repair-status` opzione al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Per determinare se le riparazioni sono state completate:
 - a. Selezionare **NODI > Nodo di archiviazione in riparazione > ILM**.
 - b. Esaminare gli attributi nella sezione Valutazione. Una volta completate le riparazioni, l'attributo **In attesa - Tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
 - a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - b. Selezionare **grid > Nodo di archiviazione in riparazione > LDR > Data Store**.
 - c. Utilizzare una combinazione dei seguenti attributi per determinare, nel miglior modo possibile, se le riparazioni replicate sono complete.



Potrebbero essere presenti incongruenze in Cassandra e le riparazioni non riuscite non vengono tracciate.

- **Riparazioni tentate (XRPA)**: utilizzare questo attributo per monitorare l'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di archiviazione tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo più lungo del periodo di scansione corrente (fornito dall'attributo **Periodo di scansione - Stimato**), significa che la scansione ILM non ha trovato oggetti ad alto rischio che necessitano di riparazione su alcun nodo.



Gli oggetti ad alto rischio sono oggetti che rischiano di andare completamente persi. Sono esclusi gli oggetti che non soddisfano la loro configurazione ILM.

- **Periodo di scansione - Stimato (XSCM)**: utilizzare questo attributo per stimare quando una modifica della policy verrà applicata agli oggetti precedentemente acquisiti. Se l'attributo **Riparazioni tentate** non aumenta per un periodo più lungo del periodo di scansione corrente, è probabile che siano state eseguite riparazioni replicate. Si noti che il periodo di scansione può variare. L'attributo **Periodo di scansione - Stimato (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione dei nodi. È possibile interrogare la cronologia degli attributi **Periodo di scansione - Stima** per la griglia per determinare un intervallo di tempo appropriato.

Dati con codice di cancellazione (EC)

Per monitorare la riparazione dei dati codificati in modo da cancellarli e riprovare eventuali richieste non riuscite:

1. Determinare lo stato delle riparazioni dei dati codificati tramite cancellazione:
 - Selezionare **SUPPORTO > Strumenti > Metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, seleziona **Panoramica EC** nella sezione Grafana. Consulta i dashboard **Tempo stimato per il completamento del lavoro EC in griglia** e **Percentuale completata del lavoro EC in griglia**.
 - Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` operazione:

```
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 eseguite in precedenza e attualmente.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

Questo comando riprova una riparazione del nodo non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Questo comando riprova una riparazione del volume non riuscita, utilizzando l'ID di riparazione 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Ripristino da errori del nodo di amministrazione

Ripristino del nodo di amministrazione primario o non primario

Il processo di ripristino per un nodo amministrativo varia a seconda che si tratti del nodo amministrativo primario o di un nodo amministrativo non primario.

I passaggi generali per il ripristino di un nodo amministrativo primario o non primario sono gli stessi, sebbene i dettagli dei passaggi differiscano.

Seguire sempre la procedura di ripristino corretta per il nodo di amministrazione che si sta ripristinando. Ad alto livello le procedure sembrano le stesse, ma differiscono nei dettagli.

Scelte

- ["Ripristino da errori del nodo di amministrazione primario"](#)
- ["Ripristino da errori del nodo di amministrazione non primario"](#)

Ripristino da errori del nodo di amministrazione primario

Ripristino da errori del nodo di amministrazione primario

Per ripristinare un errore del nodo di amministrazione primario è necessario completare una serie specifica di attività. Il nodo di amministrazione primario ospita il servizio Configuration Management Node (CMN) per la griglia.



È necessario riparare o sostituire tempestivamente un nodo amministrativo primario non funzionante, altrimenti la griglia potrebbe perdere la capacità di acquisire nuovi oggetti. Il periodo di tempo esatto dipende dalla velocità di acquisizione degli oggetti: se hai bisogno di una valutazione più accurata dell'intervallo di tempo per la tua griglia, contatta l'assistenza tecnica.

Il servizio Configuration Management Node (CMN) sul nodo di amministrazione primario è responsabile dell'emissione di blocchi di identificatori di oggetti per la griglia. Questi identificatori vengono assegnati agli oggetti quando vengono acquisiti. Non è possibile acquisire nuovi oggetti se non sono disponibili identificatori. L'acquisizione degli oggetti può continuare anche quando la CMN non è disponibile, perché circa un mese di fornitura di identificatori è memorizzata nella cache della griglia. Tuttavia, una volta esauriti gli identificatori memorizzati nella cache, non sarà più possibile aggiungere nuovi oggetti.

Per ripristinare un nodo di amministrazione primario, seguire questi passaggi generali:

1. ["Copia i registri di controllo dal nodo di amministrazione primario non riuscito"](#)
2. ["Sostituisci il nodo di amministrazione primario"](#)
3. ["Configurare il nodo di amministrazione primario sostitutivo"](#)
4. ["Determinare se è necessario un hotfix per il nodo di amministrazione primario recuperato"](#)
5. ["Ripristina il registro di controllo sul nodo di amministrazione primario recuperato"](#)
6. ["Ripristinare il database del nodo di amministrazione durante il ripristino di un nodo di amministrazione primario"](#)
7. ["Ripristina le metriche di Prometheus durante il ripristino di un nodo di amministrazione primario"](#)

Copia i registri di controllo dal nodo di amministrazione primario non riuscito

Se riesci a copiare i registri di controllo dal nodo di amministrazione primario non riuscito, dovresti conservarli per mantenere la registrazione dell'attività e dell'utilizzo del sistema nella griglia. È possibile ripristinare i registri di controllo conservati nel nodo di amministrazione primario recuperato dopo che è attivo e funzionante.

Informazioni su questo compito

Questa procedura copia i file del registro di controllo dal nodo di amministrazione non riuscito in una posizione temporanea su un nodo della 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 la distribuzione ha un solo nodo amministrativo, il nodo amministrativo recuperato inizia a registrare gli eventi nel registro di controllo in un nuovo file vuoto e i dati registrati in precedenza vengono persi. Se la distribuzione include più di un nodo amministrativo, è possibile recuperare i registri di controllo da un altro nodo amministrativo.



Se al momento non è possibile accedere ai registri di controllo sul nodo di amministrazione non riuscito, potresti riuscire ad accedervi in un secondo momento, ad esempio dopo il ripristino dell'host.

Passi

1. Se possibile, accedere al nodo di amministrazione non riuscito. In caso contrario, accedi al nodo di

amministrazione principale o a un altro nodo di amministrazione, se disponibile.

- a. Immettere il seguente comando: `ssh admin@grid_node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Arrestare il servizio AMS per impedire che crei un nuovo file di registro: `service ams stop`
3. Passare alla directory di esportazione dell'audit:

```
cd /var/local/log
```

4. Rinomina la fonte `audit.log` file in un nome di file univoco e numerato. 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 registro di controllo in una posizione temporanea su un nodo della griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando richiesto, immettere la password per l'amministratore.

7. Copia tutti i file del registro di controllo nella posizione temporanea: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando richiesto, immettere la password per l'amministratore.

8. Disconnettersi come root: `exit`

Sostituisci il nodo di amministrazione primario

Per ripristinare un nodo amministrativo primario, è necessario prima sostituire l'hardware fisico o virtuale.

È possibile sostituire un nodo amministrativo primario non riuscito con un nodo amministrativo primario in esecuzione sulla stessa piattaforma oppure è possibile sostituire un nodo amministrativo primario in esecuzione su VMware o un host Linux con un nodo amministrativo primario ospitato su un'appliance di servizi.

Utilizzare la procedura corrispondente alla piattaforma sostitutiva selezionata per il nodo. Dopo aver completato la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), la procedura indirizzerà al passaggio successivo per il ripristino del nodo di amministrazione primario.

Piattaforma sostitutiva	Procedura
VMware	"Sostituisci un nodo VMware"
Linux	"Sostituisci un nodo Linux"
Servizi elettrodomestici	"Sostituire un apparecchio di servizio"
OpenStack	I file del disco della macchina virtuale e gli script forniti da NetApp per OpenStack non sono più supportati per le operazioni di ripristino. Se devi ripristinare un nodo in esecuzione in una distribuzione OpenStack, scarica i file per il tuo sistema operativo Linux. Quindi, seguire la procedura per "sostituzione di un nodo Linux" .

Configura il nodo di amministrazione primario sostitutivo

Il nodo sostitutivo deve essere configurato come nodo di amministrazione primario per il sistema StorageGRID.

Prima di iniziare

- Per i nodi amministrativi primari ospitati su macchine virtuali, la macchina virtuale è stata distribuita, accesa e inizializzata.
- Per i nodi amministrativi primari ospitati su un'appliance di servizi, hai sostituito l'appliance e hai installato il software. Vedi il ["Istruzioni di installazione per il tuo elettrodomestico"](#).
- Hai l'ultimo backup del file del pacchetto di ripristino(`sgws-recovery-package-id-revision.zip`).
- Hai la passphrase di provisioning.

Passi

1. Apri il tuo browser web e vai su `https://primary_admin_node_ip`.
2. Gestisci una password di installazione temporanea secondo necessità:
 - Se è già stata impostata una password utilizzando uno di questi metodi, immetterla per procedere.
 - Un utente ha impostato la password durante l'accesso al programma di installazione in precedenza
 - Per i sistemi bare metal, la password è stata importata automaticamente dal file di configurazione del nodo in `/etc/storagegrid/nodes/<node_name>.conf`
 - Per le VM, la password SSH/console è stata importata automaticamente dalle proprietà OVF
 - Se non è stata impostata una password, impostarne una facoltativamente per proteggere il programma di installazione StorageGRID.
3. Fare clic su **Recupera un nodo amministrativo primario non riuscito**.

Install

Welcome

Use this page to install a new StorageGRID system, or recover a failed primary Admin Node for an existing system.

Note: You must have access to a StorageGRID license, network configuration and grid topology information, and NTP settings to complete the installation. You must have the latest version of the Recovery Package file to complete a primary Admin Node recovery.



Install a StorageGRID system



Recover a failed primary Admin
Node

4. Carica il backup più recente del pacchetto di ripristino:
 - a. Fare clic su **Sfoggia**.
 - b. Individua il file Recovery Package più recente per il tuo sistema StorageGRID e fai clic su **Apri**.
5. Immettere la passphrase di provisioning.
6. Fare clic su **Avvia ripristino**.

Inizia il processo di recupero. Grid Manager potrebbe non essere disponibile per alcuni minuti, in quanto vengono avviati i servizi richiesti. Una volta completato il ripristino, verrà visualizzata la pagina di accesso.

7. Se l'accesso Single Sign-On (SSO) è abilitato per il sistema StorageGRID e il trust della relying party per il nodo di amministrazione ripristinato è stato configurato per utilizzare il certificato dell'interfaccia di gestione predefinito, aggiornare (o eliminare e ricreare) il trust della relying party 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 della parte affidabile, vedere ["Configurare l'accesso singolo"](#). Per accedere al certificato del server predefinito, accedi alla shell dei comandi del nodo di amministrazione. Vai al `/var/local/mgmt-api` directory e selezionare la `server.crt` file.



Dopo aver ripristinato un nodo di amministrazione primario, ["determinare se è necessario applicare un hotfix"](#).

Determinare il requisito di hotfix per il nodo di amministrazione primario

Dopo aver ripristinato un nodo di amministrazione primario, determinare se è necessario

applicare un hotfix.

Prima di iniziare

Il ripristino del nodo di amministrazione primario è completo.

Passi

1. Sign in a Grid Manager utilizzando un ["browser web supportato"](#) .
2. Selezionare **NODES**.
3. Dall'elenco a sinistra, seleziona il nodo di amministrazione primario.
4. Nella scheda Panoramica, annotare la versione visualizzata nel campo **Versione software**.
5. Selezionare un altro nodo della griglia.
6. Nella scheda Panoramica, annotare la versione visualizzata nel campo **Versione software**.
 - Se le versioni visualizzate nei campi **Versione software** sono le stesse, non è necessario applicare un hotfix.
 - Se le versioni visualizzate nei campi **Versione software** sono diverse, è necessario ["applicare un hotfix"](#) per aggiornare il nodo amministrativo primario recuperato alla stessa versione.

Ripristina il registro di controllo sul nodo di amministrazione primario recuperato

Se sei riuscito a conservare il registro di controllo dal nodo amministrativo primario non riuscito, puoi copiarlo nel nodo amministrativo primario che stai ripristinando.

Prima di iniziare

- Il nodo amministrativo recuperato è installato e funzionante.
- Hai copiato i registri di controllo in un'altra posizione dopo che il nodo di amministrazione originale ha avuto esito negativo.

Informazioni su questo compito

Se un nodo di amministrazione non funziona, i registri di controllo salvati su quel nodo di amministrazione potrebbero andare persi. Potrebbe essere possibile preservare i dati dalla perdita copiando i registri di controllo dal nodo di amministrazione non riuscito e quindi ripristinando tali registri di controllo nel nodo di amministrazione recuperato. A seconda dell'errore, potrebbe non essere possibile copiare i registri di controllo dal nodo di amministrazione non riuscito. In tal caso, se la distribuzione ha più di un nodo amministrativo, è possibile recuperare i log di controllo da un altro nodo amministrativo poiché i log di controllo vengono replicati su tutti i nodi amministrativi.

Se è presente un solo nodo di amministrazione e il registro di controllo non può essere copiato dal nodo non riuscito, il nodo di amministrazione ripristinato inizia a registrare gli eventi nel registro di controllo come se l'installazione fosse nuova.

È necessario ripristinare un nodo di amministrazione il prima possibile per ripristinare la funzionalità di registrazione.

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:



- Hai configurato un server syslog esterno e i log di controllo vengono ora inviati al server syslog anziché ai nodi di amministrazione.
- Hai specificato esplicitamente che i messaggi di controllo devono essere salvati solo sui nodi locali che li hanno generati.

Vedere "[Configurare i messaggi di controllo e le destinazioni dei registri](#)" per i dettagli.

Passi

1. Accedi al nodo di amministrazione recuperato:

- a. Immettere il seguente comando: `ssh admin@recovery_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Dopo aver effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Controlla quali file di controllo sono stati conservati: `cd /var/local/log`

3. Copiare i file di registro di controllo conservati nel nodo di amministrazione recuperato: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Quando richiesto, immettere la password per l'amministratore.

4. Per motivi di sicurezza, eliminare i registri di controllo dal nodo della griglia non riuscito dopo aver verificato che siano stati copiati correttamente nel nodo di amministrazione ripristinato.

5. Aggiornare le impostazioni utente e gruppo dei file di registro di controllo sul nodo di amministrazione recuperato: `chown ams-user: bycast *`

6. Disconnettersi come root: `exit`

Ripristinare il database del nodo amministrativo durante il ripristino del nodo amministrativo primario

Se si desidera conservare le informazioni cronologiche sugli attributi e sugli avvisi su un nodo di amministrazione primario che ha subito un errore, è possibile ripristinare il database del nodo di amministrazione. È possibile ripristinare questo database solo se il sistema StorageGRID include un altro nodo di amministrazione.

Prima di iniziare

- Il nodo amministrativo recuperato è installato e funzionante.
- Il sistema StorageGRID include almeno due nodi amministrativi.
- Tu hai il `Passwords.txt` file.
- Hai la passphrase di provisioning.

Informazioni su questo compito

Se un nodo di amministrazione si guasta, le informazioni storiche memorizzate nel suo database vanno perse. Questo database include le seguenti informazioni:

- Cronologia degli avvisi
- Dati degli attributi storici, utilizzati nei grafici in stile legacy nella pagina Nodi

Quando si ripristina un nodo di amministrazione, il processo di installazione del software crea un database del nodo di amministrazione vuoto sul nodo ripristinato. Tuttavia, il nuovo database include solo informazioni sui server e sui servizi che fanno attualmente parte del sistema o che saranno aggiunti in seguito.

Se hai ripristinato un nodo amministrativo primario e il tuo sistema StorageGRID ha un altro nodo amministrativo, puoi ripristinare le informazioni storiche copiando il database del nodo amministrativo da un nodo amministrativo non primario (il *nodo amministrativo di origine*) al nodo amministrativo primario ripristinato. Se il sistema ha solo un nodo di amministrazione primario, non è possibile ripristinare il database del nodo di amministrazione.



La copia del database del nodo di amministrazione potrebbe richiedere diverse ore. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi sono interrotti sul nodo di amministrazione di origine.

Passi

1. Accedi al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.
2. Dal nodo di amministrazione 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 recuperato:
 - a. Accedi al nodo di amministrazione recuperato:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla root: `su -`
 - iv. Inserisci la password elencata nel `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. Inserisci: `ssh-add`
 - e. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.
 - f. Copiare il database dal nodo amministrativo di origine al nodo amministrativo recuperato:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Quando richiesto, confermare che si desidera sovrascrivere il database MI sul nodo di amministrazione recuperato.

Il database e i suoi dati storici vengono copiati nel nodo di amministrazione recuperato. Una volta completata l'operazione di copia, lo script avvia il nodo di amministrazione recuperato.

- h. Quando non è più necessario l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserisci: `ssh-add -D`

5. Riavviare i servizi sul nodo di amministrazione di origine: `service servermanager start`

Ripristina le metriche di 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 subito un errore. Le metriche Prometheus possono essere ripristinate solo se il sistema StorageGRID include un altro nodo di amministrazione.

Prima di iniziare

- Il nodo amministrativo recuperato è installato e funzionante.
- Il sistema StorageGRID include almeno due nodi amministrativi.
- Tu hai il `Passwords.txt` file.
- Hai la passphrase di provisioning.

Informazioni su questo compito

Se un nodo di amministrazione fallisce, le metriche mantenute nel database Prometheus sul nodo di amministrazione vanno perse. Quando si ripristina il nodo di amministrazione, il processo di installazione del software crea un nuovo database Prometheus. Dopo l'avvio del nodo amministrativo ripristinato, le metriche vengono registrate come se fosse stata eseguita una nuova installazione del sistema StorageGRID .

Se hai ripristinato un nodo amministrativo primario e il tuo sistema StorageGRID ha un altro nodo amministrativo, puoi ripristinare le metriche storiche copiando il database Prometheus da un nodo amministrativo non primario (il *nodo amministrativo di origine*) al nodo amministrativo primario ripristinato. Se il sistema ha solo 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 sono interrotti sul nodo di amministrazione di origine.

Passi

1. Accedi al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.
2. Dal nodo di amministrazione di origine, arrestare il servizio Prometheus: `service prometheus stop`
3. Completare i seguenti passaggi sul nodo di amministrazione recuperato:
 - a. Accedi al nodo di amministrazione recuperato:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`

- ii. Inserisci la password elencata nel `Passwords.txt` file.
- iii. Immettere il seguente comando per passare alla root: `su -`
- iv. Inserisci la password elencata nel `Passwords.txt` file.
- b. Interrompere il servizio Prometheus: `service prometheus stop`
- c. Aggiungere la chiave privata SSH all'agente SSH. Inserisci: `ssh-add`
- d. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.
- e. Copiare il database Prometheus dal nodo amministrativo di origine al nodo amministrativo recuperato:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. Quando richiesto, premere **Invio** per confermare che si desidera eliminare il nuovo database Prometheus sul nodo di amministrazione recuperato.

Il database Prometheus originale e i suoi dati storici vengono copiati nel nodo di amministrazione recuperato. Una volta completata l'operazione di copia, lo script avvia il nodo di amministrazione recuperato. Viene visualizzato il seguente stato:

Database clonato, avvio dei servizi

- a. Quando non è più necessario l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserisci: `ssh-add -D`
- 4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine. `service prometheus start`

Ripristino da errori del nodo di amministrazione non primario

Ripristino da errori del nodo di amministrazione non primario

Per ripristinare un errore del nodo di amministrazione non primario, è necessario completare le seguenti attività. Un nodo amministrativo ospita il servizio Configuration Management Node (CMN) ed è noto come nodo amministrativo primario. Sebbene sia possibile avere più nodi amministrativi, ogni sistema StorageGRID include un solo nodo amministrativo primario. Tutti gli altri nodi amministrativi sono nodi amministrativi non primari.

Per ripristinare un nodo di amministrazione non primario, seguire questi passaggi generali:

1. ["Copia i registri di controllo dal nodo di amministrazione non primario non riuscito"](#)
2. ["Sostituisci il nodo di amministrazione non primario"](#)
3. ["Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario"](#)
4. ["Ripristina il registro di controllo su un nodo di amministrazione non primario recuperato"](#)
5. ["Ripristinare il database del nodo di amministrazione durante il recupero di un nodo di amministrazione non primario"](#)
6. ["Ripristina le metriche di Prometheus durante il ripristino di un nodo di amministrazione non primario"](#)

Copia i registri di controllo dal nodo di amministrazione non primario non riuscito

Se riesci a copiare i registri di controllo dal nodo di amministrazione non riuscito, dovresti

conservarli per mantenere la registrazione dell'attività e dell'utilizzo del sistema nella griglia. È possibile ripristinare i registri di controllo conservati nel nodo di amministrazione non primario recuperato dopo che è attivo e funzionante.

Questa procedura copia i file del registro di controllo dal nodo di amministrazione non riuscito in una posizione temporanea su un nodo della 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 la distribuzione ha un solo nodo amministrativo, il nodo amministrativo recuperato inizia a registrare gli eventi nel registro di controllo in un nuovo file vuoto e i dati registrati in precedenza vengono persi. Se la distribuzione include più di un nodo amministrativo, è possibile recuperare i registri di controllo da un altro nodo amministrativo.



Se al momento non è possibile accedere ai registri di controllo sul nodo di amministrazione non riuscito, potresti riuscire ad accedervi in un secondo momento, ad esempio dopo il ripristino dell'host.

1. Se possibile, accedere al nodo di amministrazione non riuscito. In caso contrario, accedi al nodo di amministrazione principale o a un altro nodo di amministrazione, se disponibile.

- a. Immettere il seguente comando: `ssh admin@grid_node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Arrestare il servizio AMS per impedire che crei un nuovo file di registro: `service ams stop`
3. Passare alla directory di esportazione dell'audit:

```
cd /var/local/log
```

4. Rinominare il file `audit.log` di origine con un nome 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 registro di controllo in una posizione temporanea su un nodo della griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando richiesto, immettere la password per l'amministratore.

7. Copia tutti i file del registro di controllo nella posizione temporanea: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando richiesto, immettere la password per l'amministratore.

8. Disconnettersi come root: `exit`

Sostituisci il nodo di amministrazione non primario

Per ripristinare un nodo amministrativo non primario, è necessario prima sostituire l'hardware fisico o virtuale.

È possibile sostituire un nodo amministrativo non primario non riuscito con un nodo amministrativo non primario in esecuzione sulla stessa piattaforma oppure è possibile sostituire un nodo amministrativo non primario in esecuzione su VMware o un host Linux con un nodo amministrativo non primario ospitato su un'appliance di servizi.

Utilizzare la procedura corrispondente alla piattaforma sostitutiva selezionata per il nodo. Dopo aver completato la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), la procedura indirizzerà al passaggio successivo per il ripristino del nodo di amministrazione non primario.

Piattaforma sostitutiva	Procedura
VMware	"Sostituisci un nodo VMware"
Linux	"Sostituisci un nodo Linux"
Servizi elettrodomestici	"Sostituire un apparecchio di servizio"
OpenStack	I file del disco della macchina virtuale e gli script forniti da NetApp per OpenStack non sono più supportati per le operazioni di ripristino. Se devi ripristinare un nodo in esecuzione in una distribuzione OpenStack, scarica i file per il tuo sistema operativo Linux. 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 di amministrazione non primario, è necessario selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo in sostituzione del nodo guasto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).
- Hai la passphrase di provisioning.
- Hai distribuito e configurato il nodo sostitutivo.

Passi

1. Da Grid Manager, seleziona **MANUTENZIONE > Attività > Ripristino**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Nodi in sospeso.

I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionarne uno finché non è

stato reinstallato e non è pronto per il ripristino.

3. Immettere la **Passphrase di provisioning**.
4. Fare clic su **Avvia ripristino**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	☒

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitorare l'avanzamento del ripristino nella tabella Nodo griglia in fase di ripristino.



Mentre la procedura di ripristino è in esecuzione, puoi fare clic su **Reimposta** per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che se si reimposta la procedura, il nodo verrà lasciato in uno stato indeterminato.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware:** Elimina il nodo della griglia virtuale distribuito. Quindi, quando sei pronto per riavviare il ripristino, ridistribuisce 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 ["Preparare l'apparecchio per la reinstallazione \(solo sostituzione della piattaforma\)"](#).

6. Se l'accesso Single Sign-On (SSO) è abilitato per il sistema StorageGRID e il trust della relying party per il nodo di amministrazione ripristinato è stato configurato per utilizzare il certificato dell'interfaccia di gestione predefinito, aggiornare (o eliminare e ricreare) il trust della relying party 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 della parte affidabile, vedere ["Configurare l'accesso singolo"](#). Per accedere al certificato del server predefinito, accedi alla shell dei comandi del nodo di amministrazione. Vai al `/var/local/mgmt-api` directory e selezionare la `server.crt` file.

Ripristina il registro di controllo sul nodo di amministrazione non primario recuperato

Se sei riuscito a conservare il registro di controllo dal nodo di amministrazione non primario non riuscito, in modo da conservare le informazioni cronologiche del registro di controllo, puoi copiarlo nel nodo di amministrazione non primario che stai ripristinando.

Prima di iniziare

- Il nodo amministrativo recuperato è installato e funzionante.
- Hai copiato i registri di controllo in un'altra posizione dopo che il nodo di amministrazione originale ha avuto esito negativo.

Informazioni su questo compito

Se un nodo di amministrazione non funziona, i registri di controllo salvati su quel nodo di amministrazione potrebbero andare persi. Potrebbe essere possibile preservare i dati dalla perdita copiando i registri di controllo dal nodo di amministrazione non riuscito e quindi ripristinando tali registri di controllo nel nodo di amministrazione recuperato. A seconda dell'errore, potrebbe non essere possibile copiare i registri di controllo dal nodo di amministrazione non riuscito. In tal caso, se la distribuzione ha più di un nodo amministrativo, è possibile recuperare i log di controllo da un altro nodo amministrativo poiché i log di controllo vengono replicati su tutti i nodi amministrativi.

Se è presente un solo nodo di amministrazione e il registro di controllo non può essere copiato dal nodo non riuscito, il nodo di amministrazione ripristinato inizia a registrare gli eventi nel registro di controllo come se l'installazione fosse nuova.

È necessario ripristinare un nodo di amministrazione il prima possibile per ripristinare la funzionalità di registrazione.

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:



- Hai configurato un server syslog esterno e i log di controllo vengono ora inviati al server syslog anziché ai nodi di amministrazione.
- Hai specificato esplicitamente che i messaggi di controllo devono essere salvati solo sui nodi locali che li hanno generati.

Vedere "[Configurare i messaggi di controllo e le destinazioni dei registri](#)" per i dettagli.

Passi

1. Accedi al nodo di amministrazione recuperato:

a. Inserisci il seguente comando:

```
ssh admin@recovery_Admin_Node_IP
```

b. Inserisci la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Dopo aver effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Controlla quali file di controllo sono stati conservati:

```
cd /var/local/log
```

3. Copiare i file di registro di controllo conservati nel nodo di amministrazione recuperato:

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Quando richiesto, immettere la password per l'amministratore.

4. Per motivi di sicurezza, eliminare i registri di controllo dal nodo della griglia non riuscito dopo aver verificato che siano stati copiati correttamente nel nodo di amministrazione ripristinato.

5. Aggiornare le impostazioni utente e gruppo dei file di registro di controllo sul nodo di amministrazione recuperato:

```
chown ams-user:bycast *
```

6. Disconnettersi come root: `exit`

Ripristina il database del nodo amministrativo durante il ripristino del nodo amministrativo non primario

Se si desidera conservare le informazioni cronologiche sugli attributi e sugli avvisi su un nodo di amministrazione non primario che ha subito un errore, è possibile ripristinare il database del nodo di amministrazione dal nodo di amministrazione primario.

Prima di iniziare

- Il nodo amministrativo recuperato è installato e funzionante.

- Il sistema StorageGRID include almeno due nodi amministrativi.
- Tu hai il `Passwords.txt` file.
- Hai la passphrase di provisioning.

Informazioni su questo compito

Se un nodo di amministrazione si guasta, le informazioni storiche memorizzate nel suo database vanno perse. Questo database include le seguenti informazioni:

- Cronologia degli avvisi
- Dati degli attributi storici, utilizzati nei grafici in stile legacy nella pagina Nodi

Quando si ripristina un nodo di amministrazione, il processo di installazione del software crea un database del nodo di amministrazione vuoto sul nodo ripristinato. Tuttavia, il nuovo database include solo informazioni sui server e sui servizi che fanno attualmente parte del sistema o che saranno aggiunti in seguito.

Se hai ripristinato un nodo amministrativo non primario, puoi ripristinare le informazioni cronologiche copiando il database del nodo amministrativo dal nodo amministrativo primario (il *nodo amministrativo di origine*) al nodo ripristinato.



La copia del database del nodo di amministrazione potrebbe richiedere diverse ore. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi sono interrotti sul nodo sorgente.

Passi

1. Accedi al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.
2. Eseguire il seguente comando dal nodo di amministrazione di origine. Quindi, se richiesto, immettere la passphrase di provisioning: `recover-access-points`
3. Dal nodo di amministrazione 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 recuperato:
 - a. Accedi al nodo di amministrazione recuperato:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla root: `su -`
 - iv. Inserisci la password elencata nel `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. Inserisci:`ssh-add`
- e. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.
- f. Copiare il database dal nodo amministrativo di origine al nodo amministrativo recuperato:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
- g. Quando richiesto, confermare che si desidera sovrascrivere il database MI sul nodo di amministrazione recuperato.

Il database e i suoi dati storici vengono copiati nel nodo di amministrazione recuperato. Una volta completata l'operazione di copia, lo script avvia il nodo di amministrazione recuperato.

- h. Quando non è più necessario l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserisci:`ssh-add -D`

6. Riavviare i servizi sul nodo di amministrazione di origine: `service servermanager start`

Ripristina le metriche di Prometheus durante il ripristino del nodo di amministrazione non primario

Facoltativamente, è possibile conservare le metriche storiche gestite da Prometheus su un nodo di amministrazione non primario che ha subito un errore.

Prima di iniziare

- Il nodo amministrativo recuperato è installato e funzionante.
- Il sistema StorageGRID include almeno due nodi amministrativi.
- Tu hai il `Passwords.txt` file.
- Hai la passphrase di provisioning.

Informazioni su questo compito

Se un nodo di amministrazione fallisce, le metriche mantenute nel database Prometheus sul nodo di amministrazione vanno perse. Quando si ripristina il nodo di amministrazione, il processo di installazione del software crea un nuovo database Prometheus. Dopo l'avvio del nodo amministrativo ripristinato, le metriche vengono registrate come se fosse stata eseguita una nuova installazione del sistema StorageGRID.

Se hai ripristinato un nodo amministrativo non primario, puoi ripristinare le metriche storiche copiando il database Prometheus dal nodo amministrativo primario (il *nodo amministrativo di origine*) al nodo amministrativo ripristinato.



La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi sono interrotti sul nodo di amministrazione di origine.

Passi

1. Accedi al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.
2. Dal nodo di amministrazione di origine, arrestare il servizio Prometheus: `service prometheus stop`

3. Completare i seguenti passaggi sul nodo di amministrazione recuperato:

- a. Accedi al nodo di amministrazione recuperato:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla root: `su -`
 - iv. Inserisci la password elencata nel `Passwords.txt` file.
- b. Interrompere il servizio Prometheus: `service prometheus stop`
- c. Aggiungere la chiave privata SSH all'agente SSH. Inserisci: `ssh-add`
- d. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.
- e. Copiare il database Prometheus dal nodo amministrativo di origine al nodo amministrativo recuperato:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. Quando richiesto, premere **Invio** per confermare che si desidera eliminare il nuovo database Prometheus sul nodo di amministrazione recuperato.

Il database Prometheus originale e i suoi dati storici vengono copiati nel nodo di amministrazione recuperato. Una volta completata l'operazione di copia, lo script avvia il nodo di amministrazione recuperato. Viene visualizzato il seguente stato:

Database clonato, avvio dei servizi

- a. Quando non è più necessario l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserisci: `ssh-add -D`

4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine. `service prometheus start`

Ripristino da guasti del nodo gateway

Sostituisci nodo gateway

È possibile sostituire un Gateway Node non riuscito con un Gateway Node in esecuzione sullo stesso hardware fisico o virtuale, oppure è possibile sostituire un Gateway Node in esecuzione su VMware o un host Linux con un Gateway Node ospitato su un'appliance di servizi.

La procedura di sostituzione del nodo da seguire dipende dalla piattaforma che verrà utilizzata dal nodo sostitutivo. Dopo aver completato la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), la procedura indirizzerà al passaggio successivo per il ripristino del nodo gateway.

Piattaforma sostitutiva	Procedura
VMware	"Sostituisci un nodo VMware"
Linux	"Sostituisci un nodo Linux"
Servizi elettrodomestici	"Sostituire un apparecchio di servizio"

Piattaforma sostitutiva	Procedura
OpenStack	I file del disco della macchina virtuale e gli script forniti da NetApp per OpenStack non sono più supportati per le operazioni di ripristino. Se devi ripristinare un nodo in esecuzione in una distribuzione OpenStack, scarica i file per il tuo sistema operativo Linux. Quindi, seguire la procedura per "sostituzione di un nodo Linux" .

Selezionare Avvia ripristino per configurare il nodo gateway

Dopo aver sostituito un nodo gateway, è necessario selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo in sostituzione del nodo guasto.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#) .
- Hai la passphrase di provisioning.
- Hai distribuito e configurato il nodo sostitutivo.

Passi

1. Da Grid Manager, seleziona **MANUTENZIONE > Attività > Ripristino**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Nodi in sospeso.

I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionarne uno finché non è stato reinstallato e non è pronto per il ripristino.

3. Immettere la **Passphrase di provisioning**.
4. Fare clic su **Avvia ripristino**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search Q				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	☒

Passphrase

Provisioning Passphrase

.....

Start Recovery

5. Monitorare l'avanzamento del ripristino nella tabella Nodo griglia in fase di ripristino.



Mentre la procedura di ripristino è in esecuzione, puoi fare clic su **Reimposta** per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che se si reimposta la procedura, il nodo verrà lasciato in uno stato indeterminato.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware:** Elimina il nodo della griglia virtuale distribuito. Quindi, quando sei pronto per riavviare il ripristino, ridistribuisce 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 ["Preparare l'apparecchio per la reinstallazione \(solo sostituzione della piattaforma\)"](#).

Ripristino da errori del nodo di archivio

Ripristino da errori del nodo di archivio

Il supporto per i nodi di archivio è stato rimosso.

Per informazioni sul recupero dei nodi di archivio, vedere ["Ripristino da errori del nodo di archivio \(sito di documentazione di StorageGRID 11.8\)"](#).

Sostituisci nodo Linux

Sostituisci nodo Linux

Se un errore richiede la distribuzione di uno o più nuovi host fisici o virtuali o la reinstallazione di Linux su un host esistente, distribuire e configurare l'host sostitutivo prima di poter ripristinare il nodo della griglia. Questa procedura è un passaggio del processo di ripristino del nodo della griglia per tutti i tipi di nodi della griglia.

"Linux" si riferisce a una distribuzione Red Hat® Enterprise Linux®, Ubuntu® o Debian®. Per un elenco delle versioni supportate, vedere ["Strumento matrice di interoperabilità NetApp \(IMT\)"](#).

Questa procedura viene eseguita solo come passaggio nel processo di ripristino dei nodi di archiviazione basati su software, dei nodi amministrativi primari o non primari o dei nodi gateway. I passaggi sono identici indipendentemente dal tipo di nodo della griglia che si sta ripristinando.

Se più di un nodo della griglia è ospitato su un host Linux fisico o virtuale, è possibile ripristinare i nodi della griglia in qualsiasi ordine. Tuttavia, il ripristino di un nodo amministrativo primario, se presente, impedisce che il ripristino di altri nodi della griglia si blocchi mentre tentano di contattare il nodo amministrativo primario per registrarsi per il ripristino.

Distribuisci nuovi host Linux

Salvo poche eccezioni, i nuovi host vengono preparati come durante il processo di installazione iniziale.

Per distribuire host Linux fisici o virtuali nuovi o reinstallati, seguire la procedura di preparazione degli host nelle istruzioni di installazione di StorageGRID per il sistema operativo Linux:

- ["Installa Linux \(Red Hat Enterprise Linux\)"](#)
- ["Installa Linux \(Ubuntu o Debian\)"](#)

Questa procedura include i passaggi per realizzare le seguenti attività:

1. Installa Linux.
2. Configurare la rete host.
3. Configurare l'archiviazione host.
4. Installare il motore del contenitore.
5. Installare il servizio host StorageGRID.



Interrompere l'operazione dopo aver completato l'attività "Installa il servizio host StorageGRID" nelle istruzioni di installazione. Non avviare l'attività "Distribuzione nodi griglia".

Mentre esegui questi passaggi, tieni presente le seguenti importanti linee guida:

- Assicurati di utilizzare gli stessi nomi di interfaccia host utilizzati sull'host originale.
- Se si utilizza l'archiviazione condivisa per supportare i nodi StorageGRID o si sono spostate alcune o tutte le unità o gli SSD dai nodi guasti a quelli sostitutivi, è necessario ristabilire le stesse mappature di archiviazione presenti sull'host originale. Ad esempio, se hai utilizzato 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 storage assegnato da un sistema NetApp ONTAP, verificare che il volume non abbia un criterio di suddivisione in livelli FabricPool abilitato. La disattivazione della suddivisione in livelli FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di archiviazione.



Non utilizzare mai FabricPool per riportare i dati relativi a StorageGRID a StorageGRID stesso. Il riordino dei dati StorageGRID su StorageGRID aumenta la complessità operativa e la risoluzione dei problemi.

Ripristina i nodi della griglia sull'host

Per ripristinare un nodo della griglia non riuscito su un nuovo host Linux, eseguire questi passaggi per ripristinare il file di configurazione del nodo.

1. [Ripristina e convalida il nodo](#) ripristinando il file di configurazione del nodo. Per una nuova installazione, è necessario creare un file di configurazione del nodo per ogni nodo della griglia da installare su un host. Quando si ripristina un nodo della griglia su un host sostitutivo, si ripristina o si sostituisce il file di configurazione del nodo per tutti i nodi della griglia non riusciti.
2. [Avviare il servizio host StorageGRID](#) .
3. Secondo necessità, [recuperare tutti i nodi che non riescono ad avviarsi](#) .

Se sono stati conservati volumi di archiviazione a blocchi dall'host precedente, potrebbe essere necessario eseguire ulteriori procedure di ripristino. I comandi in questa sezione aiutano a determinare quali procedure aggiuntive sono necessarie.

Ripristinare e convalidare i nodi della griglia

È necessario ripristinare i file di configurazione della griglia per tutti i nodi della griglia non riusciti, quindi convalidare i file di configurazione della griglia e risolvere eventuali errori.

Informazioni su questo compito

È possibile importare qualsiasi nodo della griglia che dovrebbe essere presente sull'host, purché il suo `/var/local` il volume non è andato perso a causa del guasto dell'host precedente. Ad esempio, il `/var/local` Il volume potrebbe ancora esistere se hai utilizzato un archivio condiviso per i volumi di dati del sistema StorageGRID , come descritto nelle istruzioni di installazione di StorageGRID per il tuo sistema operativo Linux. L'importazione del nodo ripristina il file di configurazione del nodo nell'host.

Se non è possibile importare i nodi mancanti, è necessario ricreare i relativi file di configurazione della griglia.

È quindi necessario convalidare il file di configurazione della griglia e risolvere eventuali problemi di rete o di archiviazione che potrebbero verificarsi prima di riavviare StorageGRID. Quando si ricrea il file di configurazione per un nodo, è necessario utilizzare per il nodo sostitutivo lo stesso nome utilizzato per il nodo che si sta ripristinando.

Per maggiori informazioni sulla posizione del `/var/local` volume per un nodo.

- ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
- ["Installa StorageGRID su Ubuntu o Debian"](#)

Passi

1. Nella riga di comando dell'host ripristinato, elencare tutti i nodi StorageGRID attualmente configurati: `sudo storagegrid node list`

Se non è configurato alcun nodo della griglia, non ci sarà alcun output. Se alcuni nodi della griglia sono configurati, l'output dovrebbe 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 della griglia che hanno un `/var/local` volume:

- a. Eseguire il seguente comando per ogni nodo che si desidera importare: `sudo storagegrid node import node-var-local-volume-path`

Il `storagegrid node import` comando riesce solo se il nodo di destinazione è stato arrestato correttamente sull'host su cui è stato eseguito l'ultima volta. In caso contrario, verrà visualizzato 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 vedi l'errore che il nodo è di proprietà di un altro host, esegui di nuovo il comando con `--force` flag 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 di potersi ricongiungere alla griglia, come descritto in ["Prossimi passi: eseguire ulteriori passaggi di ripristino, se necessario"](#).

3. Per i nodi della griglia che non hanno un `/var/local` volume, ricreare il file di configurazione del nodo per ripristinarlo sull'host. Per le istruzioni, vedere:

- ["Crea file di configurazione del nodo per Red Hat Enterprise Linux"](#)
- ["Crea file di configurazione del nodo per Ubuntu o Debian"](#)



Quando si ricrea il file di configurazione per un nodo, è necessario utilizzare per il nodo sostitutivo lo stesso nome utilizzato per il nodo che si sta ripristinando. Per le distribuzioni Linux, assicurarsi che il nome del file di configurazione contenga il nome del nodo. Quando possibile, dovresti utilizzare le stesse interfacce di rete, le stesse mappature dei dispositivi a blocchi e gli stessi indirizzi IP. Questa pratica riduce al minimo la quantità di dati che devono essere copiati sul nodo durante il ripristino, il che potrebbe rendere il ripristino significativamente più rapido (in alcuni casi, minuti anziché settimane).



Se si utilizzano nuovi dispositivi a blocchi (dispositivi che il nodo StorageGRID non utilizzava in precedenza) come valori per una qualsiasi delle variabili di configurazione che iniziano con `BLOCK_DEVICE_` quando si ricrea il file di configurazione per un nodo, seguire le linee guida in [Correggi gli errori dei dispositivi 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 mostrato nell'output dell'elenco dei nodi storagegrid:

```
sudo storagegrid node validate node-name
```

È necessario risolvere eventuali errori o avvisi prima di avviare il servizio host StorageGRID. Le sezioni seguenti forniscono maggiori dettagli sugli errori che potrebbero avere un significato particolare durante il ripristino.

Correggi gli errori di interfaccia di rete mancante

Se la rete host non è configurata correttamente o un nome è scritto in modo errato, si verifica un errore quando StorageGRID controlla la mappatura specificata nel `/etc/storagegrid/nodes/node-name.conf` file.

Potresti visualizzare un errore o un avviso corrispondente a questo schema:

```
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 la rete Grid, la rete di amministrazione o la rete client. Questo errore significa che il `/etc/storagegrid/nodes/node-name.conf` il file mappa la rete StorageGRID indicata all'interfaccia host denominata `host-interface-name`, ma non esiste alcuna interfaccia con quel nome sull'host corrente.

Se ricevi questo errore, verifica di aver completato i passaggi in ["Distribuisci nuovi host Linux"](#). Utilizzare per tutte le interfacce host gli stessi nomi 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 cambiare 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 bond o bridge. È necessario configurare una VLAN (o un'altra interfaccia virtuale) sul dispositivo di bonding sull'host oppure utilizzare un bridge e una coppia Ethernet virtuale (veth).

Correggi gli errori dei dispositivi a blocchi mancanti

Il sistema verifica che ogni nodo recuperato sia mappato a un file speciale valido del dispositivo a blocchi o a

un collegamento simbolico valido a un file speciale del 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 osserva un errore corrispondente a questo schema:

```
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
```

Ciò significa che `/etc/storagegrid/nodes/node-name.conf` mappa il dispositivo a blocchi utilizzato da *node-name* per PURPOSE al percorso specificato nel file system Linux, ma in quella posizione non è presente un file speciale valido per il dispositivo a blocchi o un collegamento simbolico a un file speciale per il dispositivo a blocchi.

Verifica di aver completato i passaggi in ["Distribuisci nuovi host Linux"](#). Utilizzare gli stessi nomi di dispositivo persistenti 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 archiviazione appropriate e modificare il file di configurazione del nodo per cambiare il valore di `BLOCK_DEVICE_PURPOSE` per puntare al nuovo file speciale del dispositivo a blocchi.

Determina la dimensione e la categoria di archiviazione appropriate utilizzando le tabelle per il tuo sistema operativo Linux:

- ["Requisiti di archiviazione e prestazioni per Red Hat Enterprise Linux"](#)
- ["Requisiti di archiviazione e prestazioni per Ubuntu o Debian"](#)

Prima di procedere con la sostituzione del dispositivo a blocchi, rivedere i consigli per la configurazione dell'archiviazione host:

- ["Configurare l'archiviazione host per Red Hat Enterprise Linux"](#)
- ["Configurare l'archiviazione host per Ubuntu o Debian"](#)



Se è necessario fornire un nuovo dispositivo di archiviazione a blocchi per una qualsiasi delle variabili del file di configurazione che iniziano con `BLOCK_DEVICE_` poiché il dispositivo a blocchi originale è andato 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 sarà formattato se si utilizza un archivio condiviso ed è stato creato un nuovo volume. In caso di dubbi, eseguire il seguente comando su tutti i nuovi file speciali del dispositivo di archiviazione a blocchi.



Eseguire il seguente comando solo per i nuovi dispositivi di archiviazione a blocchi. Non eseguire questo comando se ritieni che l'archiviazione a blocchi contenga ancora dati validi per il nodo da ripristinare, poiché tutti i dati presenti sul dispositivo andranno persi.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Avvia il servizio host StorageGRID

Per avviare i nodi StorageGRID e assicurarsi che si riavviino dopo un riavvio dell'host, è necessario abilitare e avviare il servizio host StorageGRID .

Passi

1. Eseguire i seguenti comandi su ciascun host:

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

2. Eseguire il seguente comando per assicurarsi che la distribuzione proceda:

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

3. Se un nodo restituisce lo stato "Non in esecuzione" o "Arrestato", eseguire il seguente comando:

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

4. Se in precedenza hai abilitato e avviato il servizio host StorageGRID (o se non sei sicuro che il servizio sia stato abilitato e avviato), esegui anche il seguente comando:

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

Recupera i nodi che non riescono ad avviarsi normalmente

Se un nodo StorageGRID non si ricongiunge normalmente alla griglia e non viene visualizzato come recuperabile, potrebbe essere danneggiato. È possibile forzare il nodo in modalità di ripristino.

Passi

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 errate dell'interfaccia di rete o di un indirizzo IP o gateway di rete della griglia non corretti.

2. Se la configurazione di rete è corretta, emettere il `force-recovery` comando:

```
sudo storagegrid node force-recovery node-name
```

3. Eseguire i passaggi di ripristino aggiuntivi per il nodo. Vedere ["Prossimi passi: eseguire ulteriori passaggi di ripristino, se necessario"](#) .

Prossimi passi: eseguire ulteriori passaggi di ripristino, se necessario

A seconda delle azioni specifiche intraprese per far funzionare i nodi StorageGRID sull'host sostitutivo, potrebbe essere necessario eseguire ulteriori passaggi 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 non riuscito sul nuovo host.

Azioni correttive e prossimi passi

Durante la sostituzione del nodo, potrebbe essere stato necessario adottare una delle seguenti misure correttive:

- Dovevi usare il `--force` flag per importare il nodo.
- Per qualsiasi `<PURPOSE>`, il valore del `BLOCK_DEVICE_<PURPOSE>` La variabile del file di configurazione si riferisce a un dispositivo a blocchi che non contiene gli stessi dati che conteneva prima del guasto dell'host.
- Hai emesso `storagegrid node force-recovery node-name` per il nodo.
- Hai aggiunto un nuovo dispositivo a blocchi.

Se hai adottato **una** di queste azioni correttive, devi eseguire ulteriori passaggi di ripristino.

Tipo di recupero	Passo successivo
Nodo di amministrazione primario	"Configura il nodo di amministrazione primario sostitutivo"
Nodo amministratore 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 (basato su software): • Se dovessi usare il <code>--force</code> flag per importare il nodo, oppure hai emesso <code>storagegrid node force-recovery node-name</code> • Se hai dovuto eseguire una reinstallazione completa del nodo o hai dovuto ripristinare <code>/var/local</code>	"Selezionare Avvia ripristino per configurare il nodo di archiviazione"
Nodo di archiviazione (basato su software): • Se hai aggiunto un nuovo dispositivo a blocchi. • Se, per qualsiasi <code><PURPOSE></code>, il valore del <code>BLOCK_DEVICE_<PURPOSE></code> La variabile del file di configurazione si riferisce a un dispositivo a blocchi che non contiene gli stessi dati che conteneva prima del guasto dell'host.	"Ripristinare da un errore del volume di archiviazione in cui l'unità di sistema è intatta"

Sostituisci nodo VMware

Quando si ripristina un nodo StorageGRID non riuscito ospitato su VMware, si rimuove il nodo non riuscito e si distribuisce un nodo di ripristino.

Prima di iniziare

Hai stabilito che la macchina virtuale non può essere ripristinata e deve essere sostituita.

Informazioni su questo compito

Per prima cosa, utilizzare VMware vSphere Web Client per rimuovere la macchina virtuale associata al nodo della griglia non riuscito. Quindi, puoi distribuire una nuova macchina virtuale.

Questa procedura è solo un passaggio nel processo di ripristino del nodo della griglia. La procedura di rimozione e distribuzione dei nodi è la stessa per tutti i nodi VMware, inclusi i nodi di amministrazione, i nodi di archiviazione e i nodi gateway.

Passi

1. Accedi a VMware vSphere Web Client.
2. Passare alla macchina virtuale del nodo della griglia non riuscita.
3. Prendi nota di tutte le informazioni necessarie per distribuire il nodo di ripristino.
 - a. Fare clic con il pulsante destro del mouse sulla macchina virtuale, selezionare la scheda **Modifica impostazioni** e prendere nota delle impostazioni in uso.
 - b. Selezionare la scheda **Opzioni vApp** per visualizzare e registrare le impostazioni di rete del nodo della griglia.
4. Se il nodo della griglia non riuscito è un nodo di archiviazione, determinare se uno qualsiasi dei dischi rigidi virtuali utilizzati per l'archiviazione dei dati è integro e conservarlo per ricollegarlo al nodo della griglia ripristinato.
5. Spegnerne la macchina virtuale.
6. Selezionare **Azioni > Tutte le azioni vCenter > Elimina dal disco** per eliminare la macchina virtuale.
7. Distribuisce una nuova macchina virtuale come nodo sostitutivo e collegala a una o più reti StorageGRID . Per le istruzioni vedere ["Distribuzione di un nodo StorageGRID come macchina virtuale"](#) .

Quando si distribuisce il nodo, è possibile rimappare le porte del nodo o aumentare le impostazioni della CPU o della memoria.



Dopo aver distribuito il nuovo nodo, è possibile aggiungere nuovi dischi virtuali in base ai requisiti di archiviazione, ricollegare eventuali dischi rigidi virtuali conservati dal nodo grid non riuscito rimosso in precedenza, oppure effettuare entrambe le operazioni.

8. Completare la procedura di ripristino del nodo, in base al tipo di nodo che si sta ripristinando.

Tipo di nodo	Vai a
Nodo di amministrazione primario	"Configura il nodo di amministrazione primario sostitutivo"
Nodo amministratore non primario	"Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario"

Tipo di nodo	Vai a
Nodo Gateway	"Selezionare Avvia ripristino per configurare il nodo gateway"
Nodo di archiviazione	"Selezionare Avvia ripristino per configurare il nodo di archiviazione"

Sostituisci il nodo non riuscito con l'appliance dei servizi

Sostituisci il nodo non riuscito con l'appliance dei servizi

È possibile utilizzare un'appliance di servizi per ripristinare un nodo gateway non riuscito, un nodo amministrativo non primario non riuscito o un nodo amministrativo primario non riuscito ospitato su VMware, un host Linux o un'appliance di servizi. Questa procedura è un passaggio della procedura di ripristino del nodo della griglia.

Prima di iniziare

- Hai stabilito che una delle seguenti situazioni è vera:
 - La macchina virtuale che ospita il nodo non può essere ripristinata.
 - L'host Linux fisico o virtuale per il nodo della griglia è guasto e deve essere sostituito.
 - È necessario sostituire l'appliance di servizi che ospita il nodo della griglia.
- Hai confermato che la versione di StorageGRID Appliance Installer sull'appliance dei servizi corrisponde alla versione software del tuo sistema StorageGRID . Vedere ["Verificare e aggiornare la versione di StorageGRID Appliance Installer"](#) .



Non distribuire contemporaneamente un'appliance di servizi SG110 e SG1100 oppure un'appliance di servizi SG100 e SG1000 nello stesso sito. Potrebbero verificarsi prestazioni imprevedibili.

Informazioni su questo compito

È possibile utilizzare un'appliance di servizi per ripristinare un nodo della griglia non riuscito nei seguenti casi:

- Il nodo non riuscito era ospitato su VMware o Linux (["cambio di piattaforma"](#))
- Il nodo non riuscito era ospitato su un'appliance di servizi (["sostituzione della piattaforma"](#))

Installa l'appliance dei servizi (solo cambio piattaforma)

Quando si ripristina un nodo della griglia non riuscito ospitato su VMware o 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 del nodo (nome del sistema) del nodo non riuscito.

Prima di iniziare

Sono disponibili le seguenti informazioni sul nodo non riuscito:

- **Nome nodo:** è necessario installare l'appliance dei servizi utilizzando lo stesso nome nodo del nodo non riuscito. Il nome del nodo è il nome host (nome del sistema).

- **Indirizzi IP:** è possibile assegnare all'appliance dei servizi gli stessi indirizzi IP del nodo guasto, che è l'opzione preferita, oppure è possibile selezionare un nuovo indirizzo IP non utilizzato su ciascuna rete.

Informazioni su questo compito

Eseguire questa procedura solo se si sta ripristinando un nodo non riuscito ospitato su VMware o Linux e lo si sta sostituendo con un nodo ospitato su un'appliance di servizi.

Passi

1. Seguire le istruzioni per installare un nuovo dispositivo di servizi. Vedere ["Avvio rapido per l'installazione dell'hardware"](#).
2. Quando viene richiesto un nome nodo, utilizzare il nome del nodo non riuscito.

Preparare l'apparecchio per la reinstallazione (solo sostituzione della piattaforma)

Quando si ripristina un nodo della griglia ospitato su un'appliance di servizi, è necessario innanzitutto preparare l'appliance per la reinstallazione del software StorageGRID.

Eseguire questa procedura solo se si sta sostituendo un nodo non riuscito ospitato su un'appliance di servizi. Non seguire questi passaggi se il nodo non riuscito era originariamente ospitato su VMware o su un host Linux.

Passi

1. Accedi al nodo della griglia non riuscito:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.Quando si accede come root, il prompt cambia da `$` a `#`.
2. Preparare l'appliance per l'installazione del software StorageGRID. Inserisci: `sgareinstall`
3. Quando ti viene chiesto di continuare, inserisci: `y`

L'appliance si riavvia e la sessione SSH termina. In genere occorrono circa 5 minuti prima che StorageGRID Appliance Installer diventi disponibile, anche se in alcuni casi potrebbe essere necessario attendere fino a 30 minuti.

L'appliance dei servizi viene reimpostata e i dati sul nodo della griglia non sono più accessibili. Gli indirizzi IP configurati durante il processo di installazione originale dovrebbero rimanere intatti; tuttavia, si consiglia di confermarlo al termine della procedura.

Dopo aver eseguito il `sgareinstall` comando, tutti gli account, le password e le chiavi SSH forniti StorageGRID vengono rimossi e vengono generate nuove chiavi host.

Avvia l'installazione del software sull'appliance dei servizi

Per installare un Gateway Node o un Admin Node su un'appliance di servizi, utilizzare StorageGRID Appliance Installer, incluso nell'appliance.

Prima di iniziare

- L'apparecchio è installato in un rack, connesso alle reti e acceso.
- I collegamenti di rete e gli indirizzi IP vengono configurati per l'appliance tramite StorageGRID Appliance Installer.
- Se si installa un Gateway Node o un Admin Node non primario, si conosce l'indirizzo IP del Admin Node primario per la griglia StorageGRID .
- Tutte le subnet della rete Grid elencate nella pagina Configurazione IP del programma di installazione dell'appliance StorageGRID sono definite nell'elenco delle subnet della rete Grid sul nodo di amministrazione primario.

Vedere ["Avvio rapido per l'installazione dell'hardware"](#) .

- Stai utilizzando un ["browser web supportato"](#) .
- Hai uno degli indirizzi IP assegnati all'appliance. È possibile utilizzare l'indirizzo IP per la rete amministrativa, la rete Grid o la rete client.
- Se si installa un nodo di amministrazione 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 dei servizi durante la produzione. Se la versione precaricata del software corrisponde alla versione utilizzata nella distribuzione StorageGRID , i file di installazione non sono necessari.

Informazioni su questo compito

Per installare il software StorageGRID su un'appliance di servizi:

- Per un nodo di amministrazione primario, è necessario specificare il nome del nodo e quindi caricare i pacchetti software appropriati (se necessario).
- Per un nodo amministrativo non primario o un nodo gateway, specificare o confermare l'indirizzo IP del nodo amministrativo primario e il nome del nodo.
- Si avvia l'installazione e si attende che i volumi vengano configurati e il software installato.
- A metà del processo, l'installazione si interrompe. Per riprendere l'installazione, è necessario accedere a Grid Manager e configurare il nodo in sospeso come sostituto del nodo non riuscito.
- Dopo aver configurato il nodo, il processo di installazione dell'appliance viene completato e l'appliance viene riavviata.

Passi

1. Aprire un browser e immettere uno degli indirizzi IP per l'appliance dei servizi.

```
https://Controller_IP:8443
```

Viene visualizzata la home page del programma di installazione dell'appliance StorageGRID .

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking
Configure Hardware
Monitor Installation
Advanced

Home

This Node

Node type
Gateway

Node name
NetApp-SGA

Cancel
Save

Primary Admin Node connection

Enable Admin Node discovery
☒
Uncheck to manually enter the Primary Admin Node IP

Connection state
Admin Node discovery is in progress

Cancel
Save

Installation

Current state
Unable to start installation. The Admin Node connection is not ready.

Start installation

2. Per installare un nodo di amministrazione primario:

- Nella sezione Questo nodo, per **Tipo di nodo**, seleziona **Amministratore principale**.
- Nel campo **Nome nodo**, immettere lo stesso nome utilizzato per il nodo che si sta ripristinando e fare clic su **Salva**.
- Nella sezione Installazione, controlla la versione del software elencata in Stato attuale
Se la versione del software pronta per l'installazione è corretta, passare direttamente alla sezione [Fase di installazione](#) .
- Se è necessario caricare una versione diversa del software, nel menu **Avanzate** selezionare ***Carica software StorageGRID ***.

Viene visualizzata la pagina Carica software StorageGRID .

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking
Configure Hardware
Monitor Installation
Advanced

Upload StorageGRID Software

If this node is the primary Admin Node of a new deployment, you must use this page to upload the StorageGRID software installation package, unless the version of the software you want to install has already been uploaded. If you are adding this node to an existing deployment, you can avoid network traffic by uploading the installation package that matches the software version running on the existing grid. If you do not upload the correct package, the node obtains the software from the grid's primary Admin Node during installation.

Current StorageGRID Installation Software

Version	None
Package Name	None

Upload StorageGRID Installation Software

Software Package	Browse
Checksum File	Browse

- a. Fare clic su **Sfoglia** per caricare il **Pacchetto software** e il **File di checksum** 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 **Tipo di nodo**, seleziona **Gateway** o **Amministratore non primario**, a seconda del tipo di nodo che stai ripristinando.
 - b. Nel campo **Nome nodo**, immettere lo stesso nome utilizzato per il nodo che si sta ripristinando e fare clic su **Salva**.
 - c. Nella sezione Connessione al nodo di amministrazione primario, determinare se è necessario specificare l'indirizzo IP per il nodo di amministrazione primario.

Il programma di installazione dell'appliance StorageGRID può rilevare automaticamente questo indirizzo IP, presupponendo che il nodo di amministrazione primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente sulla stessa subnet.

- d. Se questo indirizzo IP non viene visualizzato o è necessario modificarlo, specificare l'indirizzo:

Opzione	Descrizione
Inserimento manuale dell'IP	a. Deselezionare la casella di controllo Abilita individuazione nodo amministratore. b. Inserire manualmente l'indirizzo IP. c. Fare clic su Salva. d. Attendi che lo stato di connessione per il nuovo indirizzo IP diventi "pronto".

Opzione	Descrizione
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo Abilita individuazione nodo amministratore. b. Dall'elenco degli indirizzi IP rilevati, seleziona il nodo di amministrazione primario per la griglia in cui verrà distribuito questo dispositivo di servizi. c. Fare clic su Salva. d. Attendi che lo stato di connessione per il nuovo indirizzo IP diventi "pronto".

4. Nella sezione Installazione, confermare che lo stato corrente sia Pronto per avviare l'installazione del nome del nodo e che il pulsante **Avvia installazione** sia abilitato.

Se il pulsante **Avvia installazione** non è abilitato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per le istruzioni, consultare le istruzioni di manutenzione dell'apparecchio.

5. Dalla home page di StorageGRID Appliance Installer, fare clic su **Avvia installazione**.

Lo stato corrente cambia in "Installazione in corso" e viene visualizzata la pagina Installazione del monitor.



Se è necessario accedere manualmente alla pagina Installazione monitor, fare clic su **Installazione monitor** dalla barra dei menu.

Installazione di apparecchiature di monitoraggio dei servizi

Il programma di installazione dell'appliance StorageGRID fornisce informazioni sullo stato fino al completamento dell'installazione. Una volta completata l'installazione del software, l'appliance viene riavviata.

Passi

1. Per monitorare l'avanzamento dell'installazione, fare clic su **Monitora installazione** dalla barra dei menu.

La pagina Installazione del monitor mostra lo stato di avanzamento dell'installazione.

Monitor Installation

1. Configure storage		Complete
2. Install OS		Running
Step	Progress	Status
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running
3. Install StorageGRID		Pending
4. Finalize installation		Pending

La barra di stato blu indica quale attività è attualmente in corso. Le barre di stato verdi indicano le attività completate con successo.



Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si sta rieseguendo un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "Ignorato".

2. Esaminare lo stato di avanzamento delle prime due fasi di installazione.

◦ 1. Configura l'archiviazione

Durante questa fase, il programma di installazione cancella qualsiasi configurazione esistente dalle unità e configura le impostazioni dell'host.

◦ 2. Installa 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 oppure installa il sistema operativo di base dal pacchetto di installazione per il nodo di amministrazione primario.

3. Continuare a monitorare l'avanzamento dell'installazione finché non si verifica una delle seguenti situazioni:

- Per i nodi gateway dell'appliance o i nodi amministrativi dell'appliance non primaria, la fase **Install StorageGRID** si interrompe e sulla console incorporata viene visualizzato un messaggio che richiede di approvare questo nodo sul nodo amministrativo tramite Grid Manager.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

```

Connected (unencrypted) to: QEMU
/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Per i nodi amministrativi primari dell'appliance, viene visualizzata una quinta fase (Caricamento del programma di installazione StorageGRID). Se la quinta fase dura più di 10 minuti, aggiornare la pagina manualmente.

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking
Configure Hardware
Monitor Installation
Advanced

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Complete
4. Finalize installation	Complete
5. Load StorageGRID Installer	Running

Step	Progress	Status
Starting StorageGRID Installer		Do not refresh. You will be redirected when the installer is ready

4. Passare al passaggio successivo del processo di ripristino per il tipo di nodo griglia dell’appliance che si sta ripristinando.

Tipo di recupero	Riferimento
Nodo Gateway	"Selezionare Avvia ripristino per configurare il nodo gateway"
Nodo amministratore non primario	"Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario"
Nodo di amministrazione primario	"Configura il nodo di amministrazione primario sostitutivo"

Come il supporto tecnico recupera un sito

In caso di guasto di un intero sito StorageGRID o di guasto di più nodi di archiviazione, è necessario contattare l’assistenza tecnica. Il supporto tecnico valuterà la tua situazione, svilupperà un piano di ripristino e quindi ripristinerà i nodi o il sito guasti in modo da soddisfare i tuoi obiettivi aziendali, ottimizzare i tempi di ripristino ed evitare inutili perdite di dati.



Il ripristino del sito può essere eseguito solo dal supporto tecnico.

I sistemi StorageGRID sono resistenti a un’ampia gamma di guasti e consentono di eseguire autonomamente con successo numerose procedure di ripristino e manutenzione. Tuttavia, è difficile creare una procedura di ripristino del sito semplice e generalizzata, perché i passaggi dettagliati dipendono da fattori specifici della situazione. Per esempio:

- **I tuoi obiettivi aziendali:** dopo la perdita completa di un sito StorageGRID , dovresti valutare il modo migliore per soddisfare i tuoi obiettivi aziendali. Ad esempio, vuoi ricostruire il sito perduto sul posto? Desideri sostituire il sito StorageGRID perso in una nuova posizione? La situazione di ogni cliente è diversa e il piano di ripristino deve essere progettato tenendo conto delle tue priorità.
- **Natura esatta del guasto:** prima di iniziare il ripristino del sito, verificare se i nodi del sito danneggiato sono intatti o se i nodi di archiviazione contengono oggetti recuperabili. Se si ricostruiscono nodi o volumi di archiviazione contenenti dati validi, potrebbero verificarsi perdite di dati non necessarie.

- **Criteri ILM attivi:** il numero, il tipo e la posizione delle copie degli oggetti nella griglia sono controllati dai criteri ILM attivi. Le specifiche delle policy ILM possono influire sulla quantità di dati recuperabili, nonché sulle tecniche specifiche richieste per il recupero.



Se un sito contiene l'unica copia di un oggetto e il sito viene perso, anche l'oggetto viene perso.

- **Coerenza del bucket (o contenitore):** la coerenza applicata a un bucket (o contenitore) determina se StorageGRID replica completamente i metadati degli oggetti su tutti i nodi e siti prima di comunicare a un client che l'acquisizione dell'oggetto è avvenuta correttamente. Se il valore di coerenza consente una coerenza finale, alcuni metadati dell'oggetto potrebbero essere andati persi a causa dell'errore del sito. Ciò può influire sulla quantità di dati recuperabili e potenzialmente sui dettagli della procedura di recupero.
- **Cronologia delle modifiche recenti:** i dettagli della procedura di ripristino possono essere influenzati dal fatto che al momento del guasto fossero in corso procedure di manutenzione o che siano state apportate modifiche recenti alle policy ILM. Prima di iniziare il ripristino del sito, il supporto tecnico deve valutare la cronologia recente della rete e la sua situazione attuale.



Il ripristino del sito può essere eseguito solo dal supporto tecnico.

Questa è una panoramica generale del processo utilizzato dal supporto tecnico per ripristinare un sito non funzionante:

1. Supporto tecnico:
 - a. Effettua una valutazione dettagliata del fallimento.
 - b. Collaboriamo con voi per rivedere i vostri obiettivi aziendali.
 - c. Sviluppa un piano di recupero su misura per la tua situazione.
2. Se il nodo di amministrazione primario non funziona, il supporto tecnico lo recupera.
3. Il supporto tecnico recupera tutti i nodi di archiviazione, seguendo questo schema:
 - a. Sostituire l'hardware del nodo di archiviazione o le macchine virtuali secondo necessità.
 - b. Ripristinare i metadati dell'oggetto nel sito in cui si è verificato il problema.
 - c. Ripristinare i dati degli oggetti nei nodi di archiviazione recuperati.



Se vengono utilizzate le procedure di ripristino per un singolo nodo di archiviazione guasto, si verificherà una perdita di dati.



Quando un intero sito non funziona più, il supporto tecnico utilizza comandi specializzati per ripristinare correttamente gli oggetti e i metadati degli oggetti.

4. Il supporto tecnico recupera altri nodi guasti.

Dopo aver recuperato i metadati e i dati degli oggetti, il supporto tecnico utilizza procedure standard per recuperare i nodi gateway non funzionanti o i nodi amministrativi non primari.

Informazioni correlate

["Dismissione del sito"](#)

Come abilitare StorageGRID nel tuo ambiente

Vai a "[Come abilitare StorageGRID](#)" per scoprire come testare e abilitare le applicazioni nel tuo ambiente StorageGRID .

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 ristrutturata, 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 accesso a dichiarazioni di copyright, marchi commerciali, brevetti e altro ancora.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina Marchi NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

["https://www.netapp.com/company/legal/trademarks/"](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>

Politica sulla riservatezza

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp .

https://library.netapp.com/ecm/ecm_download_file/ECMLP3330669

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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